

Fin Accelerate  | EMPOWERED BY
Jones Day



FINACCELERATIONS

The Legal Oracle to Fintech

www.finaccelerate.com

CONTENTS

CHAPTER I	INTRODUCTION TO THE FINACCELERATE PROGRAM	1
CHAPTER II	STATE-BY-STATE LEGAL SURVEY OF DIGITAL ASSET REGULATIONS	4
	Heat Map of 50-State Digital Asset Regulations*	5
	Alabama	6
	Alaska	6
	Arizona	6
	Arkansas	7
	California	7
	Colorado	8
	Connecticut	8
	Delaware	8
	District of Columbia	9
	Florida	9
	Georgia	9
	Guam	10
	Hawaii	10
	Idaho	10
	Illinois	11
	Indiana	11
	Iowa	12
	Kansas	12
	Kentucky	12
	Louisiana	13
	Maine	13
	Maryland	13
	Massachusetts	14
	Michigan	14
	Minnesota	14
	Mississippi	15
	Missouri	15
	Montana	16
	Nebraska	16
	Nevada	17
	New Hampshire	17
	New Jersey	18
	New Mexico	18
	New York	18
	North Carolina	19
	North Dakota	19
	Ohio	19
	Oklahoma	20
	Oregon	20
	Pennsylvania	20
	Puerto Rico	21
	Rhode Island	21
	South Carolina	21
	South Dakota	22
	Tennessee	22
	Texas	23

CONTENTS

Utah	23	Washington	25
Vermont	24	West Virginia	25
Virgin Islands	24	Wisconsin	26
Virginia	24	Wyoming	26
CHAPTER III	2022 UCC DIGITAL ASSET AMENDMENTS		27
	2022 Amendments to Uniform Commercial Code: Welcome Clarity on Commercial Transactions Involving Digital Assets		28
CHAPTER IV	REGULATORY ISSUES (U.S. FEDERAL)		30
	Digital Assets Defined: Writing Digital Assets into the Bankruptcy Code		31
	Digital Assets Defined: Federal Agencies Weigh Response to President Biden’s Executive Order on Digital Assets		34
	A DAO is No Defense: CFTC Says Decentralization does not Immunize DeFi from Regulation		41
	Proposed Stabenow-Boozman Bill Falls Short in Bringing Regulatory Certainty to Digital Assets Space		45
	Digital Assets Defined: How Lummis-Gillibrand Will Shape the Coming Fintech Debate		49
	Digital Assets Defined: Consumer Protection and Cybersecurity Enter the Stage		58
	Digital Assets Defined: SEC, CFTC, and Ancillary (Illusory?) Assets		63
	Digital Assets Defined: How Lummis-Gillibrand Will Shore Up Stablecoins		68
	Digital Assets Defined The Tax Code’s Take		72
	What the Federal Government Is Doing About Stablecoins		74
	CFPB to Invoke “Dormant Authority” to Supervise Nonbank Fintech Companies		77
	The \$Year of the Rug Pull (Real Clear Markets)		78
	White House Issues Executive Order Calling for Inter-Agency Study of Digital Assets		80
	SDNY Issues Two Rulings in Closely Watched Enforcement Action Against Ripple Labs		81
	FinCEN Warns Institutions of Sanctions Evasion Risks		84
	SEC Proposes to Broadly Expand the Definition of an “Exchange” and Amend Regulation ATS		86

CONTENTS

The Legal Revolution That Might Save Cryptocurrency	90
The Brewing Turf War in Crypto Regulation (CoinDeskTV)	92
U.S. Federal Banking Regulators Announce Plan for Crypto-Asset Policy Initiative	93
Regulating the Ether: Lessons for the MENA Digital Asset Industry from U.S. Enforcement Actions	95
OFAC Issues Additional Ransomware Guidance and Designates Virtual Currency Exchange	99
SEC Chairman Signals Intensified Enforcement and Regulatory Scrutiny of Crypto and DeFi	101
FinCEN Issues First U.S. Priorities for Anti-Money Laundering and Counter-Terrorism Financing	102
OCC Victory in Second Circuit Not a Clear Victory for Fintech Charters	103
Takeaways from a Landmark Cryptocurrency Antitrust Case	106
DeFi Identified as Potential Focus for CFTC Enforcement Action	107
Cryptocurrency Tax Update: Impact of New IRS Guidance and Proposed U.S. Tax Rate Increase	108
SEC’s Division of Examinations Reiterates Focus on Digital Asset Securities	109
SEC’s Division of Examinations Issues 2021 Examination Priorities	110
Fintech: OCC Takes Significant Step in Permitting National Banks to Use INVN and Stablecoin Technology	114
Court Rules That Sales of Digital Tokens Were Illegal Unregistered Securities Offerings	117
FinCEN Issues Guidance on Ransomware Attacks	118
OCC Concludes That National Banks May Provide Cryptocurrency Custody Services	120
No Search Warrant Required for Records of Bitcoin Transactions, the Fifth Circuit Holds	121
Digital Assets Defined: Federal Agencies Weigh Response to President Biden’s Executive Order on Digital Assets	123
Digital Assets Defined: Writing Digital Assets into the Bankruptcy Code	130
Bank Regulators Issue Joint Statement on Safety and Soundness of Crypto Activities	133
CFTC Partners with SEC and DOJ to Bring Coordinated DeFi Enforcement Action Targeting Oracle Manipulation	135
Fed Policy Statement Adds Hurdles to Digital Asset Activities and Innovation by State Banks	137
“MetaBirkins” Bagged: NFT Creator Found Liable for Trademark Infringement	139
Hard Forks and Airdrops: The IRS Issues Cryptocurrency Tax Guidance	140

CONTENTS

CHAPTER V	REGULATORY ISSUES (U.S.-STATE LEVEL)	141
	California Moves to Regulate Digital Asset Exchanges and Cryptocurrency Companies	142
	California Governor Orders Agencies to Create Transparent Regulatory Framework for Blockchain and Digital Assets	144
	New York Joins Other States in Enforcement Actions Against Unregistered Virtual Currency Lending Platforms	145
	Crypto and the Reach of Unclaimed Property Laws: Is New Illinois Legislation the Future?	146
	New York Department of Financial Services Imposes Penalty and Consent Order for Cybersecurity Violations	149
	California Passes Legislation to Create Mini-CFPB	150
	First Department Upholds NY AG’s Authority to Investigate Virtual Currency Under the Martin Act	152
	New York Department of Financial Services Issues Guidance on Virtual Currency Custodial Services	154
CHAPTER VI	REGULATORY ISSUES (INTERNATIONAL, EU)	156
	Dubai’s Digital Assets Aspirations	157
	Digital Markets Act: European Union Adopts New “Competition” Regulations for Certain Digital Platforms	161
	EU Extends Travel Rule to Crypto-Assets	169
	Australian Financial Services Regulatory Update	170
	Breakthrough in Italian Cryptocurrency Regulation: Statutory Registration for Providers and Exchangers	172
	Capital Relief for Software Assets: European Commission Amends Own Fund Requirements	173
	No-Deal Brexit—Preventing Disruption to Data Transfers	175
	Boosting Blockchain: Germany to Introduce Electronic Securities	177
	Facilitating Transatlantic Fintech Innovation and Cooperation: The New MOU Between the NYDFS and the French ACPR	179
	China Accelerates Blockchain Adoption in the New Decade	181

CONTENTS

CHAPTER VII AI AND NFTs	184
Which AI Components Are Copyright Protectable and Which Are Not?	185
Regulating Artificial Intelligence: European Commission Launches Proposals	187
IP Protection of Artificial Intelligence in Europe: Tailor-Made Solutions Required	190
White House Announces Artificial Intelligence Bill of Rights	193
NFTs: U.S., EU, and UK Key Copyright Considerations	194
NFTs: Key U.S. Legal Considerations for an Emerging Asset Class	197
U.S. Supreme Court Ends Decade-Long Software Copyright Battle: Google Wins	201
Texas and Alabama Securities Regulators File Enforcement Actions Against Online Casino Developer Selling NFTs to Operate Casinos in a Metaverse	202
European Commission Unveils Sweeping Proposals to Regulate the Digital Sector	204
 JONES DAY GLOBAL TEAM AND AUTHORS	 209
United States	208
EMEA	213
Asia/Pacific	216
Latin America	217
Additional Jones Day Authors and Contributors	217

www.finaccelerate.com | finaccelerate@jonesday.com

Jones Day publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our “Contact Us” form, which can be found on our website at www.jonesday.com. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.

© 2023 Jones Day

CHAPTER I INTRODUCTION TO THE FINACCELERATE PROGRAM

FinAccelerations is an unprecedented compilation of legal knowhow about the fintech industry inspired by Jones Day's FinAccelerate program.

FinAccelerations is also available on the FinAccelerate App.

DOWNLOAD HERE:

[Apple App Store](#) | [Google Play](#) | [Web Version](#)

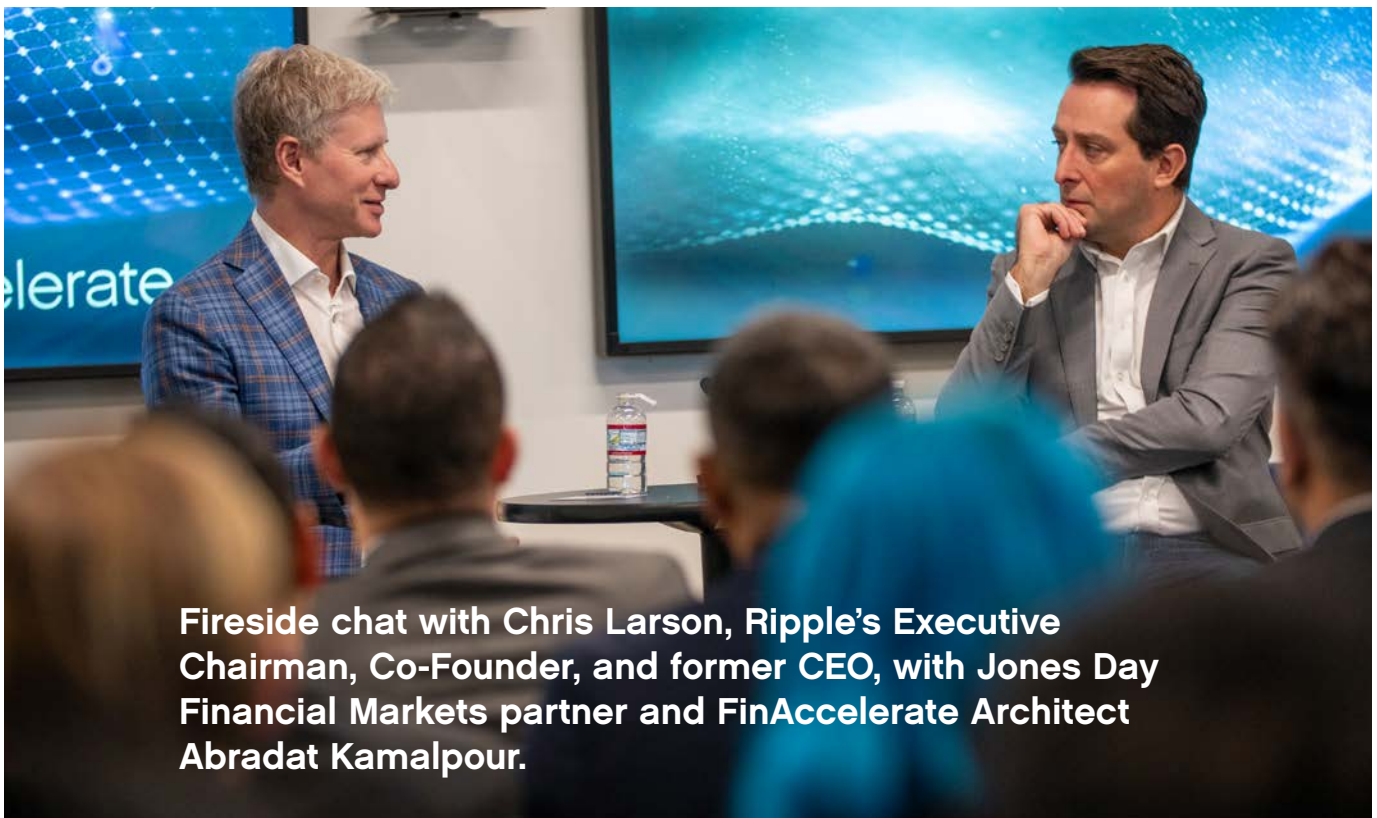
For more information about FinAccelerations or to join the FinAccelerate mailing list, please contact FinAccelerate@jonesday.com.

ABOUT THE FINACCELERATE PROGRAM

FinAccelerate is an intense accelerator program empowered by one of the world's leading and largest law firms, Jones Day. The program covers the fundamental areas of law relevant to innovative fintech companies and enables selected fintech businesses to access leading investors, corporations, financial institutions, and potential JV partners to accelerate their business.

LEADING INDUSTRY INFLUENCERS

Jones Day's inaugural FinAccelerate program kicked off on October 25–27, 2022, in Jones Day's San Francisco and Silicon Valley offices with an overwhelming response from the tech industry.



Fireside chat with Chris Larson, Ripple's Executive Chairman, Co-Founder, and former CEO, with Jones Day Financial Markets partner and FinAccelerate Architect Abradat Kamalpour.



VC & Investors Panel with Matthew Le Merle (Blockchain ColInvestors), Stephen MacKenzie (Koch Disruptive Technologies), Christopher Britton (Lazard), Julian Rooees (Picus Capital Americas), and Ben Hoxie (Vectr Fintech Partners).



Institutions & Innovation panel with Elliot Han (Cantor Fitzgerald), Anthony Bassili (Coinbase Institutional Americas), George Lewin-Smith (Goldman Sachs), Rebecca Macieira-Kaufman (RMK Group), and Kevin Bouey (Wells Fargo Startup Accelerator).

2022 FinAccelerate Cohort and Jones Day Team



Demo Day: Cohort presentations from fintech innovators from around the world—from Paris to Sydney to South Africa.



CHAPTER II

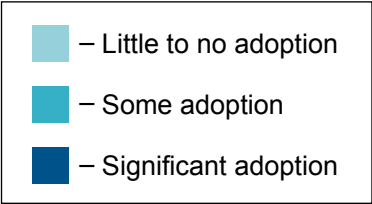
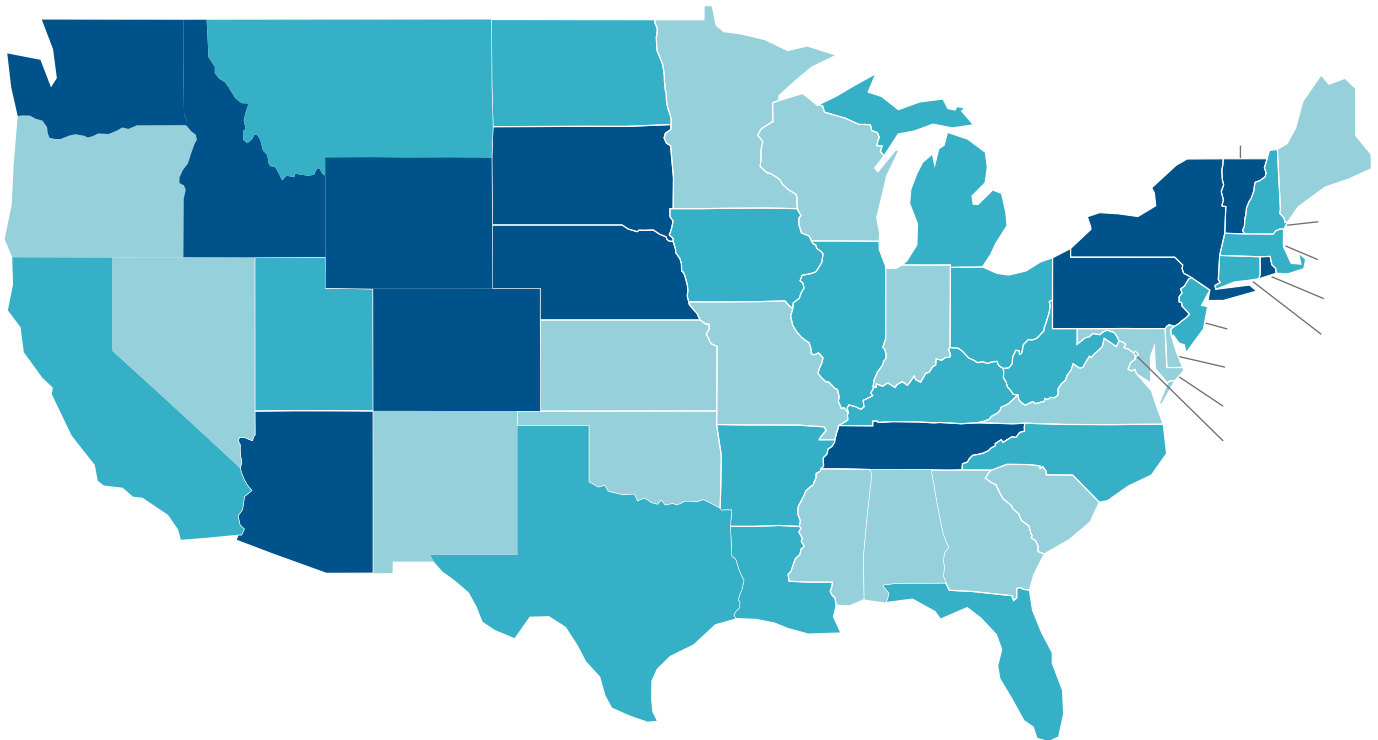
STATE-BY-STATE LEGAL SURVEY OF DIGITAL ASSET REGULATIONS

Jones Day associate Christina Mastrucci Lehn led a group of associates from the Firm's Digital Assets Ecosystem (DAE) Group in preparing this survey.

HEAT MAP OF 50-STATE DIGITAL ASSET REGULATIONS*

Adoption Levels Of Digital Asset-Related Concepts

Click on the state abbreviations below to link to the summary of the state's digital asset regulations.



*As of April 2023

Alabama

Alabama has passed little legislation bearing directly on digital assets, decentralized autonomous organizations (“DAOs”), or other concepts germane to the digital assets ecosystem. However, the state does define “monetary value” under its money transmission law to include virtual currency, without any exclusions or exemptions for certain types of transactions or business models.

The state’s regulators have taken a very aggressive enforcement-first approach notwithstanding the lack of statutory framework. The Alabama Securities Commission (“ASC”) has issued various cease and desist orders against companies working with digital assets for allegedly offering or selling unregistered securities, and reached a settlement with one of those companies in 2022. The ASC also administers the state money transmitter regime.

A bill proposed in April 2023 would, if passed, amend the state’s commercial code to incorporate the amendments to the Uniform Commercial Code (“UCC”) approved by the Uniform Law Commission (“ULC”) in 2022 to address emerging technologies, including the UCC’s newly created Article 12. The new provisions would govern transactions involving “controllable electronic records,” “controllable accounts,” and “controllable payment intangibles”; define “control”; and provide for the perfection of security interests.

Alabama does not have programs with subsidies directly relevant to digital asset-related activities. Nor does Alabama have a regulatory sandbox for fintech or technology-based endeavors. A bill proposed in 2022, if passed, would have exempted virtual currency from state ad valorem taxation; however, the bill died in committee.

Alaska

Alaska has made some progress in modernizing its statutory environment to address digital assets. But Alaska has not addressed smart contracts, DAOs, or other digital asset ecosystems.

A new virtual currency bill introduced in February 2023, though, may broaden Alaska’s regulatory scope over digital assets. The bill, if passed, would amend Alaska’s money transmitter statute to require companies engaging in “virtual currency business activity” to obtain a money transmitter license. In the meantime, effective January 1, 2023, Alaska has incorporated virtual currency into its money transmission regulations. However, the regulations contain exclusions for affinity or rewards programs and online gaming.

Since 2021, Alaskans have been able to buy several cryptocurrencies, including Bitcoin and Ether, at certain ATMs. And the parent company of state airline Ravn Alaska has created a cryptocurrency to reward frequent flyers with a digital token.

Alaska does not offer specific subsidies or exemptions to entities operating in the digital asset space, but the state has no state sales tax.

Arizona

Arizona has made significant changes, and is considering making additional changes, to its statutory environment to address digital assets. For example, Arizona explicitly recognizes the legal effect of smart contracts. Arizona also explicitly recognizes that virtual coins can be securities under its state securities laws. To the extent residents include the sales of virtual currencies and non-fungible tokens (“NFTs”) in their state gross income, Arizona allows residents to make certain deductions from that income. A bill introduced in the state legislature in January 2023 would, if passed, exempt virtual currency from state property taxes. And Arizona prohibits its counties from restricting the running of nodes on blockchain technology in a residence.

Arizona also has the Regulatory Sandbox Program, which allows participants to obtain limited access to Arizona’s market to test financial products or services based on new or emerging technology without first obtaining full state licensure or other authorization that otherwise may be required.

While Arizona does not explicitly define “monetary value” to include virtual currency under its money transmission laws, its definition of “monetary value” could be interpreted broadly enough to encompass virtual currency. If the definition were so interpreted, companies working with virtual currency would likely be required to obtain a money transmitter license in the state. A bill introduced in the state’s legislature in January 2023 would, if passed, make Bitcoin legal tender in the state.

A bill proposed in February 2023 would, if passed, amend the state’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records).



Arkansas

Arkansas law addresses digital assets and blockchain technology in a variety of contexts. For example, Arkansas recognizes smart contracts as valid and enforceable when they meet the statutory definition and relate to a transaction, and signatures secured through blockchain technology are considered electronic signatures.

The Arkansas money transmission statute applies to “virtual currency,” as defined – with certain exclusions. Unless excluded, money transmitters must be licensed and must meet other security and consumer-protection requirements. The Arkansas Securities Department has issued a number of no-action letters clarifying when certain activities involving virtual currency or digital assets may be exempt from money transmitter licensing requirements.

The state’s commercial code covers rights in and control of virtual currency and protects a purchaser who obtains control of virtual currency for value and without notice of adverse claims. A bill proposed in March 2023, if passed, would have amended the state’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records). However, the bill has been withdrawn.

In 2022 and 2023, Arkansas, along with other states, reached major securities law settlements with digital asset financial services companies over alleged offers and sales of unregistered securities in violation of state securities laws. Arkansas state securities statutes do not expressly address digital assets or virtual currency, but Arkansas courts will look at all the facts to decide whether an investment plan or other asset is regulated as a security within the Arkansas Securities Act.

A bill proposed in March 2023 and passed by the state legislature in April 2023, if signed into law, would clarify that digital asset mining businesses may operate in the state if they comply with certain laws, ordinances, and other obligations, and would prevent local governments from adopting regulations discriminating against such businesses.

California

California is home to many large, well-established companies that work with cryptocurrency, as well as an enormous number of blockchain-based businesses, including crypto-based startup companies. The state has so far imposed little state regulation on virtual currency or digital assets, though regulation of the crypto space in California seems poised for additional development.

In May 2022, Governor Gavin Newsom issued an executive order establishing four state agency workstreams to 1) collect stakeholder input, 2) create a crypto regulatory approach that harmonizes between federal and state authorities, 3) incorporate blockchain technologies into state operations, and 4) build research and workforce pipelines. Agencies directly involved include the Governor’s Office of Business and Economic Development and the Department of Financial Protection and Innovation (“DFPI”), among others. In September 2022, Governor Newsom vetoed as premature a digital financial assets bill, citing the state’s ongoing work under his executive order, as well as forthcoming federal actions. The now-vetoed bill would have established a comprehensive licensing and regulatory framework administered by the DFPI. In December 2022, the California Blockchain Working Group issued a report with recommendations regarding the implementation of Governor Newsom’s executive order. In January 2023, the digital financial assets bill was reintroduced in the California Assembly.

The DFPI has issued a series of no-action letters in the last several years stating that certain virtual currency activities and business models did not require a money transmitter license (although warning that its conclusions could change at any time). The DFPI has issued cease and desist orders to, or reached settlements with, several digital asset financial services companies that allegedly offered and sold unregistered securities in violation of state securities laws.

Businesses providing a virtual currency that buyers are allowed or required to use to purchase products are marketplace facilitators under the California sales and use tax statute. A September 2022 amendment to the California health and safety code allows counties to issue certified copies of birth certificates and certain other records by means of verifiable credential using blockchain technology.

A bill proposed in April 2023 would, if passed, amend the state’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records).



Colorado

In recent years, Colorado has made a push to embrace digital assets through passing various laws. Colorado has passed notable acts such as the Colorado Digital Token Act, which exempts cryptocurrencies from some of the state's securities regulations, as well as an act concerning state capital financing that defines "blockchain technology" and multiple terms relating to security tokens. While no law currently recognizes the legal status of DAOs in the state, a DAO may be able to organize as a limited cooperative association in the state to obtain legal status.

The principal state regulator is composed of two divisions of the Colorado Department of Regulatory Agencies. Specifically, the Division of Banking reviews applications and issues licenses for money transmitters, while the Division of Securities reviews notices of intent for Digital Token Act exemption (although no license or registration is involved). Notably, a money transmitter license may be required only if fiat currency is involved; the complete absence of fiat currency from a transmission from one consumer to another is not viewed as a money transmission.

Colorado does not offer tax subsidies or exemptions to blockchain- or digital asset-based companies, and does not have laws or regulations governing smart contracts. However, in 2022, Colorado became the first state to accept cryptocurrency as an additional form of payment for all state taxpayers. A bill proposed in January 2023 would, if passed, amend the state's commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records).

Connecticut

Connecticut has made modest progress toward modernizing its statutory environment to address digital assets, particularly virtual currencies. But while Connecticut has codified a definition of "virtual currency" in its money transmitter statute, Connecticut statutes still do not address smart contracts, DAOs, or other digital asset ecosystems or their treatment under Connecticut's commercial code.

Connecticut law requires entities that engage in "money transmission," which is defined broadly enough to encompass some virtual currencies, to register and obtain a money transmitter license. In addition, Connecticut's Department of Banking, the principal state regulator of money transmitters, has clarified that some digital asset companies may not fall within the statutory language. This clarification is by means of an advisory and a series of opinion letters addressing whether certain actions in the digital assets space require licensure (e.g., certain virtual exchange activity or virtual currency ATMs).

Connecticut does not offer specific subsidies or exemptions to entities operating in the digital asset space; however, the state administration has issued a sizeable grant to a digital asset company relocating to the state, contingent on the company creating and retaining new jobs.

Delaware

Delaware has made some progress toward modernizing its regulatory environment to address digital assets, but much of this progress has been piecemeal through relevant Delaware Superior Court cases in which concepts have been defined and, in certain circumstances, a determination of whether a digital asset qualifies as a security has been reached.

Delaware's money transmission statute does not explicitly include or exclude virtual currency, and the state's Office of the State Bank Commissioner has not provided clear interpretative guidance on whether virtual currency falls under the statute. Delaware was the first state to allow corporations to maintain corporate records using blockchain technology.

Neither digital assets nor blockchain technologies are incorporated into Delaware's commercial code. In 2016, Delaware launched a Blockchain Initiative to create a "smart UCC," but nothing was ever codified, and it has since been dropped as a priority under the current state administration. Delaware does not currently offer any digital asset-specific subsidies or tax advantages for entities operating in the digital asset space.



District of Columbia

The District of Columbia (“D.C.”) has made modest progress toward modernizing its statutory environment to address digital assets. While D.C. has defined “virtual currency” in its Revised Uniform Unclaimed Property Act, it has not yet addressed smart contracts, DAOs, or other digital asset-related concepts in its statutes.

The D.C. Department of Insurance, Securities and Banking (“DISB”) has issued guidance stating that cryptocurrency interest-bearing accounts offered by digital asset financial services companies in D.C. constitute securities subject to registration and other securities law requirements. The DISB has also issued guidance stating that certain transactions involving Bitcoin and virtual currencies constitute money transmission, while others do not.

A bill proposed in January 2023 would, if passed, amend D.C.’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records). A bill proposed in 2021, if passed, would have created a regulatory sandbox program for innovative financial products and services; however, the bill has been postponed indefinitely.

Florida

Florida recently passed a law regarding digital assets and virtual currencies that went into effect on January 1, 2023. Among other advances, the law amends Florida’s money services business statute to define “virtual currency” and address transactions involving “virtual currency.”

Florida’s money services business statute is enforced by the Florida Office of Financial Regulation (“OFR”) and, through the end of 2022, did not explicitly address virtual currency. Before the new law went into effect, court decisions had classified Bitcoin as both “monetary value” and a “payment instrument” under the statute. Under the new law, virtual currency is incorporated into the definition of “money transmitter,” but the definition of “money transmitter” is also limited to “acting as an intermediary to transmit currency, monetary value, a payment instrument, or virtual currency from one person to another location or person.” The new law also clarifies that this definition “includes only an intermediary that has the ability to unilaterally execute or indefinitely prevent a transaction.”

Florida does not recognize DAOs, and provides no explicit framework for tax subsidies or exemptions particular to digital assets. Neither digital assets nor blockchain technologies are incorporated into Florida’s commercial code. Florida, however, has a regulatory sandbox for companies testing “innovative financial products” that will grant a license to exempt those companies from certain provisions of Florida’s Money Services Business Act and Consumer Finance Act.

In December 2022, the OFR released guidance discussing how cryptocurrencies and certain transactions involving cryptocurrencies may be deemed “securities” for purposes of Florida’s securities laws, and outlining how Florida’s securities laws may apply to different participants in the digital securities market. A bill proposed in March 2023 would, if passed, prohibit the use of a federally adopted central bank digital currency (“CBDC”) as money within Florida’s commercial code.

Georgia

Georgia is still in the early stages of updating its laws to incorporate concepts related to digital assets. The primary means by which Georgia can regulate companies working with digital assets is in the context of money transmission and the sale of payment instruments. In these contexts, Georgia defines “virtual currency” as a type of “monetary value.” In addition, the Georgia Department of Banking and Finance has interpreted the definitions of “money transmitters” and “seller of payment instruments” to include some forms of virtual currency transactions. Thus, companies working with virtual currency in the state likely need to obtain a money transmitter license and/or a license for the sale of payment instruments.

While Georgia’s securities laws do not explicitly address digital assets, in 2021 a Georgia federal court concluded that a certain type of cryptocurrency was a security under the state’s securities laws. It remains to be seen whether Georgia state courts and regulators will follow suit and also conclude that certain digital assets can be securities in Georgia.

Georgia’s Department of Banking and Finance (responsible for the enforcing the state’s laws on money transmission and sale of payment instruments) and Georgia’s Secretary of State (responsible for enforcing the state’s securities laws) are the principal state regulators that could have enforcement authority over companies working with digital assets in the state.



Guam

Guam has not taken any steps to modernize its statutory environment to address digital assets. In fact, there is no current legislation pending that involves cryptocurrencies or definitions for any related technology.

The Guam Department of Revenue and Taxation provides that “no person shall engage in the business of selling foreign currency notes or engage in the business of receiving money for the purpose of transmitting the same or its equivalent to foreign countries without first obtaining a license from the Commissioner.” While it remains to be seen how this provision may be interpreted to affect digital assets, there does not seem to be any clear applicability because key terms such as “money” and “currency” remain undefined.

Guam does not offer tax subsidies or exemptions to blockchain- or digital asset-based companies.

Hawaii

Hawaii’s inability to pass blockchain-based legislation has resulted in it being one of the least developed and most difficult states in the country for crypto transactions. The Hawaii Department of Commerce and Consumer Affairs, Division of Financial Institutions has interpreted the state’s money transmission laws as applying to digital currency companies. In 2022, the state failed to pass a bill establishing separate digital asset licensing requirements (as opposed to incorporating digital assets into the state’s money transmitter laws), thereby requiring digital asset businesses to continue looking to Hawaii’s money transmitter licensing requirements. However, the bill was reintroduced in the Hawaii Legislature in January 2023. And, Hawaii has extended its regulatory sandbox program for digital currency until June 30, 2024.

A bill proposed in January 2023 would, if passed, amend the state’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records).

Hawaii does not recognize DAOs, smart contracts, or other common blockchain-based concepts, and currently has no specific digital asset-related energy; environmental, social, and governance (“ESG”); or tax subsidy initiatives.

Idaho

Idaho’s recent passage of the Digital Assets Act provides a robust framework and in-depth definitions for many cryptocurrency-related terms. The Idaho Department of Finance has clarified that virtual/digital currency exchangers accepting legal tender for later delivery to a third party in association with the purchase of a virtual currency must be licensed as money transmitters. The Department of Finance is Idaho’s main regulator, having statutory authority over money transmission licensing and securities regulation.

By way of its Digital Assets Act, Idaho made digital assets “intangible personal property” under its commercial code. The Act also specifies that digital assets and virtual currency as property can be used as collateral to create a perfected security interest. Additionally, virtual currency is not a security under the Act.

A bill proposed in 2021, if passed, would have implemented a sandbox environment for select, innovative financial products. Another bill proposed in 2021, if passed, would have allowed banks to provide digital asset custodial services in certain circumstances. However, both bills died in committee.



Illinois

In the context of digital assets, Illinois statutes have focused on smart contracts and the use of blockchain records. Illinois has enacted a detailed blockchain technology statute that defines and recognizes the legal validity of smart contracts and blockchain records, with certain restrictions. The statute also forbids local governments from imposing taxes, fees, or licensing requirements on blockchain or smart contract use.

In regulatory guidance on digital currency, the Illinois Department of Financial and Professional Regulation (“IDFPR”) has stated that digital currency is distinct from money; thus, under the guidance, persons who transmit solely digital currencies are not be required to obtain a money transmitter license. However, persons engaging in a transaction that involves both digital currencies and “money” are advised to ask the IDFPR whether a license is required. In its guidance, the IDFPR provided examples of digital currency activity that would or would not require licensing.

In February 2023, the IDFPR announced the proposed Fintech-Digital Asset Bill, which, if passed, would require digital asset exchanges and other digital asset businesses to obtain a license from the IDFPR to operate in Illinois. The bill would also establish robust customer protections, including investment disclosures, customer asset safeguards, and customer service standards, and allow for the creation of trust companies for the special purpose of acting as fiduciaries to safeguard customers’ digital assets. Another bill proposed in February 2023 would, if passed, authorize charters for a “special purpose trust company,” and allow the IDFPR to adopt rules, opinions, or interpretive letters regarding the provision by such companies of custodial services for digital assets. Yet another bill proposed in February 2023 would, if passed, exempt certain cryptocurrency mining centers from various state and local taxes.

An Illinois blockchain business development statute tasks the Department of Commerce and Economic Opportunity with blockchain and financial technology promotion.

Indiana

Indiana has recently made its initial forays into defining foundational digital asset-related terms like “blockchain technology” and “virtual currency,” including in the gaming and gambling industries. Indiana recently revised its Unclaimed Property Act to specifically incorporate virtual currencies.

In 2022, Indiana added a new provision to its commercial code, modeled on a draft of the UCC’s newly created Article 12 (relating to controllable electronic records). In April 2023, a bill was introduced that, if passed, would further amend Indiana’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12).

The Indiana Department of Financial Institutions generally recognizes that a money transmitter license is not required for a fiat or virtual currency exchange, so as long as the consumer is strictly buying or selling the currency and the consumer does not have the ability to send fiat currency to another consumer.

In 2023, the Indiana Securities Division entered into a settlement with a digital asset financial services company that allegedly offered and sold unregistered securities in violation of state securities laws, indicating that the Division considers at least some digital assets to be securities under the state’s securities laws.

Indiana has no statutory structure regarding tax subsidies or exemptions to blockchain- or digital asset-based companies, but the Indiana Economic Development Corporation has invested in bringing blockchain jobs to the state with incentive-based tax credits.



Iowa

Iowa has made and is continuing to make important changes to its laws to address digital assets. In 2022, Iowa enacted a law recognizing the legal effect of smart contracts and contracts based on distributed ledger technology. Also in 2022, Iowa amended its commercial code, modeled on a draft of the UCC's newly created Article 12 (relating to controllable electronic records). A bill proposed in March 2023 would, if passed, further amend the state's commercial code as it relates to controllable electronic records. The bill would also amend the definition of "digital asset" by eliminating exceptions recognized by the UCC, including electronic records evidencing chattel paper, and provide that a digital asset is classified simply as personal property rather than intangible personal property.

While Iowa's Uniform Money Services Act does not explicitly address virtual currencies, its definition of "monetary value" could be interpreted broadly enough to encompass virtual currency. If so interpreted, companies working with virtual currency in Iowa would likely be required to obtain a money transmitter license in the state.

While Iowa's securities laws do not explicitly address digital assets either, a 2022 settlement between the Iowa Insurance Division and a digital asset financial services company for alleged violations of state securities laws indicates that the Division considers at least some digital assets to be securities under the state's securities laws.

Iowa's Division of Banking (responsible for enforcing the state's money transmission laws) and the Iowa Insurance Division (responsible for enforcing the state's securities laws) are the principal state regulators that could have enforcement authority over companies working with digital assets in the state.

Kansas

Kansas' Office of the State Bank Commissioner ("OSBC") has been updating its guidance on virtual currencies since 2014 through its interpretations of the Kansas Money Transmitter Act ("KMTA"). Per OSBC guidance, the KMTA does not apply to entities engaged solely in the transmission of decentralized cryptocurrencies (such as Bitcoin). However, should the transmission of virtual currency include the involvement of sovereign currency in a transaction, it may be considered money transmission depending on how such transaction is organized. The guidance provides examples of certain transactions that are, and certain transactions that are not, considered money transmission under the KMTA.

Kansas has also issued an official notice on sales tax requirements for digital currency under the Retailers' Sales and Compensating Tax Acts, requiring sellers to collect and remit sales tax for tangible personal property or services

paid by digital currency. However, transaction fees for digital currency exchange are not subject to state sales tax.

Kansas allows limited liability companies ("LLCs") to maintain their records using electronic networks or databases, including distributed electronic networks or databases, if such form is capable of conversion into written form within a reasonable time.

Kentucky

Kentucky has enacted a legislative framework that defines a wide range of blockchain- and digital asset-related concepts, though it does not incorporate digital assets into its commercial code. The state offers numerous tax incentives and subsidies surrounding energy-related businesses that explicitly mention cryptocurrency facilities, mining facilities, and commercial mining equipment.

The Kentucky Department of Financial Institutions ("DFI") does not impose any licensing or registration requirements specifically directed at businesses working with digital assets or blockchain technologies. While Kentucky does not explicitly define "money" to include virtual currency under its money transmission laws, its definition of "monetary value" could be interpreted broadly enough to encompass virtual currency. If the definition were so interpreted, companies working with virtual currency would likely be required to obtain a money transmitter license in the state.

In 2021 and 2022, the DFI issued cease and desist orders against two digital asset financial services companies for allegedly offering and selling unregistered securities in violation of state securities laws, indicating that the DFI considers at least some digital assets to be securities under the state's securities laws. The DFI settled with one of those companies in 2022.

A bill proposed in 2022, if passed, would have established a regulatory sandbox program for insurance companies working in the crypto-sphere. A bill proposed in February 2023, if passed, would have amended the state's commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records). However, both bills died in committee.

Another bill proposed in 2022, if passed, would have required developers and sellers of certain open blockchain tokens to file a notice of intent with and pay a filing fee to the state, and permit state financial institutions to provide custodial services of customer currency and digital assets. Yet another bill proposed in 2022, if passed, would have established a charter for special purpose depository institutions and allow them to manage accounts in virtual currency or hold other digital assets. However, it appears no action has been taken on these bills since their introduction.



Louisiana

Louisiana regulates virtual currency primarily through its Virtual Currency Businesses Act (“VCBA”), which imposes a licensing regime specific to virtual currency businesses and overseen by the state’s Office of Financial Institutions (“OFI”). The VCBA prohibits one from engaging in “virtual currency business activity,” or holding oneself out “as being able to engage in virtual currency business activity,” “with or on behalf of a resident” unless one is licensed, registered, or exempted under the act. The VCBA requires license applicants to submit detailed information and documentation, including providing comprehensive information about the applicants’ proposed virtual currency business activities, other licenses and registrations, financial condition, and legal status. Persons with a smaller volume of virtual currency business activity may register with the OFI rather than obtain a license, if they meet the statutory registration requirements.

The OFI began accepting license applications under the VCBA in January 2023. Completed applications for licensure and notices of registration submitted on or before April 1, 2023 will be approved, conditionally approved, or denied on or before June 30, 2023. After July 1, 2023, the licensing requirement goes into effect—that is, initial and renewal applications must be submitted in accordance with the VCBA and the Louisiana Administrative Code.

Louisiana has expressly authorized financial institutions and trust companies to engage in virtual currency custody services, provided they satisfy detailed statutory requirements to ensure that there are adequate protocols in place to effectively manage risks and comply with applicable laws.

A bill proposed in March 2023, if passed, would have amended the state’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records). However, the bill was withdrawn shortly after its introduction.

Maine

Maine has made modest progress toward modernizing its statutory environment to address digital assets. Maine’s money transmission statute defines “money transmission” to include receiving virtual currencies for transmission, but contains exclusions related to affinity or rewards programs and online gaming.

Otherwise, there are no registration requirements that specifically target businesses working with digital assets or blockchain technologies, and Maine statutes still do not address smart contracts or DAOs. However, in 2022, Maine’s Office of Securities settled with a digital asset financial services company over alleged violations of state securities

laws, indicating that the Office considers at least some digital assets to be securities.

Maine does not currently offer any digital asset-specific subsidies or tax advantages for entities operating in the space. A bill proposed in March 2023 would, if passed, authorize state special purpose depository institutions for digital assets. A broader blockchain and cryptocurrency-related bill was proposed, but did not pass, in 2021.

Maryland

Maryland has made limited progress toward updating its laws to incorporate concepts related to digital assets. For example, Maryland law authorizes certain corporate communications, consents, and requests to be made by means of a “distributed electronic network or database.” However, Maryland’s laws do not yet address many concepts related to digital assets.

The primary means by which Maryland can regulate companies working with digital assets is in the context of money transmission. Maryland’s Money Transmission Act incorporates the concept of “other value that substitutes for currency.” Virtual currency could be covered by Maryland’s money transmission laws under a reasonable reading of this provision. In addition, Maryland’s definition of “monetary value” in the context of money transmission could be interpreted broadly enough to encompass virtual currency. Therefore, companies working with virtual currency in Maryland are likely required to obtain a money transmitter license in the state.

In 2022 and 2023, the Securities Commissioner of Maryland reached major settlements with digital asset financial services companies over alleged offers and sales of unregistered securities in violation of state securities laws, indicating that the Commissioner considers at least some digital assets to be securities under the state’s securities laws.

In 2022, Maryland proposed a bill that, if passed, would have established the Decentralized Financial Regulatory Sandbox Program. This program would have facilitated limited access to the state’s financial market to test products and services that use new or emerging technology, including blockchain technology, without having to obtain a license or other authorization. However, the bill died in chamber.



Massachusetts

Massachusetts has thus far focused on securities enforcement, money transmission, and taxation in the digital asset space.

Massachusetts' securities laws do not explicitly mention digital assets. However, the Massachusetts Securities Division has exercised its enforcement authority over several cryptocurrency companies alleged to have engaged in the unregistered sale of securities, indicating that the Division considers at least some digital assets to be securities under the state's securities laws.

A Massachusetts statute requires licenses for businesses engaged in the transmission of money to foreign countries. Massachusetts does not have a domestic money transmission statute. Addressing various models for cryptocurrency businesses, the Division of Banks has opined that they do not fall under the foreign money transmission statute and therefore do not require foreign money transmitter licenses. The Division expressly advises that different facts could lead to different conclusions.

The Massachusetts sales and use tax statute covers marketplace facilitators that provide a virtual currency that buyers are allowed or required to use to purchase tangible personal property or services, but excludes mere payment processors.

A bill proposed in January 2023 would, if passed, amend the state's commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records).

Michigan

Michigan has made some progress toward modernizing its statutory environment to address digital assets. While Michigan has codified some definitions related to digital assets and blockchain technology, Michigan statutes still do not address smart contracts, DAOs, or other digital asset ecosystems, or their treatment under the state's commercial code.

Michigan's money transmission statute does not explicitly include or exclude virtual currency, and the state's Department of Insurance and Financial Services ("DIFS") has not provided clear interpretative guidance on whether virtual currency falls under the statute. The DIFS has stated that "holding funds in an e-wallet" is an example of money transmission under the statute, but does not define "e-wallet."

A bill proposed in 2022, if passed, would have created a Blockchain and Cryptocurrency Commission within the Michigan Department of Treasury. The Commission would have been charged with investigating blockchain and cryptocurrency to develop a master plan of recommendations for fostering an expansion of blockchain technology and the cryptocurrency industry in the state. However, the bill died in committee.

Michigan does not currently offer any digital asset-specific subsidies or tax advantages for entities operating in the space. However, the August 2022 Michigan Department of Treasury Update discusses the state income tax treatment of digital currencies and cryptocurrencies.

Minnesota

Minnesota is still in the initial stages of incorporating digital assets into its laws and regulations. The Minnesota Department of Commerce, the state's regulator of money transmitters, does not consider virtual currency to be "money" for purposes of the Minnesota Money Transmitter Act. Whether the Department requires a license for transmitters of virtual currency depends on whether and how exactly fiat currency is involved in a transaction. The Department has stated that certain exchanges of virtual currency would require a money transmitter license, while others would not.

The Department of Commerce, also responsible for enforcing the state's securities laws, has stated in the enforcement context that certain digital assets qualify as "securities" under the state's securities laws. In 2022, the Minnesota Department of Revenue issued guidance stating that NFTs are subject to sales and use tax when the underlying product (goods or services) is taxable in Minnesota.

A bill proposed in 2022, if passed, would have allowed for the use of electronic networks and databases to record stock ownership and other records. Another bill proposed in 2022, if passed, would have allowed certificate tokens to be issued in place of shares of stock. However, it appears no action has been taken on these bills since their introduction.



Mississippi

The Mississippi legislature has begun to consider bills addressing virtual currency and digital assets, but the state's existing statutes and regulation remain largely silent on those subjects. In 2022, the Securities Division of Mississippi's Secretary of State joined other state regulators in a settlement involving cryptocurrency activity alleged to be the sale of unregistered securities in violation of state securities laws.

Mississippi's money transmitter statute does not expressly address virtual currency, but applies to the business of receiving "monetary value," a term broadly defined as a medium of exchange, whether or not redeemable in money. The Consumer Finance Division of the Mississippi Department of Banking and Consumer Finance is responsible for the licensing and regulatory supervision of money transmitters.

In the 2022 legislative session, a number of bills were introduced in the Mississippi legislature with express provisions addressing virtual currency, digital assets, blockchain tokens, digital securities, and the like, in the context of Mississippi's money transmitter and securities laws. One pair of bills also would have authorized banks to provide custodial services for digital asset property. However, none of these bills emerged from committee.

A bill proposed in January 2023, if passed, would have created a state digital asset mining act and provided an exemption for the buying, selling, issuing, receiving, or taking custody of virtual currency under the state's money transmitter statute. Another bill proposed in January 2023, if passed, would have provided certain exemptions regarding blockchain tokens from the state's securities laws. However, both bills died in committee.

Missouri

The Missouri legislature recently made its first venture into defining foundational digital asset-related terms such as "cryptocurrency" and "digital asset."

While Missouri's securities law does not explicitly include digital assets in its definition of "security," some administrative decisions have treated certain digital assets as non-exempt securities under state law. In addition, Missouri's money transmission statute does not explicitly include or exclude virtual currency, and the state's Division of Finance has not provided clear interpretative guidance on whether virtual currency falls under the statute. However, some in-state virtual currency exchanges maintain Missouri Sale of Checks licenses.

A bill proposed in January 2023 would, if passed, preclude the state and political subdivisions from prohibiting the running of a node or series of nodes for the purpose of home mining. The bill would also prohibit discriminatory electric rates for digital asset mining businesses; exempt virtual currency from taxation for state, county, or local purposes; and create registration requirements for developers or sellers of blockchain tokens. A bill proposed in February 2023 would, if passed, amend the state's commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records).

A bill proposed in 2022, if passed, would have created a state framework categorizing and regulating digital assets, including definitions for "virtual currencies," "digital securities," and "open blockchain tokens." If passed, that bill also would have exempted cryptocurrencies from property tax. However, the bill died in committee.



Montana

The Montana legislature has broached the concept of cryptocurrency by defining “utility tokens” and exempting them from state securities laws, subject to certain prerequisites. However, the state has not yet defined other blockchain-related terms necessary to describe the concept, such as “digital ledger,” or most other blockchain- or digital asset-related terminology. The Montana Code defines “digital currency” in the money laundering context and clarifies smart contracts may not be denied legal effect or enforceability solely due to their electronic form.

The Montana Division of Banking and the Securities Department at the Office of the Montana State Auditor regulate specified in-state monetary activities. The state is notable for being the only remaining state not to have enacted a money transmission statute requiring any separate licensure apart from registration as a business with the Montana Secretary of State.

Montana was also the first state to take a stake in a Bitcoin mining operation, drawn from a public aid program aimed at supporting long-term job growth. Further, Montana amended its Electronic Contributions Act to expressly require the reporting of political contributions made “through a payment gateway” – including Bitcoin.

Montana does not recognize DAOs, and currently has no special digital asset-related energy, ESG, or tax subsidy initiatives. A bill proposed in January 2023 would, if passed, prohibit discriminatory digital asset mining utility rates, local government powers related to digital asset mining, and taxation on the use of cryptocurrency as a payment method. A bill proposed in February 2023 would, if passed, amend the state’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records). Montana’s securities registration exemption for utility tokens expires September 30, 2023.

Nebraska

Nebraska is at the forefront of updating its laws to address digital assets. In particular, Nebraska allows for the formation of a “digital asset depository institution,” a unique type of state-chartered entity that is authorized, among other things, to offer certain digital asset custody services. Similarly, existing banks in Nebraska may create divisions focused on digital assets. Nebraska also recently amended its commercial code, modeled on a draft of the UCC’s newly created Article 12 (relating to controllable electronic records).

While the Nebraska Money Transmitters Act does not explicitly address virtual currencies, its definitions of “monetary value” and “stored value” could be interpreted broadly enough to encompass virtual currency. If so interpreted, companies working with virtual currency in Nebraska would likely be required to obtain a money transmitter license in the state. However, the Act does exempt digital asset depository institutions.

While Nebraska’s securities laws do not explicitly address digital assets, a 2022 settlement between the Nebraska Department of Banking and Finance and a digital asset financial services company for alleged violations of state securities laws indicates that the Department considers at least some digital assets to be securities under the state’s securities laws.

A bill proposed in January 2023 would, if passed, further amend the state’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12).



Nevada

Nevada has made significant progress toward modernizing its laws to incorporate digital asset- and blockchain-based concepts. Nevada law recognizes a blockchain as an electronic record. It also prohibits government agencies from refusing to accept a record certified through blockchain from another agency solely because the copy is in electronic form, and provides that a person who uses a public blockchain to secure that person's information does not automatically relinquish ownership of that information. The state also recognizes the legal effect of blockchain-based signatures and contracts.

Nevada exempts virtual currency from state property taxes. The state also prohibits certain local governing bodies from imposing taxes or fees for the use of a blockchain by any person, and from requiring certificates, licenses, or permits to use a blockchain.

The Nevada Financial Institutions Division ("NFID") administers and oversees licensing requirements for financial institutions and those engaged in money transmission. The NFID will determine if digital asset-based companies require money transmission licensure on a case-by-case basis.

Nevada has a regulatory sandbox program that provides temporary exemptions for innovative financial products or services from statutory and regulatory provisions that would otherwise apply. However, a bill proposed in March 2023 would, if passed, require persons engaged in certain business activity involving digital financial assets to obtain a license from the NFID. Another bill proposed in March 2023 would, if passed, require a virtual currency business to pay an annual assessment and provide a written disclosure containing certain information to the NFID.

Yet another bill proposed in March 2023 would, if passed, amend the state's commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records).

New Hampshire

New Hampshire has made extensive progress modernizing the state's treatment of digital assets under existing regulatory schemes. In 2022, New Hampshire passed legislation that amended the state's commercial code, modeled on a draft of the UCC's newly created Article 12 (relating to controllable electronic records). New Hampshire also excludes open blockchain tokens from the state's securities laws under certain circumstances, and exempts certain virtual currency transactions from being considered "money transmission" requiring licensure under state law.

A bill proposed in 2022, if passed, would have permitted a bank to provide custodial services for digital assets; however, the bill was referred for an interim study that ultimately resulted in a 17-0 "Not Recommended for Future Legislation" designation in October 2022. Another bill proposed in 2022, if passed, would have established special purpose depository institutions; however, the bill died in chamber.

The Department of Banking is the principal state regulator for those virtual currency exchanges that do not qualify under a money transmitter license exemption. While New Hampshire has made recent progress within its statutes to account for the evolving digital asset ecosystem, it does not currently offer any digital asset-specific subsidies or tax advantages for entities operating in the space.

In January 2023, the New Hampshire Bureau of Securities Regulation issued cease and desist orders against two digital asset financial services companies for allegedly offering and selling unregistered securities, and for allegedly misrepresenting or failing to disclose material information in connection with those securities, in violation of state securities laws, indicating that the Bureau considers at least some digital assets to be securities under the state's securities laws.

A bill proposed in January 2023 would, if passed, further amend the state's commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12). Another bill proposed in January 2023 would, if passed, establish decentralized autonomous organizations as legal entities within the state.



New Jersey

New Jersey has taken significant steps toward modernizing its statutory environment to address digital assets. Two major bills are pending before the state's legislature—the Digital Asset and Blockchain Technology Act (“DABTA”) and the Virtual Currency and Blockchain Regulation Act (“VCBRA”). Both seek to define digital assets and virtual currencies, and the VCBRA goes much further to include definitions for “blockchain,” “smart contract,” and “decentralized autonomous organization,” among many other terms.

New Jersey's money transmission statute does not explicitly include or exclude virtual currency, and the state's Department of Banking and Insurance has not provided clear interpretative guidance on whether virtual currency falls under the statute. The DABTA and VCBRA would regulate digital asset business activity more generally. The VCBRA, though, would exempt virtual currency from state laws governing money transmitters, and seemingly incentivize the use of virtual currency services through tax breaks.

The New Jersey Bureau of Securities has also been active, issuing several cease and desist orders to cryptocurrency companies for allegedly failing to register securities with the Bureau. One of those cease and desist orders led to a 2022 settlement with a digital asset financial services company.

New Jersey allows corporations to keep books and records “on an electronic network,” including a distributed electronic network or a database that utilizes blockchain technology. Guidance from the New Jersey Division of Taxation states that the purchase of convertible virtual currency for investment purposes is not subject to the state's sales tax, but is subject to sales and use tax when used as payment for taxable goods or services.

New Mexico

New Mexico is still in the early innings of modernizing its statutory environment to address digital assets. In March 2023, New Mexico enacted a law amending the state's commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records). And a bill proposed in January 2023 would, if passed, establish a regulatory sandbox in the state for applicants that provide an innovative use of blockchain technology. However, state law does not yet address smart contracts, DAOs, wallets, and other common digital asset concepts.

The state Financial Institutions Division has issued guidance stating that entities engaged in the business of exchanging virtual currency for money or any other form of monetary value or stored value to persons located in New Mexico are money transmitters and must be licensed as such in the state.

New Mexico does not offer tax subsidies or exemptions to blockchain- or digital asset-based companies.

New York

New York financial authorities have instituted a stringent and rigorous licensing and regulatory program for virtual currency business activity. The state's Attorney General has also actively enforced securities laws in the digital asset and cryptocurrency space.

In June 2015, New York's Department of Financial Services (“DFS”) issued virtual currency regulation under the New York Financial Services Law. To conduct virtual currency business activity, entities can either apply for a license, known as a BitLicense, or for a charter under the New York Banking Law (e.g., a limited purpose trust charter) with approval to conduct virtual currency business. A limited purpose trust company can exercise fiduciary powers, while a BitLicensee cannot. In addition, a limited purpose trust company can engage in money transmission in New York without obtaining a separate money transmitter license. The DFS also regulates money transmitter licenses under New York law.

The DFS has granted a number of virtual currency licenses and charters. The DFS also issues frequent guidance on virtual currency-related topics. In September 2022, for example, the DFS issued industry guidance on Ethereum's upcoming change to a “proof of stake” consensus mechanism. And in January 2023, the DFS issued guidance on standards and practices that, in the DFS' view, will help ensure that virtual currency entities that act as custodians provide a high level of customer protection with respect to asset custody.

The New York Attorney General has brought securities enforcement actions against several companies working with digital assets. In 2022 and 2023, New York, along with other states, reached major settlements with digital asset financial services companies that had allegedly offered and sold unregistered securities in violation of state securities laws.

New York recently passed legislation imposing a two-year moratorium on mining operations using proof-of-work to validate blockchain transactions and subjecting them to environmental review.



North Carolina

North Carolina defines terms related to digital assets in various state laws, most notably the Money Transmitters Act. The Act defines “money transmission” to include “maintaining control of virtual currency on behalf of others,” but does exclude certain transactions conducted in virtual currency. The state’s Office of the Commissioner of Banks has issued guidance stating that certain activities and business models generally are regulated by the Money Transmitters Act, while others are not.

North Carolina has a regulatory sandbox program for makers of financial, insurance, or emerging technology products or services that include an innovation component or element, such as one based on blockchain technology.

North Carolina has a blanket sales and use tax exemption for electricity, which could be attractive to cryptocurrency miners. However, the exemption provides that the primary activity at the facility benefitting from the tax should be manufacturing. A North Carolina county is currently considering imposing a one-year cryptocurrency mining ban.

North Dakota

North Dakota has made moderate progress toward updating and providing guidance on its laws to address digital assets. For example, North Dakota’s Department of Financial Institutions (“DFI”) has published regulatory guidance stating that a bank may offer virtual currency custody services as long as the bank has adequate protocols in place to effectively manage the associated risks and comply with applicable law. The guidance also provides that state-chartered banks can take virtual currency as collateral for loans. Additional guidance from the DFI provides that credit unions have no explicit authority under North Dakota statute to provide members custody services with regards to crypto assets, and that any crypto custody services provided to a credit union member would need to be provided through a third party with these authorized powers.

The DFI has also issued guidance stating that it does not consider the control or transmission of virtual currency to fall under the scope of the state’s money transmission laws. However, a company working with virtual currency that conducts certain transfers of fiat currency would still be required to obtain a money transmitter license in the state. In March 2023, North Dakota passed a law amending its money transmission statute to require those engaging in “virtual-currency business activity” to be licensed as money transmitters, with certain exclusions and exemptions. The law is effective August 1, 2023.

While North Dakota’s securities laws do not explicitly address digital assets, in 2018 the North Dakota Securities Department issued cease and desist orders against companies promoting an initial coin offering (“ICO”), and in 2022 the Department settled with a digital asset financial services company over alleged offers and sales of unregistered securities in violation of state securities laws, indicating that the Department considers at least some digital assets to be securities under the state’s securities laws.

In March 2023, North Dakota passed a law amending the state’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records). North Dakota law also recognizes the legal effect of smart contracts.

Ohio

While a statutory regime addressing or defining digital asset- or blockchain-related concepts does not currently exist in Ohio, the Department of Commerce, the state’s main financial regulator, has defined several well-known terms such as “smart contracts” and “DeFi” in the context of investor advisories. The Department of Commerce also advises that virtual currencies like Bitcoin are subject to the Ohio Money Transmitters Act, which includes special requirements for applicants engaging in the transaction of virtual currency.

A bill proposed in 2022, if passed, would have created a substantial framework for defining and regulating digital assets. Specifically, the bill would have authorized financial institutions including banks, credit unions, and special purpose depository institutions to provide custodial services for customers’ digital assets; provided a framework for the legal formation of DAOs; and classified a “digital consumer asset” as intangible personal property and treat it as a general intangible under the secured transactions provisions of Ohio’s commercial code. However, the bill died in committee.



Oklahoma

Oklahoma has yet to pass legislation bearing directly on digital assets, but multiple attempts with comparatively broad support suggest state legislation may not be far off. Legislation proposed in 2022 (but which did not pass) would have provided important definitions of key terms, such as “blockchain,” “distributed ledger technology,” and “smart contracts.”

The state’s money transmission statute does not explicitly include or exclude virtual currency, and the Oklahoma Banking Department has not provided clear interpretative guidance on whether virtual currency falls under the statute.

In 2022, the Oklahoma Securities Commission issued cease and desist orders against two digital asset financial services companies for allegedly offering and selling unregistered securities in violation of state securities laws, indicating that the Commission considers at least some digital assets to be securities under the state’s securities laws.

A bill proposed in February 2023 would, if passed, exempt certain uses of machinery, equipment, and electricity for commercial mining of digital assets from the state’s sales tax. Another bill proposed in February 2023 would, if passed, amend the state’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records).

Oregon

Oregon has been slow to adopt blockchain-based concepts into the state’s legal and regulatory framework. However, the Oregon Division of Financial Regulation has issued guidance stating that those who are selling or issuing virtual currencies or engaged in the business of operating virtual currency exchange in the state must be licensed as money transmitters.

Oregon does not recognize DAOs, smart contracts, or other common blockchain-based concepts. A bill proposed in January 2023 would, if passed, require “high energy use facilities,” including facilities with the primary purpose of “producing or processing cryptocurrency or carrying out other operations related to cryptocurrency,” to limit their carbon emissions in the state.

Pennsylvania

Pennsylvania has made some, and considered making additional, changes to its laws to address digital assets. For example, the Pennsylvania Department of Revenue has added NFTs to the state’s list of items subject to sales and use taxes. In addition, a bill proposed in 2021, if passed, would have amended Pennsylvania statutes to require that all environmental permitting applications for emerging technologies, including those related to cryptocurrency, be processed in the central office of Pennsylvania’s Department of Environmental Protection. Another bill proposed in 2021, if passed, would have established a financial technology sandbox program in the state. However, both bills died in the legislature.

The Pennsylvania Department of Banking and Securities has stated that it does not consider virtual currency to be “money” under the state’s money transmission laws. Thus, the transmission of virtual currency alone does not require a money transmitter license in the state. Presumably, however, a company working with virtual currency that also transmits fiat currency would still be required to obtain a money transmitter license in the state.

While Pennsylvania’s securities laws do not explicitly address digital assets, a settlement between the Pennsylvania Department of Banking and Securities and a digital asset financial services company for alleged violations of state securities laws indicates that the Department considers at least some digital assets to be securities.

A bill proposed in March 2023 would, if passed, establish a task force on digital currency and the impact on widespread use of cryptocurrency and other forms of digital currencies in the state.



Puerto Rico

Puerto Rico has both passed legislation and issued regulations, in addition to regulatory guidelines and statements, that expressly address several key concepts, including virtual currency and distributed ledger technology.

The Office of the Commissioner of Financial Institutions (“OCFI”) is the principal regulator for both securities and banking regimes in Puerto Rico. The OCFI has interpreted existing statutes governing “international financial entities” (“IFE”) to permit those entities to work with virtual currency and blockchain technology. Puerto Rico was among several jurisdictions that were included in the 2022 settlement with a digital asset financial services company, which included allegations that the platform sold unregistered securities to retail investors in violation of state securities laws.

The OCFI has issued guidance stating that all money services businesses, including those that handle cryptocurrency or convertible virtual currency or operate Bitcoin Teller Machines (“BTMs”), must be licensed as money services businesses under the territory’s laws.

Puerto Rico does not have programs or subsidies directly relevant to digital asset-related activities, but does allow for an “Incentive Decree” for businesses established in Puerto Rico developing software. In February 2023, the Puerto Rico Department of Economic Development and Commerce issued guidance clarifying the scope of the terms “blockchain technology”, “digital assets based on blockchain technology” and “blockchain validation” under the territory’s Incentives Code.

Rhode Island

Rhode Island has taken various steps to integrate virtual currency into the state’s existing regulation. Rhode Island is the only state to have enacted the Uniform Regulation of Virtual-Currency Businesses Act (“URVCBA”).

Under the Rhode Island URVCBA, subject to certain exemptions, an entity engaging in a virtual currency business activity is required to be licensed as a currency transmitter. The Rhode Island URVCBA also requires covered entities to make certain statutory disclosures to their customers before establishing relationships with them. Rhode Island does, however, recognize reciprocity of a currency transmitter license from another state, subject to the Rhode Island Department of Business Regulation’s approval, but it is unclear if approval would be granted for a license existing under a non-URVCBA framework.

Outside of activity that would be deemed virtual currency business activity, Rhode Island law does not directly address many facets of the digital asset ecosystem. While Rhode Island’s securities laws do not explicitly address digital assets either, a recent settlement between the Department of Business Regulations and a digital asset financial services company for alleged violations of state securities laws indicates that the Department considers at least some digital assets to be securities.

A bill proposed in February 2023 would, if passed, amend the state’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records).

South Carolina

South Carolina has made little progress toward modernizing its statutory environment to address digital assets, instead focusing on interpretive guidance and enforcement as a means of regulation.

In 2018, the South Carolina Attorney General’s Division of Money Services Transmitters issued guidance stating that virtual currencies alone do not qualify as “monetary value” under the state’s money transmission statute, but that to the extent that virtual currency transactions also involve the transfer of fiat currency, they may be subject to the statute. The Division also noted that the characteristics of virtual currencies may evolve over time, and reserved the right to reassess the issue of the statute’s application to virtual currency in the future.

In 2022 and 2023, the Securities Division of the South Carolina Attorney General’s Office reached major settlements with digital asset financial services companies over alleged offers and sales of unregistered securities in violation of state securities laws, indicating that the Division considers at least some digital assets to be securities.

A bill proposed in 2021, if passed, would have defined “digital assets,” “virtual currencies,” and “smart contracts,” among other terms; allowed digital assets to be pledged as collateral for secured transactions; and recognized the legal effect of smart contracts. However, the bill died in committee.



South Dakota

South Dakota has codified some laws addressing digital assets or blockchain technology. There is no case law or regulatory guidance concerning the classification of smart contracts, although there are laws governing automated transactions that are likely applicable.

The South Dakota Division of Banking is responsible for issuing money transmitter licenses and serves as the money transmitter registration authority. The Division of Banking has issued guidance stating that entities receiving virtual currency for transmission would likely be required to obtain a state money transmitter license to operate in the state. Per a 2022 amendment to the state's money transmission statute, a transmitter of virtual currencies must hold like-kind virtual currencies of the same volume as that held by the transmitter but that is obligated to consumers.

The Division of Banking has demonstrated its openness to chartering digital asset custodians, including firms that custody assets for financial institutions, through its chartering decisions. Actual guidance issued by the Division, however, does not differentiate specifically between digital asset custodians and other South Dakota trust companies.

In 2018, the South Dakota Division of Insurance published guidance on ICOs from the North American Securities Administrators Association. The guidance states that equity tokens are more likely to be regulated as securities than utility tokens. The guidance further states that if a utility token is issued for a non-operational project or planned to be traded on an exchange, it may also fall under the purview of securities regulation.

A bill proposed in January 2023, and passed by the state legislature, would have amended the state's commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records). However, South Dakota's governor vetoed the bill in March 2023.

Tennessee

In 2022, Tennessee became one of the first states to provide for the legal formation of DAOs as LLCs that may be managed by smart contract or by their members, and which by statute differ in important respects from standard LLCs. Tennessee by statute also recognizes the legal effect, validity, and enforceability of smart contracts.

The Tennessee Department of Financial Institutions has defined "virtual currency" in a memorandum that distinguishes cryptocurrency from fiat currency and explains when virtual currency activity falls within the state's money transmitter statute. Generally, virtual currency is not "money," and therefore not governed by the statute unless the transaction involves sovereign currency. The memorandum provides examples of when virtual currency activity may amount to money transmission that would require a state license.

In 2022, Tennessee, along with other states, reached a major securities law settlement with a digital asset financial services company that allegedly offered and sold unregistered securities in violation of state securities laws. Tennessee's unclaimed property statute covers property that is virtual currency, as defined in that statute with certain exclusions.

Under the Tennessee commercial code, a security interest in electronic documents is enforceable if the secured party has control under specified statutory provisions. A bill proposed in January 2023 would, if passed, amend the state's commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records).

In Tennessee, local governments are forbidden from regulating online marketplaces, which are defined as including entities that "[p]rovid[e] a virtual currency that users are allowed or required to use to transact." The Tennessee Department of Revenue's Tax Manual defines the transfer of virtual currency as intangible personal property exempt from the state's business tax.



Texas

Texas has robust legislation relating to digital assets. Its commercial code explicitly defines “virtual currency,” and it is one of the few states that has issued guidance defining terms such as “digital wallet,” “blockchain technology,” “cryptocurrency,” and even “stablecoin.”

The Texas Department of Banking has provided guidance in a supervisory memorandum regarding the circumstances in which the transmission of virtual currency constitutes “money transmission” under state law. Per the memorandum, the transmission of virtual currency is generally not considered “money transmission” as long as no sovereign or fiat currency is involved in the transaction; however, if sovereign or fiat currency is involved, then the transaction may be deemed to constitute “money transmission.”

Texas permits state-chartered banks to provide customers with virtual currency custody services, as long as the banks have adequate protocols in place to effectively manage associated risks and comply with applicable law. Texas also permits certain corporate records to be maintained by or by means of “a distributed electronic network or database, including one that employs blockchain or distributed ledger technology,” provided that the records can be converted into written paper form within a reasonable time.

In October 2022, the Texas State Securities Board issued a cease and desist order to a virtual gambling company for allegedly marketing and selling unregistered securities in the form of NFTs, and for allegedly engaging in securities fraud in connection with those NFTs, indicating that the Board considers at least some digital assets to be securities under the state’s securities laws.

In 2021, Texas passed legislation that amended the state’s commercial code to define “virtual currency,” address what constitutes control of virtual currency, and govern rights for one who controls virtual currency. A bill proposed in March 2023 would, if passed, further amend the state’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12).

A bill proposed in February 2023 would, if passed, temporarily exempt certain tangible personal property related to virtual currency mines from sales and use taxes. And a bill proposed in March 2023 would, if passed, authorize the formation of decentralized unincorporated associations and allow the use of distributed ledger or blockchain technology for certain business purposes under the state’s Business Organizations Code.

Utah

Utah has made modest progress toward modernizing its statutory environment to address digital assets, particularly through its statutory definitions of “virtual currencies,” “digital assets,” and “smart contracts,” among other terms. Blockchain tokens are explicitly excluded from the state’s money transmission statute. Utah also has a regulatory sandbox program to allow participants to experiment with products, production methods, or services. And in March 2023, Utah passed the Decentralized Autonomous Organizations Act (effective January 1, 2024), which allows DAOs that have not registered as for-profit corporate entities or non-profit entities to be treated as the legal equivalent of domestic LLCs.

The Utah Digital Asset Management Act establishes a framework for the ownership of digital assets. The Act provides that digital securities are personal property and are to be considered securities and investment property under the investment securities and secured transactions chapters of the state’s commercial code. The Act also specifies that an owner of a digital user asset may demonstrate ownership of the asset through control.

Utah does not currently offer any digital asset-specific subsidies or tax advantages for entities operating in the space. But effective July 1, 2022, Utah requires its Division of Finance to contract with a third party to accept payments to participating government agencies in the form of digital assets, and authorizes the Division of Finance to contract with a third party to accept payments to political subdivisions in the form of digital assets.



Vermont

Since 2015, Vermont's initial adoption of blockchain-based concepts has expanded into a robust set of definitions bringing blockchain technology into the state's laws regarding banking and insurance, taxation and finance, and business entities (including the recognition of DAOs through so-called "blockchain-based LLCs" that may utilize smart contract voting mechanics that are recognized under state law), to name a few. Vermont also expressly gives blockchain records evidentiary force.

Vermont requires those engaging in money transmission to obtain a license from the Department of Financial Regulation ("DFR"). Based on Vermont's definition of "money transmission," purveyors of virtual currency will likely be subject to the DFR's licensing requirements. Further, in 2022, Vermont's money transmission statute was amended to require money transmitters to register each kiosk where consumers can buy or sell virtual currencies.

In 2022 and 2023, the DFR reached major settlements with two digital asset financial services companies for allegedly offering and selling unregistered securities in violation of state securities laws, indicating that the DFR considers at least some digital assets to be securities under the state's securities laws.

Vermont currently has no specific digital asset related energy, ESG, or tax subsidy initiatives.

Virgin Islands

In January 2022, the U.S. Virgin Islands Banking Board published a bulletin about the application of the territory's money transmission law to cryptocurrency. The bulletin states that the territory has no laws, rules, or regulations governing cryptocurrency services, and that licensure and regulation of cryptocurrency services do not fall under the territory's money transmission law. In December 2022, the Board denied five cryptocurrency firms' applications for money transmitter licenses in the territory, stating that the Board does not issue licenses to cryptocurrency firms not regulated by the territory.

The Virgin Islands does not have laws pertaining to the enforceability of smart contracts and does not have explicit provisions regarding DAOs. Further, the territory does not offer tax subsidies or exemptions to blockchain- or digital asset-based companies.

Virginia

In 2022, Virginia made its initial push into modernizing its statutory and regulatory environment to incorporate blockchain technology by passing a law allowing state chartered banks to custody virtual currency, subject to certain internal compliance requirements. In 2023, the state passed a law allowing credit unions to custody virtual currency as well, again subject to certain internal compliance requirements.

Virginia relies on the Bureau of Financial Institutions ("BFI"), a division of the State Corporation Commission, for consumer protection and administration of state laws regarding depository and non-depository financial institutions. The BFI also enforces the state's money transmitter laws, which may, depending on the involvement of fiat currency, apply to parties engaging in virtual currency transactions.

Virginia does not recognize DAOs, smart contracts, or other common blockchain-based concepts, and currently has no specific digital asset-related energy, ESG, or tax subsidy initiatives. A bill proposed in 2022, if passed, would have provided for the legal formation of DAOs as LLCs and exempt issuers or sellers of digital tokens from securities registration requirements under certain circumstances; however, in February 2023, the bill was passed by indefinitely.



Washington

Washington has taken significant steps toward bringing digital assets under state regulation in the areas of money transmission, securities, taxation, and banking services.

Under its money transmission laws, Washington explicitly defines “money transmission” to encompass virtual currency. Thus, many companies offering virtual currency services in Washington are likely required to obtain a money transmitter license in the state. Further, certain requirements of Washington’s money transmission laws apply specifically to licensees transmitting virtual currencies. However, Washington excludes the storage of virtual currency from its money transmission law “when the virtual currency is owned by others and the person storing the virtual currency does not have the unilateral ability to transmit the value being stored.”

With respect to securities, while Washington’s securities laws do not explicitly address digital assets, the Securities Division of the Washington Department of Financial Institutions (“DFI”) has issued guidance on the application of Washington’s securities laws to digital assets. This guidance notes that the state’s definition of a security is very broad, and indicates that the offer and sale of digital assets in ICOs and other token sales are frequently subject to regulation under state and federal securities laws. This guidance is borne out by the DFI’s numerous enforcement actions against companies working with digital assets for alleged violations of the state’s securities laws.

In the context of taxation, the Washington Department of Revenue has stated that NFTs are subject to the state’s sales and use taxes under certain circumstances. The Department has also stated that cryptocurrency is intangible property that is generally subject to capital gains tax if certain conditions are met.

As for custodianship, Washington allows state-chartered banks to provide banking services to companies working with digital assets, and to seek permission from the DFI to custody digital assets. Washington also allows state-chartered non-depository trust companies to provide custody services of digital assets.

A bill proposed in December 2022 would, if enacted, amend the state’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records). The bill passed the state legislature in April 2023 and has been submitted to the governor.

West Virginia

West Virginia has been proposing legislation to expand the state’s adoption of digital asset- and blockchain-based concepts. Two bills proposed in 2022, if passed, would have set forth requirements and specifics to regulate digital asset custodial services. One of those bills, if passed, also would have prohibited the taxation of virtual currency by counties and municipalities; prohibited public utilities from charging fees or infringing upon the use of energy used in mining of digital or virtual currency; and exempted virtual currency from regulation as checks and money order sales, money transmission services, transportation, and current exchange. However, both bills died in committee.

A bill proposed in February 2023 would, if passed, amend the state’s commercial code to incorporate the amendments to the UCC approved by the ULC in 2022 to address emerging technologies (including Article 12 relating to controllable electronic records).

West Virginia’s money transmission statute incorporates the concept of “other value that substitutes for money.” Virtual currency could be covered by West Virginia’s money transmission laws under a reasonable reading of this provision.

West Virginia does not recognize DAOs and currently has no specific digital asset-related energy, ESG, or tax subsidy initiatives. However, the state has incorporated virtual currency into its statute governing use tax. The state also has a regulatory sandbox program for companies seeking to test an innovative product or service in the state.



Wisconsin

Wisconsin is still in the early stages of developing laws relating to digital assets, although certain statutes contain provisions relating to “digital property.” These include electronic communications and computing services, but the statutes do not address cryptocurrencies directly.

Wisconsin also has not enacted legislation regarding DAOs or smart contracts. The Wisconsin Department of Financial Institutions has issued guidance stating that the state’s money transmission statute does not encompass virtual currency, but that should the transmission of virtual currency involve sovereign currency, it may be subject to license depending on how the transaction is structured.

In 2023, the Wisconsin Department of Financial Institutions reached a major settlement with a digital asset financial services company over alleged offers and sales of unregistered securities in violation of state securities laws, indicating that the Department considers at least some digital assets to be securities under the state’s securities laws.

Because Wisconsin does not treat virtual currency and other digital assets differently from other types of intangible property, Wisconsin taxpayers must report income, gains, expenses, and losses as required by the Internal Revenue Code.

Wyoming

Wyoming is the leader in adopting digital asset- and blockchain-related concepts into its legal and regulatory structure and is often considered the “Delaware for digital asset companies.” Wyoming has enacted sweeping legislation addressing these concepts in the contexts of securities, money transmission, corporate recordkeeping, taxation, corporate forms, custodianship, and commercial transactions.

Wyoming exempts certain types of digital assets from several state laws. It exempts virtual currency from its money transmission law, utility blockchain tokens from its securities laws (if certain conditions are met), and virtual currency from state property taxation. Wyoming also has a financial technology sandbox program for the testing of innovative financial products and services in the state.


Wyoming was the first state to enact legislation specifically allowing for the state registration of a DAO, allowing DAOs to incorporate as LLCs. Wyoming also authorizes the chartering of “special purpose depository institutions,” which may accept deposits and conduct other activities incidental to traditional banking activities, including custody of digital assets, asset servicing, fiduciary asset management, and other services for virtual currency businesses. Additionally, Wyoming permits banks to custody digital assets, subject to certain compliance requirements.

Further, Wyoming authorizes corporate recordkeeping by distributed or electronic records, and has incorporated three distinct classifications of digital assets (digital consumer assets, digital securities, and virtual currencies) into its commercial code.

In March 2023, Wyoming passed the Stable Token Act, which creates the Wyoming Stable Token Commission and authorizes the Commission to issue Wyoming stable tokens as specified in the Act. Thus, Wyoming became the first state to allow itself to create its own stablecoin.



CHAPTER III
**2022 UCC
DIGITAL ASSET
AMENDMENTS**





NOVEMBER 2022

Since the emergence of virtual currencies, NFTs, and other digital assets, the market has struggled with the lack of clarity under current commercial law rules that do not contemplate these types of assets, including in transactions that involve the sale of these assets or the use of these assets as collateral. While certain workarounds developed under the Uniform Commercial Code (“UCC”), doubt remained in both sale and collateral transactions on whether the owner of the digital assets acquired such assets free of other property claims.

To address these concerns, in 2019, the Uniform Law Commission (“ULC”) and American Law Institute (“ALI”) appointed a joint drafting committee (the “Joint Committee”) to consider and formulate proposed amendments to the UCC to accommodate emerging technologies. On May 18, 2022, the ALI, and on July 13, 2022, the ULC, approved the proposed amendments to the UCC (the “2022 Amendments”), which cleared the way for the 2022 Amendments to be sent to the U.S. states and territories for adoption.

In particular, the 2022 Amendments add a new Article 12 regarding sales of, and security interests in, “controllable electronic records” (or “CERs”), as well as “controllable accounts” and “controllable payment intangibles” that are evidenced by a CER. While the term “CER” would include technologies that exist today, such as Bitcoin, Ether, and NFTs, it has been designed to pick up technologies that are developed in the future as well. The 2022 Amendments also make changes to Article 9 of the UCC to address and incorporate CERs as a new asset category, thus establishing clear perfection, priority, and choice of law rules for transactions where the CER is pledged as collateral. Moreover, the 2022 Amendments provide legal assurance as to when a transferee of a CER acquires its interest therein free of conflicting property claims.

The 2022 Amendments provide a number of workable rules for transactions involving CERs.

First are the “take free” rules. If the buyer or a secured party in a transaction involving a CER is a “qualifying purchaser,” that transferee will take all rights that the transferor had in the CER and will take its interest in the CER free of competing property claims in the CER (UCC § 12-104(e)). To be a “qualifying purchaser,” the transferee must: (i) acquire the CER in a transaction that constitutes a “purchase” (within the meaning of Article 1 of the UCC, and that includes grants of liens); (ii) have control of the CER; (iii) give value (within the meaning of Article 3 of the UCC); (iv) act in good faith; and (v) not have notice of a property right claim in the CER (UCC § 12-102(a)(2)).

Second are the “control” rules. Under the 2022 Amendments, a person has “control” of a CER if that person: (i) has the power to avail itself of substantially all the benefit from the electronic record; (ii) has the exclusive power to prevent others from availing themselves of substantially all the benefit from the electronic record; and (iii) has the exclusive power to transfer control of the electronic record to another person or cause another person to obtain control of another controllable electronic record as a result of the transfer of the electronic record (UCC § 12-105). In addition, such person must have the power to readily identify itself to a third party as having the above specified powers (i.e., via a cryptographic key or other identifying number) (UCC § 12-105(a)).

Third are the “perfection by control” rules. The 2022 Amendments provide that a secured party that perfects its security interest in the CER by “control” will have non-temporal priority over another secured party that does not have control, including a secured party that has perfected its security interest solely by the filing of a financing

statement (UCC § 9-326A). A security interest in a CER can be perfected by filing a UCC-1 financing statement (UCC § 9-312(a)). However, a security interest in a CER perfected by control has priority over a security interest perfected solely by filing a financing statement. It should also be noted that, under the 2022 Amendments, the filing of a UCC-1 financing statement is not by itself notice of a property claim to a CER (UCC § 12-104(h)). This is important since, as noted above, a good-faith purchaser for value of a CER that obtains control of the CER without notice of a prior security interest or other claim of a property interest in such CER will be a «qualifying purchaser» and will be afforded greater rights than the transferor of such CER.

Fourth is the “choice of law” rule. Article 12 includes a choice of law rule to determine the jurisdiction of the CER and provides that the local law of the CER’s jurisdiction governs matters covered by Article 12, as well as perfection and priority of security interests in CERs under Article 9 (UCC § 12-107(a); 12-107(f)). Perfection by filing, though, is determined by the debtor’s location, consistent with the existing rules (UCC § 9-306B(b)(1)). Under Section 12-107(c), a CER’s jurisdiction is determined according to a waterfall of rules, each of which references ways in which an “expressly” chosen jurisdiction for the CER can be determined, in which case the law of such chosen jurisdiction will govern. As a final fallback, Washington, D.C. law governs (including “as if” Article 12 were in effect in Washington, D.C., if the District has not yet adopted Article 12 without material modification) (UCC § 12-107(c); 12-107(d)).

Finally, the 2022 Amendments address one of the workarounds noted above under current Article 8 for perfection by control of CERs maintained in a “securities account” with a “securities intermediary.” Article 8 of the UCC covering investment securities has been amended to clarify that a CER is a “financial asset” for purposes of Article 8 if Section 8-102(a)(9)(iii) applies (UCC § 8-103(h)). As a result, if a customer and a securities intermediary agree that CERs of the customer maintained in a securities account with the securities intermediary are «financial assets» under Article 8, those CERs are considered investment property for purposes of the perfection by control rules under Article 8 (UCC § 8-102(a)(9)(iii); UCC § 8-106).

As a result of El Salvador and the Central African Republic making Bitcoin legal tender in their respective countries, questions emerged in the market whether Bitcoin was now “money” as defined in the UCC and if the “perfection by possession” rules thus applied to Bitcoin, which would be practically impossible for an intangible currency. The 2022 Amendments address the resulting issue by introducing a new term, “electronic money”—which is defined in Article 9 simply as “money in electronic form”—and amending the Article 1 definition of “money” to exclude from the term an electronic medium of exchange, or digital currency, that

existed before a government adopted such preexisting medium of exchange as legal tender (UCC § 1-201(b)(24)). As a result, existing digital currencies, including Bitcoin, can never constitute «money» under the UCC, but they could constitute a CER.

The 2022 Amendments further provide that the Article 1 definition of “money” as used in Article 9 excludes: (i) deposit accounts; and (ii) money in an electronic form that cannot be subject to the control rules of Article 9 for “electronic money” (UCC § 9-102(a)(54A)). This is important because under the new rules in Article 9, the only way to perfect a security interest in electronic money as original collateral is by “control,” and the mechanism for control is the same as that for CERs noted above (UCC § 9-105A and § 9-312(b)(4)). As a result of these amendments, digital currencies that constitute electronic money or a CER can be perfected only by “control” and not by “possession” under the UCC.

To assist the transition of both existing transactions and transactions entered into after the effective date of the 2022 Amendments in the relevant state, the 2022 Amendments include “transition rules.” Under these rules, it will be up to each state to determine its own effective date of the 2022 Amendments, but to ensure an appropriate transition period, there is the concept of an “adjustment date” of at least one year from the effective date for the changes to apply to existing transactions that predate the effective date of the 2022 Amendments (UCC 2022 Amendments, Annex A).

Parties to transactions involving digital assets should follow the enactment of the 2022 Amendments and consider whether the 2022 Amendments enacted in the respective states would affect their transaction, including those transactions entered into under current law.

CHAPTER IV

**REGULATORY
ISSUES
(U.S. FEDERAL)**



DIGITAL ASSETS DEFINED: WRITING DIGITAL ASSETS INTO THE BANKRUPTCY CODE

NOVEMBER 2022 WHITE PAPER

As discussed in [previous installments of this *White Paper* series](#), the Lummis-Gillibrand Responsible Financial Innovation Act (the “Bill”) proposes a comprehensive statutory and regulatory framework in an effort to bring stability to the digital asset market. One area of proposed change relates to how digital assets and digital asset exchanges would be treated in bankruptcy. If enacted, the Bill would significantly alter the status quo from a bankruptcy perspective.

OVERVIEW OF DIGITAL ASSETS IN BANKRUPTCY

There is little reported jurisprudence in the United States specifically relating to insolvency proceedings involving digital assets (e.g., cryptocurrencies). In fact, how these assets are treated in bankruptcy in certain aspects is currently developing, as several significant players in the cryptocurrency arena have commenced bankruptcy and insolvency proceedings in the United States and abroad (e.g., Voyager Digital Holdings, Celsius Network, Three Arrows Capital). The only other analogue was in 2014, when the high-profile cryptocurrency exchange, Mt. Gox, commenced a bankruptcy proceeding in Japan after halting bitcoin trading due to major security breaches and bitcoin theft. After years of legal proceedings, the Japanese trustee announced in October 2021 that a civil rehabilitation plan was accepted by a majority of creditors, yet it remains uncertain when distributions to creditors will occur and the effect market volatility will have on such distributions.

In light of the lack of U.S. precedent and overall volatility in the cryptocurrency market, if passed, the Bill could provide much-needed certainty relating to the treatment of digital assets in a U.S. bankruptcy proceeding. To do so, the Bill largely proposes to integrate digital assets into existing statutory and regulatory frameworks relating to the

treatment of commodities and the relief available to commodity brokers in bankruptcy.

The primary objective of the existing provisions of the Bankruptcy Code relating to commodities is to minimize the ripple effect and disruption that the bankruptcy of a major commodities player could have on the markets. The statutory framework relating to the liquidation of a commodity broker has been tested very little. Moreover, the U.S. Commodity Futures Trading Commission (“CFTC”) has enacted a complicated web of rules—the Part 190 Rules—which apply in conjunction with, and sometimes supersede, the Bankruptcy Code in a commodity broker liquidation.

The Bill proposes to amend, among other things, the definition of “commodity broker” to include “digital asset exchange,” which the Bill in turn defines as “a centralized or decentralized platform which facilitates the transfer of digital assets” and “a trading facility that lists for trading at least one digital asset.” This, among other proposed changes, would enact significant changes to both the relief available to a digital asset exchange should it file for bankruptcy and the treatment and protections offered to customers and non-debtor parties to digital asset contracts in a bankruptcy proceeding. For example, should a digital asset exchange seek bankruptcy relief, the Bill proposes to require such exchange to liquidate under the chapter 7 bankruptcy

scheme relating to commodity brokers (the “Commodity Broker Liquidation Subchapter”). Conversely, in instances where a digital asset exchange is not the bankrupt entity but is party to a digital asset contract with a debtor, section 556 of the Bankruptcy Code would generally protect the digital asset exchange from certain key provisions of the Bankruptcy Code, which, if permitted to apply, could potentially cause a domino effect in the markets.

BANKRUPTCY RELIEF AVAILABLE TO DIGITAL ASSET EXCHANGES

As proposed by the Bill, the only bankruptcy relief available to a digital asset exchange would be chapter 7 liquidation under the Commodity Broker Liquidation Subchapter. A digital asset exchange would not qualify for chapter 11 relief. By limiting bankruptcy relief to the Commodity Broker Liquidation Subchapter, the Bill would, among other things, put digital asset exchanges into an established framework that specifically governs the treatment of customer property vs. non-customer property, customer rights, and the portability of customer positions in digital assets.

As noted previously, the overall purpose of the Commodity Broker Liquidation Subchapter is to minimize the ripple effect and disruption that the insolvency of a commodity broker could have on the markets. This is accomplished by a host of mechanisms, many of which equip customers with strong protections and powers that non-debtor parties ordinarily do not have in traditional chapter 7 or chapter 11 bankruptcies. The Commodity Broker Liquidation Subchapter provides a skeletal framework by which commodity brokers (as defined by the Bankruptcy Code) are liquidated, which would include the appointment of a bankruptcy trustee. The Bankruptcy Code provisions are supplemented by and, at times, superseded by the Commodity Exchange Act and the Part 190 Rules, which contain the bulk of regulations defining the trustee’s powers and responsibilities in a commodity broker liquidation.

One hallmark function of the Commodity Broker Liquidation Subchapter and the Part 190 Rules is to protect “customer property” (typically funds held by the debtor on account of a commodities customer). The Bill proposes, among other things, to include “digital asset” in the definition of “customer property.” In a commodity broker liquidation, customer funds must be segregated and treated as property of the customer, not property of the bankrupt commodity broker. The Commodity Broker Liquidation Subchapter and the Part 190 Rules also give customers the highest priority claims over customer property, subject to payment of certain expenses for administering the bankruptcy case. Another significant customer protection is that a bankrupt commodity broker must undergo best efforts to promptly transfer all customer accounts to another non-bankrupt

commodity broker. In contrast, the restructuring regime under chapter 11 of the Bankruptcy Code does not specifically enumerate these customer protections, which would likely result in the parties constantly litigating to determine or seek to enforce such rights. Accordingly, the conglomerate of statutes and rules governing a commodity broker liquidation seeks to provide more certainty, reduce litigation, and minimize the “domino” effect on the markets that could ensue by a commodity broker bankruptcy.

Another aspect of the Bankruptcy Code designed to preserve the market is that sections 546(e) and 764(b) of the Bankruptcy Code effectively insulate from avoidance all payments made pre-bankruptcy or within seven days after the bankruptcy filing from a commodity broker to its customers. These provisions also facilitate the trustee’s directive to make best efforts to transfer all customer accounts to another commodity broker as soon as possible after the bankruptcy filing.

The Commodity Broker Liquidation Subchapter and the Part 190 Rules also require the trustee to provide notice to customers of the bankruptcy filing requesting that the customer instruct the trustee as to the disposition of such customer’s specifically identifiable property and file a proof of claim. The trustee must comply with, to the extent practicable, the customer’s instructions relating to the disposition of customer property. The primary objective of these provisions is to facilitate a prompt transfer of all customer accounts to another commodity broker, ensure that customers receive their pro rata share of customer property, and mitigate the ripple effect a commodity broker bankruptcy could have on the market.

SECTION 556 COMMODITY BROKER AND COMMODITY CONTRACT PROTECTIONS

The Bill also proposes to provide a digital asset exchange with certain protections in instances where such exchange is not the bankrupt entity but is party to a digital asset contract with a debtor. Specifically, the Bill seeks to expand section 556 of the Bankruptcy Code to enable a digital asset exchange to exercise its contract rights notwithstanding certain provisions of the Bankruptcy Code.

First, upon a bankruptcy filing, the “automatic stay” immediately halts all litigation and actions against the debtor or its property, including a non-debtor’s efforts to enforce its contract rights against the debtor. Section 556 permits non-defaulting “protected parties”—e.g., commodity brokers—to commodity contracts with a debtor to exercise their contractual rights notwithstanding the automatic stay. These rights can include, for example, the right to liquidate, terminate, cancel, or set off mutual debts and claims relating to commodity contracts. Were this not so, a commodity

contract could be in a state of limbo for the entire pendency of the bankruptcy—possibly years—which could wreak havoc on the markets.

Second, in ordinary bankruptcy circumstances, section 365 of the Bankruptcy Code empowers a debtor to assume or reject executory contracts (i.e., contracts where both counterparties have material unperformed obligations). In a chapter 11 reorganization case, the debtor may assume or reject an executory contract at any time before confirmation of a plan, possibly years after commencement of the case. In the context of commodities and derivatives contracts, the debtor would be, at minimum, incentivized to delay assuming or rejecting the contract until after the date on which the debtor was required to perform to see if the market price of the commodity fluctuated to the debtor's benefit. To mitigate this problem, section 556 allows a protected party at any time to exercise its contractual rights.

Third, a debtor is equipped with certain powers to claw back fraudulent or preferential pre-bankruptcy transfers or transactions. Section 556 operates in conjunction with section 546(e) of the Bankruptcy Code to exempt from clawback a transfer “made by or to (or for the benefit of) a [protected party]” that is “in connection with a . . . commodity contract.” These protections limit the trustee's ability to avoid a host of transfers that are germane to the commodity and derivatives markets—in particular, for example, maintenance margin and mark-to-market payments. Section 546(e) does not, however, disarm the debtor's powers to avoid transfers made with the actual intent to hinder, delay, or defraud creditors.

CONCLUSION AND OUTLOOK

While it is unlikely the Bill will pass in its current form, it proposes a framework that could establish much-needed certainty regarding how digital assets are treated in bankruptcy. The pending bankruptcy and insolvency cases involving digital assets may highlight additional issues unique to the treatment of digital assets in bankruptcy and prompt Congress to propose further changes to the Bankruptcy Code. At present, while subject to some debate, a digital asset exchange could seek to reorganize or liquidate under chapter 11 of the Bankruptcy Code, which means far less certainty for customers than if the digital asset exchange were subject to the Commodity Broker Liquidation Subchapter and Part 190 Rules.

ENDNOTES

- 1 Lummis-Gillibrand Responsible Financial Innovation Act, S. 4356, 117th Cong., § 101(a) (2022) (proposed 31 U.S.C. § 9801(2)).
- 2 “Mt. Gox Creditors to Get Billions in Bitcoin After Plan Approved,” Bloomberg.com, October 20, 2021.
- 3 11 U.S.C. §§ 101 *et seq.*
- 4 See, e.g., *In re Peregrine Financial Group, Inc.*, Case No. 12-27488 (Bankr. N.D. Ill. July 10, 2012).
- 5 17 C.F.R. § 190.00 *et seq.*
- 6 S. 4356, § 203(a) (proposed 26 U.S.C. § 864(b)(C)).
- 7 *Id.* § 401 (amending 7 U.S.C. § 1a).
- 8 11 U.S.C. §§ 761-767.
- 9 *Id.* § 556.
- 10 See *id.* § 109(d) (providing that “[o]nly . . . a person that may be a debtor under chapter 7 of this title (except a stockbroker or a commodity broker) . . . may be a debtor under chapter 11 of this title”); §§ 761-767 (liquidation regime for commodity brokers).
- 11 *Id.* § 101(6).
- 12 7 U.S.C. § 1 *et seq.*
- 13 11 U.S.C. § 761(10) (defining “customer property” as “cash, a security, or other property, or proceeds of such cash, security, or property, received, acquired, or held by or for the account of the debtor, from or for the account of a customer. . .”). Not all cash, securities, or property subject to a commodity contract fall within the “customer property” protections.
- 14 S. 4356, § 407(e)(2) (amending 11 U.S.C. § 761(10)).
- 15 See 11 U.S.C. § 766(c).
- 16 While the Commodity Broker Liquidation Subchapter definitively establishes customer protections, whether a party or property is entitled to such protections could be subject to litigation.
- 17 Commodity Fut. Trad. Comm'n, Bankruptcy—Proposed Rules, 46 Fed. Reg. 57,535 *et seq.* (Nov. 24, 1981).
- 18 11 U.S.C. §§ 546(e); 764(b). Specifically, section 764(b) and the Part 190 Rules protect, in most instances, any transfer or liquidation of a commodity contract from avoidance if such transfer or liquidation is approved by the CFTC by rule or order.
- 19 *Id.* § 765.
- 20 S. 4356, § 407(c) (amending 11 U.S.C. § 556).
- 21 11 U.S.C. § 362(a).
- 22 *Id.* § 365.
- 23 See *id.* § 365(d)(2).
- 24 See *id.* §§ 544, 547, and 548.
- 25 *Id.* § 546(e).
- 26 Courts hold that the safe harbor provisions of section 546(e) do not automatically bar avoidance claims, but are an affirmative defense that is waived if not timely raised. See, e.g., *Tronox Inc. v. Kerr McGee Corp. (In re Tronox Inc.)*, 503 B.R. 239, 338–40 (Bankr. S.D.N.Y. 2013).



DIGITAL ASSETS DEFINED: FEDERAL AGENCIES WEIGH RESPONSE TO PRESIDENT BIDEN'S EXECUTIVE ORDER ON DIGITAL ASSETS

OCTOBER 2022 WHITE PAPER

On March 9, 2022, President Biden issued Executive Order 14067 (“EO”), “Ensuring Responsible Development of Digital Assets.” The EO, which we discussed in “[White House Issues Executive Order Calling for Inter-Agency Study of Digital Assets](#),” required a number of federal agencies to issue reports regarding issues raised by digital assets with respect to each agency’s area of jurisdiction. Those agencies have now issued nine reports, covering topics ranging from central bank digital currencies (“CBDC”) to anti-money laundering (“AML”) to the climate and energy implications of creating and using digital assets.

In this *White Paper*, we discuss the high-level takeaways from each report, and what they likely mean for the future development and regulation of digital assets going forward. In two follow-on papers, we will take a closer look at the reports prepared by the White House Office of Science and Technology Policy (“OSTP”), and the U.S. Department of the Treasury.

WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY

The White House OSTP prepared a technical evaluation of developing a U.S. CBDC system (“[Technical Evaluation for a U.S. Central Bank Digital Currency System](#)”). In doing so, the OSTP also set forth the policy objectives of such a system. The report outlines the various choices and limitations that should inform the design and implementation of a “CBDC system” in the United States. Crucially, “CBDC system” includes not only the CBDC itself, but “the public and private sector components built to interact with it, and the laws and regulations that would apply to those components.” The term “components” is to be broadly construed and, by way of example, could encompass things such as smart cards, mobile applications, and intermediaries fulfilling various roles in the system.

The report (“[Policy Objectives for a U.S. Central Bank Digital Currency System](#)”) set forth eight policy objectives, which focus on nuts-and-bolts matters like interoperability with other payment systems as well as higher-level goals such as economic growth, equitable access, national security, and human rights:

The CBDC¹ system should include appropriate protections for consumers, investors, and businesses including guard-rails against fraud and market failures.

1. The CBDC system should be designed to integrate seamlessly with traditional forms of the U.S. dollar, and be both governable and sufficiently adaptable enough to promote competition and innovation.
2. The CBDC system should provide a good customer experience; make investments and domestic and

- cross-border fund transfers and payments cheaper, faster, and safer; and include appropriate cybersecurity and incident management so as to be protected against cybersecurity attacks and resilient against other potential disasters or failures. The CBDC system itself should be extensible and upgradeable such that it can be iterated upon quickly to improve and harness new innovation, as well as changing technologies, regulations, and needs.
3. The CBDC system should be appropriately interoperable to facilitate transactions with other currencies and systems, such as physical cash, commercial bank deposits, CBDCs issued by other monetary authorities, and the global financial system.
 4. The CBDC system should be available to all and expand equitable access to deposit and payment products and services, as well as credit provided by banks.
 5. The CBDC system should promote compliance with anti-money laundering (“AML”) and combating the financing of terrorism (“CFT”) requirements as well as relevant sanctions obligations.
 6. The CBDC system should be designed and used in accordance with civil and human rights, such as those protected by the U.S. Constitution and outlined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.
 7. The CBDC system should adhere to privacy engineering and risk management best practices, including privacy by design and disassociability.
- While some of the objectives may be in tension with each other, the document asserts that its aim is not to prioritize or reconcile any of the concepts, or even take a position on whether a U.S. CBDC should be released at all.
- In terms of a technical assessment, the report considers various design options and the ways in which they would further or hinder the realization of the above-stated policy objectives. Those options are broken into six different categories: Participants, Governance, Security, Transactions, Data, and Adjustments. In assessing the options, the report is careful to emphasize that it does not make any assumptions, prioritize any design choices, claim the list of design choices is complete, or take any positions on whether a CBDC system would be in the best interests of the United States.
- **Participants:** This section looks at different options for the transport layer and interoperability. The design of the transport layer within a CBDC system determines the degree to which transactions between two parties are intermediated by a third party, and who that third party is. Interoperability determines the extent to which a CBDC system can execute transactions with other payment systems, domestic or international, digital assets vs. nondigital assets, etc.
 - **Governance:** This section looks at permissioning, access tiering, identity privacy, and remediation. “Permissioning” determines whether a system is governed by a set of verified and trusted entities or by a collection of interested participants. Access tiering has to do with the way in which transactions could be parsed and handled differently according to specific attributes. “Identity privacy” relates to who, if anyone, knows the identity of the parties transacting within the CBDC system. And “remediation” has to do with how transaction errors, whether the result of fraud or a simple mistake, are corrected within the system.
 - **Security:** This section looks at cryptography and secure hardware. “Cryptography” involves the techniques used to ensure that transactions within the CBDC system are secure. “Secure hardware” considers the extent to which security features within the CBDC system are built into the hardware used to access and operate the system (e.g., smart cards, embedded chips, etc.) vs. managed through software running on general-purpose devices (e.g., computers, tablets, and smartphones).
 - **Transactions:** This section looks at signature, transaction privacy, offline transactions, and transaction programmability. “Signatures” concerns how many digital signatures are required to complete a transaction and who must provide them. “Transaction privacy” considers the degree to which transaction details (e.g., account balances, participant location(s), goods sold, etc.) are observable within the system and by whom. “Offline transactions” examines the extent to which parties could effectuate transactions between themselves and then later communicate those transactions to a transaction processor. And “transaction programmability” considers whether third-party developers could develop programs to run within the CBDC system, such as smart contracts.
 - **Data:** This section looks at data models and ledger history. “Data models” concerns the way in which ownership records would be stored. “Ledger history” considers whether an ownership and transaction ledger would be stored in a central location or distributed among various locations.
 - **Adjustments:** This section looks at fungibility, holding limits, adjustments on transactions, and adjustments on balances. “Fungibility” considers whether a CBDC would have a unique identifier, similar to serial numbers associated with U.S. dollar-denominated bills, or no unique identifier at all. “Holding limits” examines whether to limit entities to holding a set amount of CBDC. And “adjustments on transactions” and “adjustments on balances” looks at whether and how to impose fees on CBDC system users, and whether and how to allow balance adjustments for things like fees and interest, respectively.

A recurring theme in these sections is the sliding scale of privacy vs. AML/CFT compliance, with enhanced privacy making AML/CFT compliance more difficult, and vice versa. The sections also routinely focus on expanding access to the financial system in an equitable manner, and ensuring interoperability with payments systems that currently exist, and that may come into existence in the future.

The White House OSTP also prepared a report on climate and energy implications associated with digital assets (“Climate and Energy Implications of Crypto-Assets in the United States”). The report provides answers to several questions specifically set forth in the EO:

How do digital assets affect energy usage, including grid management and reliability, energy efficiency incentives and standards, and sources of energy supply?

The OSTP finds that crypto-asset networks use electricity to power four major functions: (i) data storage; (ii) computing; (iii) cooling; and (iv) data communications—with computing representing the vast majority of electricity use.² It concludes that crypto-assets impact electricity usage and the grid, but that their impact varies depending on the type of crypto-asset. Specifically, the report emphasizes the energy-use differences between proof-of-work (“PoW”) and proof-of-stake (“PoS”) blockchains. The OSTP points to 2021 research showing that each PoS computing device requires 10 to 500 times less power than a typical rig used for PoW Bitcoin mining.³ However, the report finds that total power usage from today’s crypto-asset networks cannot be directly monitored because many computing or mining centers do not disclose their location or report their electricity usage. Another challenge is that energy usage can fluctuate significantly, based on market value fluctuations of the underlying crypto-asset. Despite these challenges, the report estimates the United States’ PoW mining electricity usage to be in the range of 0.9% to 1.7% of total U.S. electricity usage. It also points to such a large range as suggesting a need for miners to report their actual electricity usage to reduce the uncertainties presented to policymakers.⁴

What is the scale of climate, energy, and environmental impacts of digital assets relative to other energy uses, and what innovations and policies are needed in the underlying data to enable robust comparisons?

This section of the OSTP report focuses on the environmental impact of crypto-assets and finds that crypto-asset mining produces GHG emissions and exacerbates climate

change primarily by burning coal, natural gas, or other fossil fuels to generate electricity in: (i) an onsite dedicated power plant; (ii) purchasing electricity from the power grid; and/or (iii) producing and disposing of computers and mining infrastructure, and production of power plant fuels and infrastructure.⁵

What are the potential uses of blockchain technology that could support climate monitoring or mitigating technologies?

The OSTP is not optimistic about the value of distributed ledger technology (“DLT”) in certain environmental markets. The report identifies two main types of environmental markets: those created pursuant to a regulatory program and those that are voluntary.⁶ While either market requires the type of robust market infrastructure that DLT is adept at providing—trade execution, payments, clearing and settlement, record-keeping, and security—environmental markets are currently highly centralized.⁷ Given that DLT is designed to solve issues associated with decentralization, the OSTP finds that there may not be a clear advantage to introducing DLT in environmental markets sufficient to justify the switching cost.

Despite its dim view of DLT in environmental markets, the OSTP appears to see potential for DLT in the context of grid reliability and distributed energy resources, or DERs, such as electric vehicles, fuel cells, residential and commercial battery systems, and solar power systems. The OSTP finds that DLT-supported innovation could help to digitize, automate, and decentralize the operation of an electricity grid that estimates say will have more than 100 million new storage devices connected by 2040.⁸ Since such numbers will require greater automation, the OSTP sees smart contracting as a candidate for supporting this aspect of the evolving clean energy marketplace.⁹

What key policy decisions, critical innovations, research and development, and assessment tools are needed to minimize or mitigate the climate, energy, and environmental implications of digital assets?

The OSTP report outlines a number of recommendations to ensure the responsible development of digital assets. These include collaboration among various government entities and the private sector to develop effective performance standards, conduct reliability assessments of crypto-asset mining operations, and analysis of information from crypto-asset miners and electric utilities. They also include promulgating and updating energy conservation standards for crypto-asset mining, encouraging crypto-asset industry

associations to publicly report certain information, and promoting and supporting further research and development priorities to improve the environmental sustainability of digital assets.

Overall, the report appears to be aimed at setting the stage for further legislation and regulation that would impact the crypto-asset industry by: (i) informally pressuring the industry to establish certain “best practices” even if such practices are not initially required; (ii) increasing required reporting; and (iii) setting increasingly stringent performance standards.

DEPARTMENT OF THE TREASURY

The Treasury’s report on “[The Future of Money and Payments](#)” includes three main components: (i) a section setting forth Treasury’s overview of the current payment system in place today, including recent developments; (ii) a section evaluating options for the U.S. government to pursue in developing a CBDC; and (iii) its four recommendations for improving the U.S. money and payments system.

The overview of the current payments system covers the different retail and wholesale payments systems in use for domestic and cross-border payments; the consumer choices available for consumer-facing payment systems; the roles that banks and non-bank intermediaries play in the current system; and recent developments such as stablecoins, FedNow, and ACH’s Real Time Payments network.

The section on a future CBDC is largely reminiscent of the OSTP report on the same topic. It lays out a number of choices to be considered in establishing a CBDC system, such as retail vs. wholesale transactions, whether a CBDC would pay interest, the extent of transaction programmability, the nature of the DLT technology underlying the system, interoperability with foreign CBDCs, and single- vs. two-tier intermediation with the Federal Reserve.

Finally, the report sets forth its recommendations for achieving the policy considerations presented in the EO—namely, building the future of money and payments, supporting U.S. global financial leadership, advancing financial inclusion and equity, and minimizing risks. The recommendations are not detailed, but a few items of note are:

- With respect to a CBDC, Treasury considers potential unintended consequences of a CBDC, including a run to CBDC in times of stress and a reduction in credit availability to the extent that CBDC uptake reduces bank deposits and, indirectly, bank lending.
- On the subject of federal payments regulation, Treasury notes that a federal framework would provide a common floor for existing state standards (such as minimum financial resource requirements) and also that it should

address run risk, payments risks, and other operational risks consistently and comprehensively.

The Treasury’s report on crypto-assets (“[Crypto-Assets: Implications for Consumers, Investors, and Businesses](#)”) includes four main components: (i) a section setting forth Treasury’s overview of the current crypto-assets market; (ii) a section providing a description of current uses of crypto-assets; (iii) a set of risks and exposures for consumers, investors, and businesses in the crypto-asset market, categorized into conduct risks, operational risks, and intermediation risks; and (iv) Treasury’s four recommendations to address risks associated with the crypto-asset sector.

The section on the current crypto-assets market describes three categories of relevant entities: crypto-asset platforms, miners and validators, and data aggregators. It also provides four central use cases for crypto-assets: (i) financial markets, products, and services that use native crypto-assets for trading, lending, and collateral activities of other crypto-assets, that are mostly speculative in nature; (ii) use as a medium of exchange for goods and services, in limited cases; (iii) market infrastructure for traditional assets using permissioned blockchains for payments, clearing, and settlement; and (iv) other commercial activities, largely non-fungible tokens (“NFTs”).

Treasury views three categories of risks and exposures as the most significant in this space: conduct risks, operational risks, and intermediation risks. Conduct risks include the use of crypto-assets for fraud and scams, information asymmetries between users and platforms, and platforms providing access to bad actors, providing products and services to retail investors without disclosing conflicts or ensuring suitability, and engaging in frontrunning and market manipulation. Operational risks include hacks, difficulty patching bugs in immutable smart contracts, tradeoffs between security and scalability, deanonymization, and misaligned incentives for miners and validators. Intermediation risks include inadequate resources or capabilities for risk mitigation, inability to absorb financial shocks, and bankruptcy/insolvency.

The report asserts that some risk arises from deliberate noncompliance with existing regulation but also from gaps and lack of clarity in the current framework for financial regulation, supervision, and enforcement as it applies to crypto-assets. In that vein, the report makes the following recommendations:

- U.S. regulatory and law enforcement authorities should pursue “vigilant monitoring” of the crypto-asset sector, aggressively pursue investigations, and expand and increase investigations and enforcement, particularly into misrepresentations made to consumers and investors;

- Agencies should review existing regulations and clarify regulatory requirements applicable to crypto-asset products and services, and should act in collaboration with each other while providing guidance in plain language; and
- Agencies should provide education to consumers and investors.

Treasury also issued a report, titled “[Action Plan to Address Illicit Financing Risks of Digital Assets](#)” (“Illicit Financing Strategy”), which outlines priorities and action items to ensure that the U.S. government modernizes the U.S. Department of Treasury’s anti-money-laundering/countering-the-financing-of-terrorism (“AML/CFT”) regime to keep abreast of structural and technological changes to the financial services and markets that result from the increasing issuance and use of digital assets.

Treasury’s Illicit Financing Strategy identifies illicit finance and national security risks and proposes a number of action items to address those risks. However, most of the action items are presented in the Illicit Financing Strategy at a high level of generality, and will have to be fleshed out by Treasury, FinCEN, and others going forward before the industry can or should take concrete action in response.

The identified risks are as follows: money laundering, proliferation financing, terrorist financing, cross-border nature and gaps in AML/CFT regimes across countries, anonymity-enhancing technologies, disintermediation, and virtual asset service provider (“VASP”) registration and compliance obligations. Treasury identifies a number of go-forward action items for combating and mitigating these identified risks, including: monitoring emerging risks; improving global AML/CFT regulation and enforcement; updating Bank Secrecy Act regulations; strengthening U.S. AML/CFT supervision of virtual asset activities; holding cybercriminals and other illicit actors accountable; engaging with the private sector; supporting U.S. leadership in financial and payments technology; and advancing work on a CBDC, in case one is determined to be in the national interest.

DEPARTMENT OF JUSTICE

As with the other reports discussed in this *White Paper*, the report of the Attorney General on “[The Role of Law Enforcement In Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets](#)” was produced in response to the EO. The report gives a brief taxonomy of criminal activity related to digital assets, but—at the direction of the EO—focuses mainly on the role of law enforcement in identifying and investigating crime related to digital assets. The report also adds several potential legislative and regulatory recommendations that could “enhance” DOJ’s efforts to disrupt and prosecute digital asset-related criminal activity. Each section is summarized below.

The report begins by noting that the majority of relevant activity resides in three categories: (i) digital assets as a means of payment for or to facilitate criminal activity; (ii) digital assets as a means of concealing criminal activity; and (iii) crimes involving the digital asset ecosystem. The report also flags an emerging area of concern—the rise of decentralized finance (“DeFi”). While there is no agreed-upon definition of “DeFi,” in the context of DOJ enforcement, it broadly refers to digital asset protocols and platforms that allow for some form of automated peer-to-peer transactions—usually through the use of smart contracts based on blockchain technology. DOJ is particularly concerned regarding these platforms’ application to fraud, investor and consumer protection, and market integrity. Under the DeFi umbrella, the report also notes that the rise of NFTs presents an opportunity for similar exploitation.

With respect to the role of law enforcement, the report notes recent multi-agency efforts to crack down on the illicit use of digital assets, including classic cases like the Silk Road and DOJ’s Digital Currency Initiative. The report continues by outlining numerous divisions at DHS, Treasury, and the Secret Service charged with varying duties in monitoring and investigating fraud and other criminal activity related to digital assets. After briefly discussing a particular example involving \$10 million in bitcoin, the report concludes with a brief overview of other enforcement mechanisms arising from the SEC, CFTC, CFPB, OCC, FDIC, FTC, and other private-sector partnerships.

Lastly, the report outlines a laundry list of possible regulatory moves that would enhance law enforcement’s ability to crack down on illicit digital asset activity. The report designates each with varying levels of priority. DOJ’s top priority is an extension of the existing prohibition against disclosing subpoenas to VASPs that operate as money-services businesses. In addition, DOJ also recommends strengthening federal law prohibiting the operation of an unlicensed money-transmitting business and extending the statute of limitations for crimes involving digital assets from five to 10 years. Lower priorities include supporting legislation designed to address the challenges in gathering evidence of such crimes and stronger penalties to further deter criminal digital asset activity.

DEPARTMENT OF COMMERCE

In the Department of Commerce’s report on “[Responsible Advancement of U.S. Competitiveness in Digital Assets](#),” Commerce sets forth broader conceptual frameworks, with fewer specific recommendations. And Commerce regularly defers to other departmental reports that are discussed above. Commerce’s framework sets forth four categories of actions: (i) regulatory approaches; (ii) international engagement; (iii) public–private engagement; and (iv) research and development.

Regulatory Approaches

Commerce takes the position that the SEC is already attempting to apply existing financial regulations to digital assets, and Commerce believes this is critical to future success: “Continued and regular enforcement of applicable financial laws and regulations is a foundational principle of U.S. competitiveness in financial services, including digital assets.” Moreover, “Commerce endorses regulators’ existing approach that both ensures regulation of the financial sector, including through application of existing law, and responsible innovation that identifies and mitigates risks prior to launch.”

International Engagement

Commerce recommends that federal departments and agencies should “continue to engage internationally to promote development of digital asset policies and CBDC technologies consistent with U.S. values and standards.” Commerce also recommends engagement with the Organization for Economic Cooperation and Development, multilateral development banks, and Asia-Pacific Economic Cooperation.

Public–Private Engagement

Commerce recommends a number of key issues that warrant public–private engagement: (i) an advisory committee; (ii) consumer and investor protection and education; (iii) diversity, equity, and inclusion; (iv) workforce development; (v) payment system modernization; (vi) sustainability; and (vii) accurate and complete economic statistics on economic activity.

Research and Development

Commerce notes the role of federal agencies in foundational research, and recommends continued promotion of research and development in financial technologies and digital assets to continue U.S. technological leadership.

FINANCIAL STABILITY OVERSIGHT COUNCIL

The Financial Stability Oversight Council’s (“FSOC”) [“Report on Digital Assets Financial Stability Risks and Regulation”](#) assesses the extent to which digital assets might pose systemic risks to the financial system.

The report begins by defining the scope of digital assets—which it defines as CBDCs and crypto-assets. The report focuses primarily on the latter, which it defines as private-sector digital assets that depend primarily on cryptography and distributed ledger or similar technology. Two primary examples, therefore, would be Bitcoin and Ethereum. The report also discusses key technological developments

and financial innovations and market developments in this space, including the market capitalization peak of \$3 trillion in November 2021 to its current level of around \$900 billion.

The report next discusses potential financial stability risks. Those risks are, for the moment, tempered by the lack of significant interconnections between the crypto-asset ecosystem and the traditional financial system. Those interconnections could, however, rapidly grow as the crypto-asset ecosystem continues to evolve. Thus, the report assesses the vulnerabilities within that ecosystem, such as drops in asset prices, financial exposures via interconnections within the ecosystem, operational vulnerabilities, funding mismatches, the risk of runs on assets, and the use of leverage. The report also notes that, interconnections aside, crypto-assets could pose financial stability risks if they were to attain a large enough scale.

The report also discusses regulation of crypto-assets in the context of the above-identified risks. The report observes that the “current regulatory framework, along with the limited overall scale of crypto-asset activities, has helped largely insulate traditional financial institutions from financial stability risks associated with crypto-assets,” before going on to discuss various regulators and regulations, and their (potential) applicability to crypto-assets.

The report’s more interesting aspects reside in the FSOC’s recommendations. There, the report begins by noting that “large parts of the crypto-asset ecosystem are covered by the existing regulatory structure.” That may come as a bit of a surprise, given the ongoing legal battles concerning whether certain crypto-assets are securities, commodities, or something else altogether. It is, however, consistent with recent regulatory enforcement actions in this space, where both the SEC and the CFTC have been increasingly aggressive in asserting their authority over crypto-asset ecosystem participants. The report then notes the “gaps” in the regulation of crypto-asset activities that would benefit from additional attention:

- Limited direct federal oversight of the spot market for crypto-assets that are not securities;
- Opportunities for regulatory arbitrage; and
- Whether vertically integrated market structures can or should be accommodated under existing law and regulations.

The first gap primarily concerns, in the report’s eyes, spot markets for bitcoin “and possibly other crypto-assets that are not securities.” By the report’s own assessment, this market is rather limited. But the report urges additional regulation to “ensure orderly and transparent trading, to prevent conflicts of interest and market manipulation, and to protect investors and the economy more broadly.”

The second gap, relating to regulatory arbitrage, characterizes optionality in the existing U.S. regulatory framework as a design defect rather than an intentional feature to permit innovation. FSOC states that opportunities for regulatory arbitrage can occur “when the same activity can be carried out lawfully under more than one regulatory framework.” This fact is, of course, a hitherto noncontroversial hallmark of the U.S. banking system, in which banks may choose to be chartered under state or federal law and from a variety of different banking charters, for example. But the FSOC views this flexibility as creating opportunities for crypto-asset providers to “provide financial services that resemble services provided by banks, traditional securities intermediaries, or other financial institutions, but without being subject to, or in compliance with, the same standards and obligations.”

The report therefore urges regulators to coordinate with one another in their supervision of crypto-asset entities, especially when “different entities with similar activities may be subject to different regulatory regimes or when no one regulator has visibility across all affiliates, subsidiaries, and service providers of an entity.” In a similar vein, the report recommends that the FDIC, FRB, OCC, and state bank regulators use their existing authority to review services provided to banks by crypto-asset service providers. The report also recommends that Congress pass legislation that would create: (i) a comprehensive prudential framework for stablecoin issuers; and (ii) a supervisory framework where regulators have visibility into the activities of all the affiliates and subsidiaries of crypto-asset entities.

The third gap, relating to vertically integrated market structures, largely concerns recent requests by some market participants to disintermediate certain aspects of the market for crypto-assets. Specifically, these participants seek to provide direct retail access to investors. The report’s primary concerns stem from consumer protection and managing the risk associated with the leverage or credit offered to retail investors. The report draws particular attention to the practice of managing risk by marking positions to market on a very frequent basis and conducting automatic liquidations where margin calls go unmet. While this may be an effective risk management tool, exposing retail investors to rapid liquidations raises its own set of concerns around disclosures, education, and potential conflicts of interest.

The report is, in some ways, more notable for what it does not say or do. It does not, for instance, provide any additional clarity on whether crypto-assets are securities, commodities, or something else. It also does not call for dramatic regulatory changes. Rather, it essentially calls on the member agencies to keep doing what they are doing. That posture would seem to benefit entities already within the regulatory perimeter, which can explore crypto-asset services and products within a risk management and control framework with which regulators are more comfortable and, in so doing, shape regulatory views on these activities to their advantage. In contrast, firms outside of or unable to gain access to the regulatory perimeter, including would-be “disruptors” to incumbent providers, are more likely to find themselves in an adversarial relationship with regulators.

ENDNOTES

- 1 News reports indicate that the Department of Justice issued a legal opinion on the Federal Reserve’s authority regarding a CBDC, but those legal views have not yet been shared with Congress (or the public).
- 2 White House Office of Science and Technology Policy, *Climate and Energy Implications of Crypto-Assets in the United States* 13 (Sept. 8, 2022).
- 3 *Id.*
- 4 *Id.* at 15.
- 5 *Id.* at 21.
- 6 *Id.* at 27.
- 7 *Id.* at 28.
- 8 *Id.* at 29.
- 9 *Id.*



OCTOBER 2022 COMMENTARY

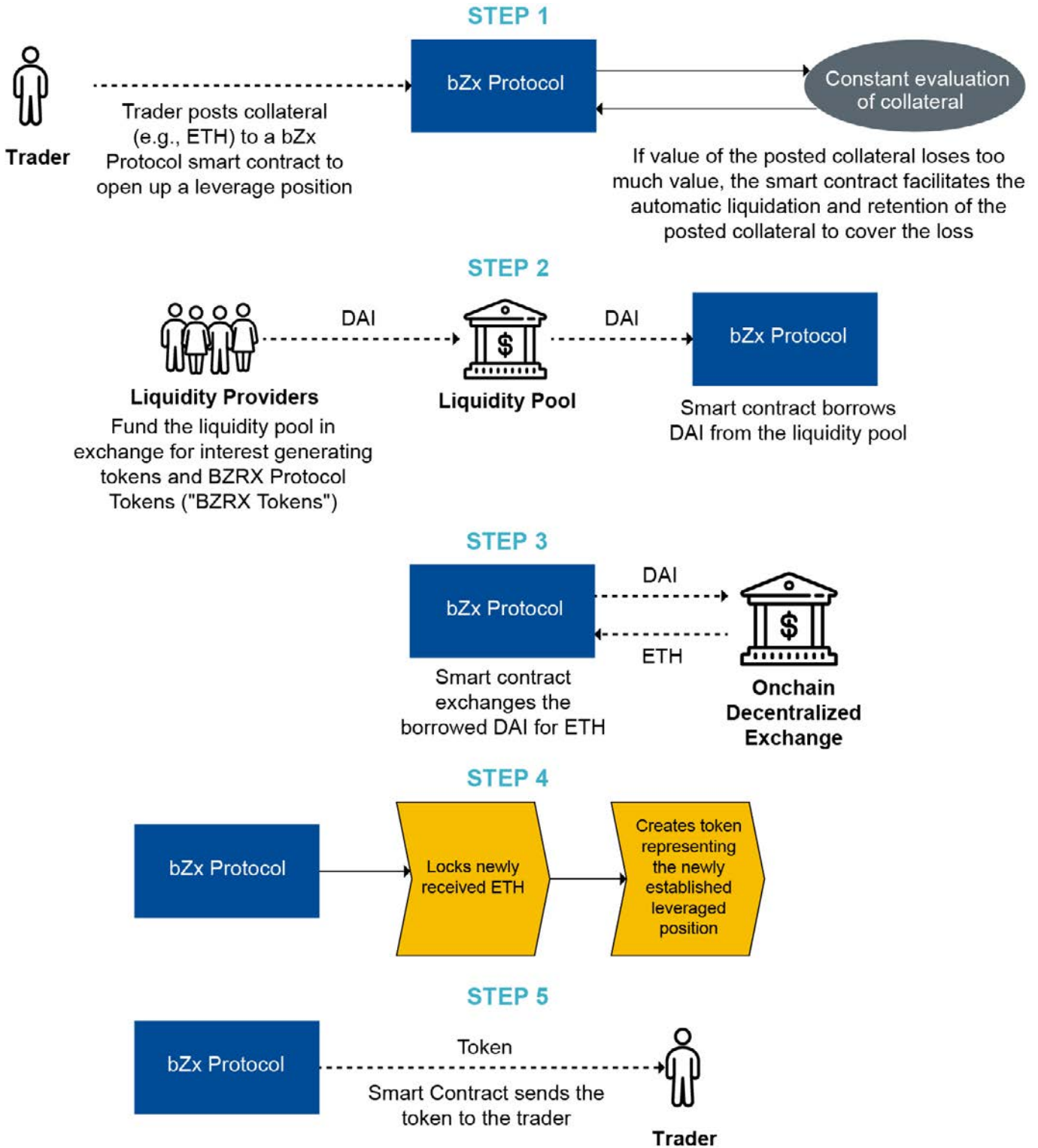
The Situation: Under the existing legal regimes, decentralized autonomous organizations (“DAO” or “DAOs”) have been viewed as a way to hedge against regulatory action by way of a decentralized structure. The Commodity Futures Trading Commission’s (“CFTC”) recent and first attempt to impose liability on a DAO and its members disrupts that assumption and helps provide insight into the future of decentralized finance (“DeFi”) in the United States.

The Result: The CFTC’s recent [Order](#) found bZeroX, LLC and its two founders violated the Commodity Exchange Act (“CEA”) by unlawfully engaging in activities that could lawfully be performed only by a registered futures commission merchant (“FCM”) or designated contract market (“DCM”), and contended that individual DAO members that voted on governance measures are jointly and severally liable for debts of the DAO as an unincorporated association.

Looking Ahead: The CFTC’s complaint against Ooki DAO (the successor to bZeroX’s DAO that operated the same software protocol as bZeroX) charged the same violations that the CFTC found in the Order. Even if the federal court does not adopt the CFTC’s “unincorporated association” theory of liability for DAO voters, its very prospect seems likely to chill DeFi participation in the United States in the near future.

On September 22, 2022, the CFTC filed an Order announcing it had reached a settlement with bZeroX, LLC and its two founders, Kyle Kistner and Tom Bean (collectively, “Respondents”). The settlement relied in part on imposing controlling person liability on the founders, under Section 13(b) of the CEA, for bZeroX’s violations of CEA Sections 4(a) and 4(d)(1). The Order found that the Respondents violated the CEA by operating an Ethereum-based DeFi platform (“bZx Protocol”) that accepted orders and facilitated tokenized leveraged retail trading of virtual currencies such as ETH, DAI, and others.

According to the Order, the bZx Protocol permitted users to contribute margin to open leveraged positions, the ultimate value of which was determined by the price difference between two digital assets from the time the position was established to the time it was closed. In doing so, the CFTC found, the Respondents “unlawfully engaged in activities that could only lawfully be performed by a designated contract market (“DCM”) and other activities that could only lawfully be performed by a registered futures commission merchant (“FCM”).” The CFTC also found, by Respondents failing to conduct know-your-customer diligence on customers as part of a customer identification program, as required of both registered and unregistered FCMs, that the Respondents violated CFTC Regulation 42.2. Below is an illustration of how the bZx Protocol operated.



Concurrently with the Order, the CFTC filed a [complaint](#) against Ooki DAO, the successor to the bZx DAO—a DAO comprising bZx Protocol token holders that Respondents had transferred control to following a series of hacks in 2020 and early 2021. The Ooki DAO complaint charges the same violations in which the CFTC found in the Order that the Respondents had engaged. The CFTC characterized Ooki DAO in the Order as “an unincorporated association comprised of holders of Ooki DAO Tokens who vote those tokens to govern (e.g. to modify, operate, market, and take other actions with respect to) the [Ooki] Protocol.” In the Order, the CFTC stated that “[i]ndividual members of an unincorporated association organized for profit are personally liable for the debts of the association under principles of partnership law.”

As discussed in Commissioner Mersinger’s dissent (“Mersinger’s Dissent”), neither the CEA nor the CFTC have ever defined a DAO. More importantly, although the CFTC has to date settled one action against what it characterized as a DeFi trading platform ([Blockratize, Inc. d/b/a Polymarkets.com](#)), the Ooki DAO complaint is the first time it has attempted to impose liability on a DAO or its members. This was not entirely unexpected. For example, in footnote 63 in [the CFTC’s Digital Asset Actual Delivery Interpretive Guidance](#), the CFTC noted that “in the context of a ‘decentralized’ network or protocol, the Commission would apply this interpretation to any tokens on the protocol that are meant to serve as virtual currency as described herein” (emphasis added).

The CFTC added that “[i]n such instances, the Commission could, depending on the facts and circumstances, view ‘offerors’ as any persons presenting, soliciting, or otherwise facilitating ‘retail commodity transactions,’ including by way of a participation interest in a foundation, consensus, or other collective that controls operational decisions on the protocol, or any other persons with an ability to assert control over the protocol that offers “retail commodity transactions,” as set forth in CEA section 2(c)(2)(D).”

Former CFTC Commissioner Berkovitz also [stated in a 2021 speech](#) that “[n]ot only do I think that unlicensed DeFi markets for derivative instruments are a bad idea, I also do not see how they are legal under the CEA.” A few years prior to that, [a CFTC spokesperson stated](#) in response to questions about Augur—a DeFi prediction market offering, among other things, assassination contracts—that “[w]hile I won’t comment on the business model of any specific company, I can say generally that offering or facilitating a product or activity by way of releasing code onto a blockchain does not absolve any entity or individual from complying with pertinent laws or CFTC regulations[.]” The CFTC’s unincorporated association theory of liability is not unique: [The SEC’s 2017 DAO Report](#) pointed out that Section 3(a)(1) of the Securities Exchange Act of 1934 defines an “exchange”

as “any . . . association, or group of persons, whether incorporated or unincorporated. . . .”

However, as noted in Mersinger’s Dissent, “[d]efining the Ooki DAO unincorporated association as those who have voted their tokens inherently creates inequitable distinctions between token holders.” For instance, a single vote on a generic governance proposal having nothing to do with the CEA or CFTC rules could unknowingly subject token holder A to membership in the unincorporated association, as defined by the CFTC, and assumption of personal liability, while token holder B escapes membership/liability by virtue of incidentally neglecting to vote. Even if token holder A had voted directly against the alleged unlawful actions, it could still face joint and several liability for the full legal claim against the DAO.

Moreover, as noted in Mersinger’s Dissent, the CEA “sets out three legal theories that the Commission can rely upon to support charging a person for violations of the CEA or CFTC rules committed by another: (i) principal-agent liability; (ii) aiding-and-abetting liability; and (iii) control person liability.” The CFTC has pursued the aiding-and-abetting theory in somewhat similar circumstances. In January 2018, the [CFTC charged Jitesh Thakkar and Edge Financial Technologies, Inc.](#)—a company Mr. Thakkar founded and for which he served as president—with aiding and abetting Navinder Sarao in engaging in a manipulative and deceptive scheme by designing software used by Mr. Sarao to spoof mini S&P futures contracts.

Mr. Thakkar was also named in a criminal complaint brought by the Department of Justice (“DOJ”) related to the same conduct on charges of conspiracy to commit spoofing as well as aiding and abetting spoofing. The CFTC agreed to stay its case during the pendency of the criminal matter. After the DOJ’s charges were [dismissed with prejudice](#) in April 2019, the CFTC resumed its civil action against Mr. Thakkar in September 2019. One year later, the CFTC ultimately entered into a [consent order for permanent injunction](#) with Mr. Thakkar’s company, Edge Financial Technologies, Inc. The order included findings tracking the allegations in the CFTC’s complaint, a permanent injunction against aiding-and-abetting violations of CEA Sections 4c(a)(5)(C) (spoofing) and 6(c)(1) (manipulation) and CFTC Regulation 180.1(a)(1) and (3) (relating to the use of a manipulative and deceptive device, scheme, or artifice to defraud), and an order of disgorgement and civil monetary penalty totaling \$72,600.

While Commissioner Mersinger may have wished to hold only the founders liable for DAO-related activity, it would seem that the Commission is not so inclined and may wish to send a message to those who would trade on unlawful venues, even though the Commission usually seeks to protect such persons against misconduct arising from trading

on such venues. In the case of DAOs, the Commission may take the view that such persons operate and control the venues, in some ways.

Even if this “unincorporated association” theory of DAO liability is not ultimately endorsed by a federal court, this ruling will likely result in protocol founders increasingly choosing to maintain anonymity and/or operate offshore. This could result in decreased availability of DeFi derivatives trading to U.S. persons and, if DeFi derivatives trading remains available to U.S. persons from offshore, greater extraterritorial enforcement efforts by the CFTC.

More broadly, this action is a warning that some regulators view unregulated DeFi trading activity as incompatible with existing legal structures, notwithstanding the argument that DAO token holders are engaged in active management of the protocol and so are not dependent on the efforts of others under *SEC v. Howey Co.* Footnote 10 of the *bZeroX Order* sounds loud and clear on this point, warning that “[i]t was (and remains) Respondents’ responsibility to avoid unlawfully engaging in activities that could only be performed by registered entities and, should they ever wish to register, to structure their business in a manner that is consistent with Commission registration requirements” (emphasis added).

Incidentally, the message in that footnote is the answer to [questions raised](#) by some as to how crypto businesses are to operate when their very structures seem incompatible with existing regulatory schemes. [More recently, SEC Chairman Gensler expressed a similar sentiment](#), stating that “[t]he commingling of the various functions within crypto intermediaries creates inherent conflicts of interest and risks for investors. Thus, I’ve asked staff to work with intermediaries to ensure they register each of their functions— exchange, broker-dealer, custodial functions, and the like—which could result in disaggregating their functions into separate legal entities to mitigate conflicts of interest and enhance investor protection” (emphasis added).

DAOs possess many novel qualities not present in traditional corporate structures—transitory ownership tied to a tradeable token, user ownership and governance, and operations conducted by, in some cases, an autonomous smart contract code. While encompassing only active voters in the instant case, the CFTC’s language in its complaint against Ooki DAO seems to suggest that a smart contract protocol running programs deemed to violate regulations could continuously generate liability for DAO members simply by way of the members having “permitted” transactions executed by such programs. The greater the autonomy and automation of the smart contract underlying the protocol, the less sense attaching joint and several liability to DAO members arguably makes. Automating protocol functions to reduce

the necessity of DAO member input is another foreseeable result of the CFTC’s position.

While the potential for DAOs to avoid classification of their tokens as securities has reinforced the use of a fully decentralized structure lacking legal form, the countervailing risk of a general partnership—and especially voting member liability as an “unincorporated association”—will likely lead to increased use of traditional [legal entities](#) in DAO formation and governance for the DAO and individual participants alike. For all of the innovation the unique traits of a DAO allows, it is becoming increasingly clear that existing regulations will demand the rails of legal personhood to achieve compliance.

Whether a “test case” ramping up to something larger or simply a reminder to founders—or those who otherwise seek to legally or practically distance themselves from the DAOs that they create (e.g., by the developers “[giv\[ing\] up ownership over the ‘escape hatch’ function, which would allow a designated party to shut the system down](#)”)—that DAOs cannot be used as a tool to evade regulatory action, the outcome of the CFTC’s lawsuit against Ooki DAO is one to closely watch as a harbinger for DeFi as a whole. User ownership and voted token participation in DAOs—while not the regulatory shield some might wish it to be—is an idea unlikely to go away anytime soon.

THREE KEY TAKEAWAYS

1. The CFTC’s Ooki DAO complaint serves as warning to the DeFi market to conform to the existing legal structure and could place a premium on founder anonymity or reduce DeFi protocol access for U.S. citizens. This outcome could result in further extraterritorial enforcement efforts by the CFTC as protocols shift operations overseas to avoid unlawfully engaging in activities allowable only by registered entities.
2. The CFTC finding active voters personally liable under principles of partnership law will likely cause DAOs to increase their levels of autonomy and automation, which would reduce the necessity of DAO member input and make the argument attaching joint and several liability to DAO members less viable.
3. The risk of DAOs’ classification as general partnerships and individual voting members’ potential personal liability under an unincorporated association theory will likely lead to the increased use of traditional legal entities in DAO formation and governance.



AUGUST 2022 COMMENTARY

The Situation: Following the release of the Responsible Financial Innovation Act (the “Lummis-Gillibrand Bill”), four senators on the Senate Committee on Agriculture, Nutrition, and Forestry released their own draft legislation aiming to bring regulatory clarity to the digital asset ecosystem (the “Stabenow-Boozman Bill” or the “Bill”).

The Action: If passed, the Stabenow-Boozman Bill would impact the digital asset ecosystem in several meaningful ways by: (i) providing that the Commodity Futures Trading Commission (“CFTC”), not the Securities and Exchange Commission (“SEC”), would have exclusive jurisdiction over any account, agreement, contract, or transaction involving a digital commodity trade; (ii) providing clarity regarding who would be required to register with the CFTC; (iii) imposing AML compliance obligations under the Bank Secrecy Act on digital commodity platforms; (iv) providing clarity over how a digital commodities platform’s customer assets would be treated in the event of a bankruptcy; (v) expanding the reach of the Commodity Exchange Act (the “CEA”) to include digital commodities; and (vi) preempting state law registration requirements relating to money transmission, virtual currency, and commodity brokers.

Looking Ahead: Further legislation would be required to end the ongoing debate about what is a digital commodity and what is a digital security, as the Stabenow-Boozman Bill does not bring definitional clarity to this critical issue. Future CFTC rulemaking would also be required to address lending of digital commodities, consumer protection, and commingling of customer property.

CFTC JURISDICTION AND THE DEFINITION OF A DIGITAL COMMODITY

The Stabenow-Boozman Bill's centerpiece is its command that the CFTC “shall have exclusive jurisdiction over, any account, agreement, contract, or transaction involving a digital commodity trade.” Although the grant of jurisdiction is clear, the linkage to “digital commodities” is an Achilles heel of ambiguity and an invitation to mischief. The Stabenow-Boozman Bill defines a digital commodity as “a fungible digital form of personal property that can be possessed and transferred person-to-person without necessary reliance on an intermediary,” which would seem to exclude NFTs. It expressly includes “property commonly known as cryptocurrency or virtual currency, such as Bitcoin and Ether.” But it also expressly *excludes* such things as an interest in a physical commodity and—significantly—securities. And therein lies the problem. The SEC has consistently taken the position that most digital assets, setting aside Bitcoin and Ether, are securities. The SEC’s complaint alleging insider trading at Coinbase— *SEC v. Wahi et al.*, Case No. 2:22-cv-01009 (W.D. Was.)—is the most-recent example of that view. In it, the SEC alleges that nine different digital assets that can be traded on Coinbase’s platform are, in fact, securities that must be registered in accordance with the securities laws.

Carving out securities from the CFTC’s jurisdiction over digital commodities would not necessarily be problematic if the Bill attempted to distinguish digital assets that are securities from those that are not. By not doing so, however, the Stabenow-Boozman Bill relies on courts and the SEC to set the boundaries for which tokens can be considered commodities. History teaches that it is unlikely such a process would be smooth or painless. Given the SEC’s recent stance on the matter, in practice, the Stabenow-Boozman Bill would likely grant the CFTC clear jurisdiction over trades in Bitcoin and Ether, and nothing else. That would not seem to be the intent, given the Stabenow-Boozman Bill’s general reference to “cryptocurrency and virtual currency,” but it is a foreseeable result under the present circumstances.

Whether a digital asset is a security or a commodity is the fulcrum on which fundamental questions of regulatory authority rest. Although, based on some combination of CFTC settlement orders, federal court decisions, and statements by CFTC and SEC Chairmen, the industry has become comfortable recognizing Bitcoin (and, to a lesser extent, Ether) as a commodity, the commodity vs. security issue looms unresolved for many other digital assets. As a result, in order to provide clarity and certainty to these markets, it is imperative that future legislation in this space address this issue, by clearly defining digital assets as commodities or securities (or some of each) or by providing a means for easily determining how a digital asset will be classified and—by extension—regulated.

Digital Commodities Market Participants and Other Key Provisions

Another prominent feature of the Stabenow-Boozman Bill is its creation of various digital commodities market participants. These include digital commodities brokers, custodians, dealers, and trading facilities (along with “associated persons” of brokers and dealers, who are also required to register with the CFTC). The Stabenow-Boozman Bill awkwardly defines a “digital commodity platform” to include all of the foregoing entities, notwithstanding the disparate services that they provide and that a “platform” is usually thought of as an exchange or the like. And the definitions ascribed to these platforms generally align with the roles such entities play in traditional financial markets. It is worth noting, however, that the definition of digital commodity custodian excludes federally-insured depository institutions and credit unions. As a result, to the extent such entities provided digital commodities custody services, they would not need to register with the CFTC, but would still be permitted to provide such services pursuant to guidance provided by the Office of the Comptroller of the Currency. Further, the definitions for digital commodities brokers, dealers, and trading facilities do not include “a person solely because that person validates digital commodity transactions,” i.e., miners.

The Stabenow-Boozman Bill also states that the CFTC may prescribe rules and regulations permitting an entity to register as more than one digital commodities platform, including registered entities like swap dealers and futures commission merchants; and that a digital commodity platform registered with the CFTC may also be registered with the SEC as an exchange, broker, dealer, or another trading platform. Accordingly, a single entity could conceivably play multiple roles within the digital assets, physical commodities, and securities markets.

The Stabenow-Boozman Bill next outlines “Core Principles” for digital commodities platforms in general, and for trading facilities, brokers, and dealers in particular. These are similar in many respects to the “Core Principles” proposed for digital asset exchanges in the Lummis-Gillibrand Bill. One important similarity is the provision regarding the “Treatment of Customer Assets” applicable to all digital commodity platforms. As in the Lummis-Gillibrand Bill, the Stabenow-Boozman Bill proposes a disintermediated framework for transacting in digital commodities that does not include a provision requiring platforms to hold customer property with a Futures Commission Merchant.

The Stabenow-Boozman Bill also takes a page from the Lummis-Gillibrand Bill in limiting brokers, dealers, and trading facilities to transacting only in “transactions” or “digital commodities” that are not “readily susceptible to manipulation.” Unlike the Lummis-Gillibrand Bill, however, the Stabenow-Boozman Bill makes no attempt to define

what “readily susceptible to manipulation” means, or the factors one would consider when making such a determination, though presumably the CFTC could look to the factors that it considers when reviewing contracts on futures exchanges.

The latter point reflects a broader theme seen throughout the Stabenow-Boozman Bill. Rather than address every issue through statutory language, the Stabenow-Boozman Bill consistently contemplates future rulemaking to be conducted by the CFTC on specific matters. For instance, the Stabenow-Boozman Bill instructs that the CFTC may adopt rules or regulations regarding significant issues such as margined or leveraged trading in digital commodities, lending of digital commodities, consumer protection (including marketing and advertising standards), and commingling of customer property. Given that the Commission can consider whether a digital asset listed for trading on a digital commodity trading facility is, in fact, not readily susceptible to manipulation, it would seem that the Bill would rely on the CFTC’s expertise in addressing this issue, too.

Other significant provisions in the Stabenow-Boozman Bill include the following:

- **Bankruptcy:** The Stabenow-Boozman Bill would provide much-needed clarity on the question of how a digital commodities platform’s customer assets would be treated in the event of a bankruptcy, by extending relevant provisions of the Bankruptcy Code to digital commodities transactions, thereby ensuring protections similar to those provided for traditional commodities contracts.
- **Anti-Money Laundering:** The Stabenow-Boozman Bill would establish digital commodities platforms as “financial institutions” under the Bank Secrecy Act, thereby obligating such platforms to submit reports of suspicious transactions, and to adhere to other AML compliance obligations.
- **Extra-Territorial Effect:** The Stabenow-Boozman Bill would have a worldwide reach, in that its provisions on digital commodities would extend to any activities that (i) have a reasonably foreseeable significant effect within the United States; ii) involve the offer, execution, or confirmation of a digital commodities transaction with any United States person or the conducting of any office or business anywhere in the United States (including a territory or possession of the United States). In contrast, the current CEA cross-border jurisdiction provision related to swaps (i.e., Section 2(i)) only applies the CEA extraterritorially to activities that “have a *direct and significant* connection with activities in, or effect on, commerce of the United States.”
- **State Law Preemption:** The Stabenow-Boozman Bill would preempt state law registration requirements relating to money transmission, virtual currency, and commodity brokers, as well as state law compliance requirements relating to money transmission, virtual currency, and commodity brokerage.
- **Energy Consumption:** The Stabenow-Boozman Bill would respond to concerns regarding the amount of energy expended by—and the carbon footprint associated with—the digital assets space by requiring the CFTC to prepare a report on the energy consumption and sources of energy associated with the creation and transfer of the most widely traded digital commodities. The report would be published on the CFTC’s website and periodically updated.

Notably, the Stabenow-Boozman Bill does not attempt to take on such topics as the tax treatment of digital assets, issuance of stablecoins, or disclosures to be provided to the SEC.

CONCLUSION

In sum, although the Stabenow-Boozman Bill is significantly narrower in scope than the Lummis-Gillibrand Bill, it nonetheless provides a comprehensive regulatory framework for overseeing transactions in digital commodities and supervising several market participants in that space. And while it embraces an approach to the digital commodities market that would promote efficiency and reduce transaction time and costs, it does not attempt to define the digital assets that would be traded within that market. In its present form, for all practical purposes, the Stabenow-Boozman Bill appears to apply most clearly to Bitcoin and Ether, leaving important issues about other cryptocurrencies and virtual currencies not clearly resolved. As a result, amendments to the Stabenow-Boozman Bill or additional legislation altogether would be needed to bring more certainty to this space.

THREE KEY TAKEAWAYS

1. The Stabenow-Boozman Bill joins a growing list of legislative initiatives seeking to bring clarity to the laws governing digital assets by granting the CFTC exclusive jurisdiction over digital commodities. The Stabenow-Boozman Bill, however, does not eliminate the ambiguity present in the digital asset space—what digital asset is a commodity and what is a security—and therefore provides little real world guidance on establishing what falls within the CFTC’s exclusive jurisdiction.
2. The Stabenow-Boozman Bill does not define several key features and participants in the digital assets space and instead contemplates significant, broad rulemaking by the CFTC in the future.
3. While the Stabenow-Boozman Bill attempts to bring regulatory certainty to the digital asset space, the Bill’s limited scope means that, if it is enacted, additional piecemeal legislation may be required to provide a comprehensive regulatory framework.



DIGITAL ASSETS DEFINED: HOW LUMMIS-GILLIBRAND WILL SHAPE THE COMING FINTECH DEBATE

AUGUST 2022 WHITE PAPER

On June 7, 2022, U.S. Senators Kirsten Gillibrand (D-NY) and Cynthia Lummis (R-WY) introduced the Responsible Financial Innovation Act (“RFIA” or the “Bill”), which proposes a regulatory framework for digital assets across nine titles calling for “Responsible” activity in taxation, consumer protection, and securities, commodities, payments, and banking innovation. The proposed legislation is a comprehensive attempt to bring stability to a rapidly growing and often volatile industry.

If passed, it would affect the federal regulatory landscape in a way not seen since the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010. The Bill seeks to amend bedrock federal statutes, including, without limitation, the Securities Exchange Act of 1934 and the Commodity Exchange Act, in order to clarify regulatory roles for the Securities and Exchange Commission (“SEC”) and the Commodity Futures Trading Commission (“CFTC”), and solicits reports and rulemaking from those agencies and numerous others.

Although it is unlikely that the Bill will be passed in its current form or in the current Congress, it is a first step to the development of bipartisan legislation on this important topic.

In this *White Paper*, we discuss the Bill’s most significant implications, such as its attempt to resolve important questions concerning the legal status of digital assets, and allocation of regulatory authority. In a series of follow-on papers, we will explore the Bill’s treatment of four critical areas:

- The Regulatory Jurisdiction of the SEC and the CFTC
- Regulatory Changes Regarding Financial Instruments and Institutions
- Consumer Protection, Data Privacy, and Cybersecurity
- Effects on State Regulation, Tax, and Bankruptcy

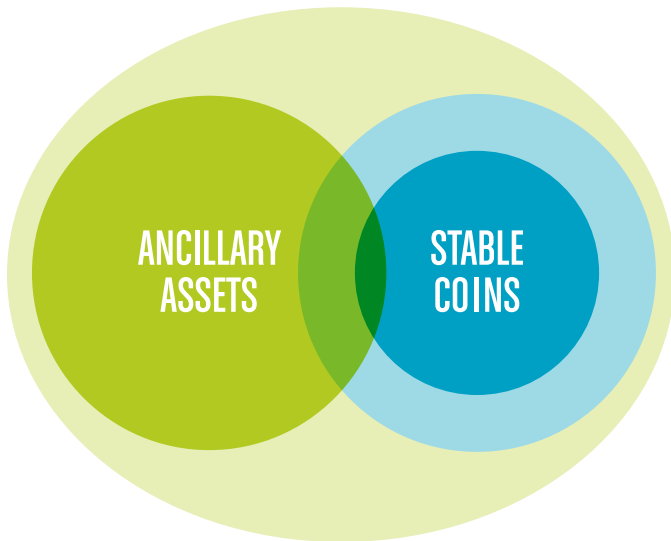
Although the Bill’s primary effects may be evident, the secondary and tertiary ramifications may take years to become apparent, as agencies introduce proposed rules and the domino effects of amending a vast array of statutes come to the fore. As a result, these observations too likely will evolve over time.

TAXONOMY

At the outset, the Bill defines two key overarching terms: “digital asset” and “digital asset intermediary.” A “digital asset” is defined as a natively electronic asset that confers

economic, proprietary, or access rights or powers, and is recorded using cryptographically secured distributed ledger technology or any similar analogue.¹ The definition expressly includes “virtual currency,” “ancillary assets,” and “payment stablecoins,” each of which the Bill separately defines.

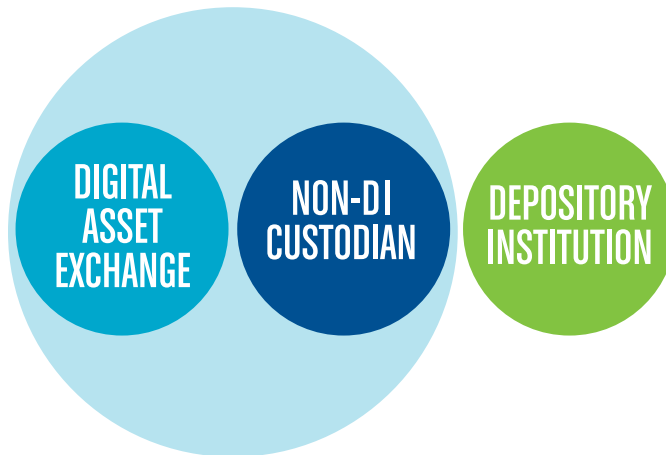
Digital Assets



The definition therefore covers well-known digital assets such as bitcoin, Ether, and NFTs, as well as governance tokens, pegged stablecoins, and native distributed ledger technology assets that may exist in the future.

A “digital asset intermediary” is defined as a person that is not a depository institution² and that: (i) holds (or is required by law to hold) a license, registration, or other similar authorization specified by the Bill or a series of other enumerated acts; (2) may conduct market activities relating to digital assets; or (3) issues a payment stablecoin. This definition includes a licensed “digital asset exchange,” which the Bill defines as “a centralized or decentralized platform which facilitates the transfer of digital assets”³ and “a trading facility that lists for trading at least one digital asset.”⁴ But a “digital asset intermediary” could also include other market participants that perform services relating to digital assets—such as digital asset service providers, custodians, and staking-as-a-service businesses—other than depository institutions.

Digital Asset Intermediary



DEPTH AND BREADTH

The Bill seeks to integrate digital assets into existing law through amending existing statutes, and expanding or clarifying the roles of existing federal regulators. In doing so, the Bill leaves few major statutes or regulatory agencies relating to the financial markets untouched:

Amended Acts	Affected Agencies / Regulators
Securities Exchange Act of 1934	Securities Exchange Commission
Commodity Exchange Act	Commodity Futures Trading Commission
Gramm-Leach-Bliley Act	Consumer Financial Protection Bureau
Internal Revenue Code of 1986	Internal Revenue Service
Bank Holding Company Act of 1956	Office of the Comptroller of the Currency
Federal Reserve Act	Federal Reserve Board of Governors
Anti-Money Laundering Act of 2020	FinCEN
Federal Deposit Insurance Act	Federal Deposit Insurance Corporation
Riegle Community Development and Regulatory Improvement Act of 1994	Department of the Treasury
Various other portions of the U.S. Code at Titles 12 (Banks and Banking) and 31 (Money and Finance)	

As a result, the Bill would affect practitioners in a broad swath of practice areas, including but not limited to tax, bankruptcy, banking, commodities, securities, cybersecurity, and consumer protection.

SIGNIFICANT TAKEAWAYS

CFTC vs. SEC

Perhaps the most significant aspect of the Bill is that it settles questions about the division of authority between the SEC and CFTC with respect to digital assets. As this space has grown in size and prominence, the dominant question has been whether a digital asset is a commodity or a security. In 2018, former SEC Chairman Jay Clayton famously asserted that bitcoin is not a security.⁵ And as far back as 2015, the CFTC stated in an order settling an enforcement action that bitcoin and other virtual currencies are commodities.⁶ In 2016, the CFTC cemented this position in another enforcement action stating that, “bitcoin and other virtual currencies are encompassed in the definition [of commodity] and properly defined as commodities, and are subject as a commodity to the applicable provisions of the [Commodity Exchange] Act and [CFTC] Regulations.”⁷

Nevertheless, although current SEC Chairman Gary Gensler has conceded that bitcoin is not a security,⁸ he has repeatedly contended that the vast majority of digital assets are securities,⁹ and that “[i]t doesn’t matter whether it’s a stock token, a stable value token backed by securities, or any other virtual product that provides synthetic exposure to underlying securities. These products are subject to the securities laws and must work within our securities regime.”¹⁰ On that basis, the SEC has brought numerous enforcement actions against entities in the digital asset space, like Munchee, Inc. and Ripple Labs.

Key Takeaway #1

The Act creates a paradigm in which many digital assets appear to be classified as commodities.

The Bill would moot the debate by granting the CFTC jurisdiction over transactions involving digital assets, with certain exceptions. The Bill excludes from the CFTC’s jurisdiction digital assets that provide the owner with any of the following rights regarding a business entity: (i) a debt or equity interest in that entity; (ii) liquidation rights with respect to that entity; (iii) an entitlement to an interest or dividend payment from that entity; (iv) a profit or revenue share in that entity derived solely from the entrepreneurial or managerial efforts of others; or (v) any other financial interest in that entity.¹¹ These excluded digital assets would be subject to the SEC’s jurisdiction.

On the SEC side, the Bill creates a reporting framework for certain issuers in the digital assets space. Per the Bill, an issuer of a security that provides or proposes to provide any holder of the security with an “ancillary asset” must provide to the SEC initial and periodic disclosures regarding enumerated topics concerning the issuer and the ancillary asset.¹² However, the Bill clarifies that if an issuer complies with these disclosure requirements, the ancillary asset “shall be presumed to be a commodity, consistent with section 2(c)(2)(F) of the Commodity Exchange Act.”¹³

Key Takeaway #2

The Act creates SEC disclosure requirements for issuers of some digital assets called ancillary assets.

On the CFTC side, the Bill grants the Commission “exclusive jurisdiction over any agreement, contract, or transaction involving a contract or sale of a digital asset in interstate commerce, including ancillary assets,” with carveouts for: (i) the reporting requirements just discussed, which “shall remain within the jurisdiction” of the SEC; (ii) nonfungible digital assets; and (iii) certain retail contracts of sale of digital assets that result in actual delivery within two days.¹⁴ The Bill goes on to grant the Commission the power to register and oversee digital asset exchanges that offer or seek to offer a market in digital assets, and to lay out a set of “Core Principles for Digital Asset Exchanges.”¹⁵

In sum, the Bill establishes that the SEC would continue to have oversight authority with respect to securities issuers, including those that provide or offer to provide an ancillary asset in conjunction with the offered security, and creates a set of disclosure requirements concerning such ancillary assets. The Bill also establishes that the CFTC would have exclusive oversight authority with respect to transactions in digital assets, including ancillary assets, that are not securities (i.e., those digital assets granting holders equity-type interests), with the exception of the above-noted carveouts.

Key Takeaway #3

The Act gives the CFTC exclusive jurisdiction over most digital asset transactions. See flowchart attached as Schedule 1.

Ancillary Assets

The Bill’s creation of a class of digital assets defined as “ancillary assets” raises a host of new questions concerning the circumstances in which that classification will apply. News reports indicate that, according to aides to Sens. Gillibrand and Lummis, the Bill “treats all digital assets as ‘ancillary’ unless they behave like a security a corporation would issue to investors to build capital.”¹⁶ That is not all

that surprising because whether something is an ancillary asset hinges on the same inquiry traditionally used to determine whether something is a security: Is it offered or sold in an arrangement or scheme that constitutes an investment contract? Under the *Howey* test, an investment contract exists if there is an “investment of money in a common enterprise with profits to come solely from the efforts of others.”¹⁷ Thus, according to the “Section-by-Section Overview” prepared by Sens. Gillibrand and Lummis, a key question in this regard will be whether the assets “benefit from entrepreneurial and managerial efforts that determine the value of the assets.”¹⁸

Key Takeaway #4

The *Howey* test lives on, and it plays a role in determining whether a digital asset is an ancillary asset.

In the construct described by the Senators’ aides, it would seem that digital assets have one of two fates: They behave like a security and, as such, are themselves securities, or they were offered or sold in connection with the sale of a security and are thus ancillary assets with commodity presumptions. In the former case, the digital asset “security” would be subject to the usual securities registration and reporting requirements, and in the latter case, the digital asset “ancillary asset” would be subject to the proposed disclosure requirements.¹⁹ The SEC would therefore appear to have significant oversight authority in the digital asset ecosystem. That oversight authority could be even greater if the SEC adopts a broad interpretation of the ancillary asset exclusion for digital assets that provide holders with “any other financial interest in that entity,” as such assets would be outside the purview of the CFTC’s authority, and not tradeable on a CFTC-registered digital asset exchange.²⁰

The language of the Bill, however, does not appear to be so deterministic. It would seem to permit the possibility of a third path in which a digital asset is neither a security nor an ancillary asset. A contrary conclusion means that it is impossible to issue a digital asset as part of a scheme or arrangement that does *not* constitute an investment contract. But one can imagine a future digital asset issuance, such as tokenized credit-card or frequent-flyer rewards points, that does not bear the hallmarks of an investment contract or even resemble one at all. One can also imagine that, if the ancillary-asset concept is included in proposed legislation that becomes law, significant efforts will go into identifying a path to issuing digital assets that are tradeable on a CFTC-registered digital exchange, but not subject to the ancillary-asset reporting requirements.

For those digital assets that do fall within the ancillary asset definition, the Bill creates disclosure obligations if, within prescribed time frames, the asset’s average daily trading volume on all spot markets exceeds \$5 million, and an

owner of 10% or more of the equity of the issuer “engaged in entrepreneurial or managerial efforts that primarily determined the asset’s value.” These relatively low thresholds would appear to be designed to ensure that many ancillary assets are subject to the newly enumerated disclosure regime—at least while their value is dependent on the efforts of others with a stake in the issuing entity.

The Bill’s clear delegation of authority to the SEC and CFTC with respect to reporting obligations on ancillary assets and trading of digital assets, respectively, is helpful in light of evolving Supreme Court jurisprudence on the Major Questions Doctrine.²¹ Less helpful is the lingering ambiguity surrounding the ancillary asset exclusions—especially when the ancillary asset definition is the linchpin to presumptive treatment as a commodity eligible for trading on a CFTC-registered exchange. Future token issuers may be concerned that the SEC will interpret the exclusions—particularly the catchall for “any other financial interest”—in a way that deprives many of the tokens found today from treatment as ancillary assets, and instead classifies them as securities. And issuers could not really be faulted for harboring such concerns, given Chairman Gensler’s comments on the topic, and the approach the SEC has taken on enforcement actions in the digital asset space under his leadership. The result, however, would be something akin to the security futures that exist (conceptually) today—perfectly legal financial products that do not exist in the United States in no small part because complying with the regulatory requirements set forth by both the SEC and CFTC makes it uneconomic to produce them. A securities token would seem to be destined for a similar fate. In light of this possibility, the Bill would benefit from greater clarity around the definition of “ancillary assets”—especially the effect of protocol voting rights that typically accompany the DAO tokens that are the centerpiece of many issuances.

Digital Asset Exchanges

Another groundbreaking feature of the Bill is its creation of an entirely new registered entity: the digital asset exchange (“DAE”).²² A DAE would function as a CFTC-regulated trading platform for digital asset spot and derivative transactions. But those digital assets would not include NFTs, owing to the Bill’s “fungibility requirement.”²³ A registered designated contract market (“DCM”) or swap execution facility (“SEF”) can elect to be considered a registered DAE, but a DAE seeking to support derivatives trading in other commodities would require additional registration as a DCM or SEF to provide those services.²⁴

Key Takeaway #5

New CFTC registered entities, digital asset exchanges, can offer trading in digital assets.

Significantly, the Bill codifies some of the disintermediation presently sought by several market participants.²⁵ The Bill allows a DAE to hold customer assets without any intermediation by a futures commission merchant (“FCM”).²⁶ As a result, a DAE would be able to independently execute and settle margined, leveraged, and financed digital asset transactions. At the same time, the Bill empowers FCMs to hold digital assets with a licensed, chartered, or registered entity.²⁷ Both DAEs and FCMs holding customer digital assets would be subject to familiar prohibitions surrounding use and commingling.²⁸ Apart from these provisions, the remaining DAE permissions and obligations align closely with those established for DCMs.

The Bill also limits DAEs to trading digital assets that “are not susceptible to manipulation.”²⁹ These are assets where it is not reasonably likely that “the transaction history of the digital asset can be fraudulently altered,” or “the functionality or operation of the digital asset can be materially altered,” in either case by a person or group of persons acting collectively or under common control.³⁰ Factors to consider in making this determination include the digital asset’s creation and release process, consensus mechanism, and governance structure. Given the recent volatility in cryptocurrency markets, and the lack of total transparency regarding cryptocurrency holdings, one can expect that the CFTC will heavily scrutinize digital assets under this provision when they are first certified for trading on a DAE.

Key Takeaway #6

A DAE can offer trading only in digital assets that are not reasonably susceptible to manipulation.

Payment Stablecoins

In addressing “Responsible Payments Innovation,” the Bill permits insured depository institutions (i.e., traditional banks) to issue payment stablecoins, and also outlines a path for non-banks to receive a charter for the exclusive purpose of issuing payment stablecoins and engaging in “incidental activities.”³¹ “Payment stablecoins” are defined as digital assets that are redeemable, on demand, on a one-to-one basis for instruments denominated in U.S. dollars and defined as legal tender, or instruments defined as legal tender under the laws of a foreign country (excluding digital assets).³² In creating this federal right, the Bill preempts state laws or regulations to the contrary.

The Bill provides for the creation of non-bank payment stablecoin issuers by amending the definition of “depository institution” in the Federal Reserve Act to include a

depository institution that is exclusively engaged in issuing payment stablecoins, providing safekeeping, trust, or custodial services, or activities incidental to the foregoing.³³ Incidental activities include a range of conduct such as market making, settlement and clearing, and post-trade services.³⁴ Like traditional banks, non-bank stablecoin issuers would receive access to a Federal Reserve master account, and to the services that come with it.³⁵ Unlike traditional banks, however, non-bank stablecoin issuers would not be required to obtain federal deposit insurance—a point that has some in the industry on edge.³⁶

Key Takeaway #7

Non-bank entities can apply to issue payment stablecoins and to open a Federal Reserve master account.

Payment stablecoin issuers, be they bank or non-bank, would be subject to the same restrictions concerning backing assets and disclosures.³⁷ Notably, the Bill *does not* endorse or permit algorithmic stablecoins such as DAI. Rather, all payment stablecoins must be backed by “high-quality liquid assets . . . equal to not less than 100 percent of the face amount of the liabilities of the institution on payment stablecoins issued by the institution.”³⁸ High-quality liquid assets include such things as legal tender, demand deposits, balances held at a Federal Reserve bank, short-term securities guaranteed by the Department of Treasury, and others, subject to certain conditions and limitations. Payment stablecoin issuers would be required to disclose, in a publicly accessible manner, and in a filing with the appropriate federal banking agency or state bank supervisor made by the institution’s chief financial officer under penalty of perjury, a description of those assets, their value, and the number of outstanding payment stablecoins following the end of each month.³⁹

Key Takeaway #8

Payment stablecoins must be 100% backed by high-quality liquid assets.

Also, bank and non-bank payment stablecoin issuers would need to have tailored recovery and resolution plans in place to ensure safe and sound operation or an orderly wind-down in times of distress.⁴⁰ And in the event of a receivership, a person with a valid claim on a payment stablecoin would have priority over all other claims other than administrative costs. It is unclear, however, whether the receivership provisions would apply to currently extant stablecoin issuers, as the section refers to “the receivership of a depository institution that has issued a stablecoin *under this section*.”⁴¹ On its face, this section would therefore not apply to any stablecoin in circulation today.

Consumer Protection

In Title V, the Bill establishes a consumer protection standard for digital assets. These standards apply to both persons and protocols⁴² The Bill does not define “protocol,” but based on the Bill’s other references to protocols, it likely means decentralized applications such as decentralize finance (“DeFi”) protocols Maker and Aave.

Key Takeaway #9

Smart contract lending arrangements would need to be fully enforceable as a matter of commercial law.

The Bill’s consumer-protection standards relate to, among other things, notice requirements, customer entitlement to subsidiary proceeds, and rehypothecation. For example, digital asset service providers would need to provide notice regarding source code updates, segregation, fees, and dispute resolution processes.⁴³ In the event a customer’s digital assets received subsidiary proceeds such as airdrops or staking gains while in the digital asset provider’s custody, the digital asset provider would need to allow the customer to withdraw its digital assets in a way that permits collection of those subsidiary proceeds.⁴⁴ Furthermore, digital asset providers would need to provide customers with a clear definition of rehypothecation and obtain customer consent prior to using customer assets for that purpose.⁴⁵

On the topic of lending arrangements, the Bill instructs that digital asset service providers must ensure that the arrangements are accompanied by the usual disclosures pertaining to risk, yield, collateral requirements, mark-to-market monitoring, and call procedures. Significantly, however, the Bill also requires digital asset service providers to ensure that the lending arrangements are “fully enforceable as a matter of commercial law.”⁴⁶ This provision could have profound implications in the context of DeFi and DAOs that deploy smart contracts to effectuate financial transactions. Questions regarding the enforceability of these smart contracts have circulated for years. In a pseudo-anonymous market, who are the parties? In a software-driven market, what is the contract? In a global internet-based market, what law controls? To date, there have been no clear answers, but this provision would appear to require them.

Tax Changes

Not to be overlooked are the Bill’s significant provisions concerning the characterization and taxation of digital assets. Among other things, these provisions would provide much-needed clarity for taxpayers and relax some of the existing tax rules widely considered impractical when applied to real-world digital asset transactions.

Key Takeaway #10

Purchasing goods and services for less than \$200 using digital currency would no longer trigger a taxable event for most individuals.

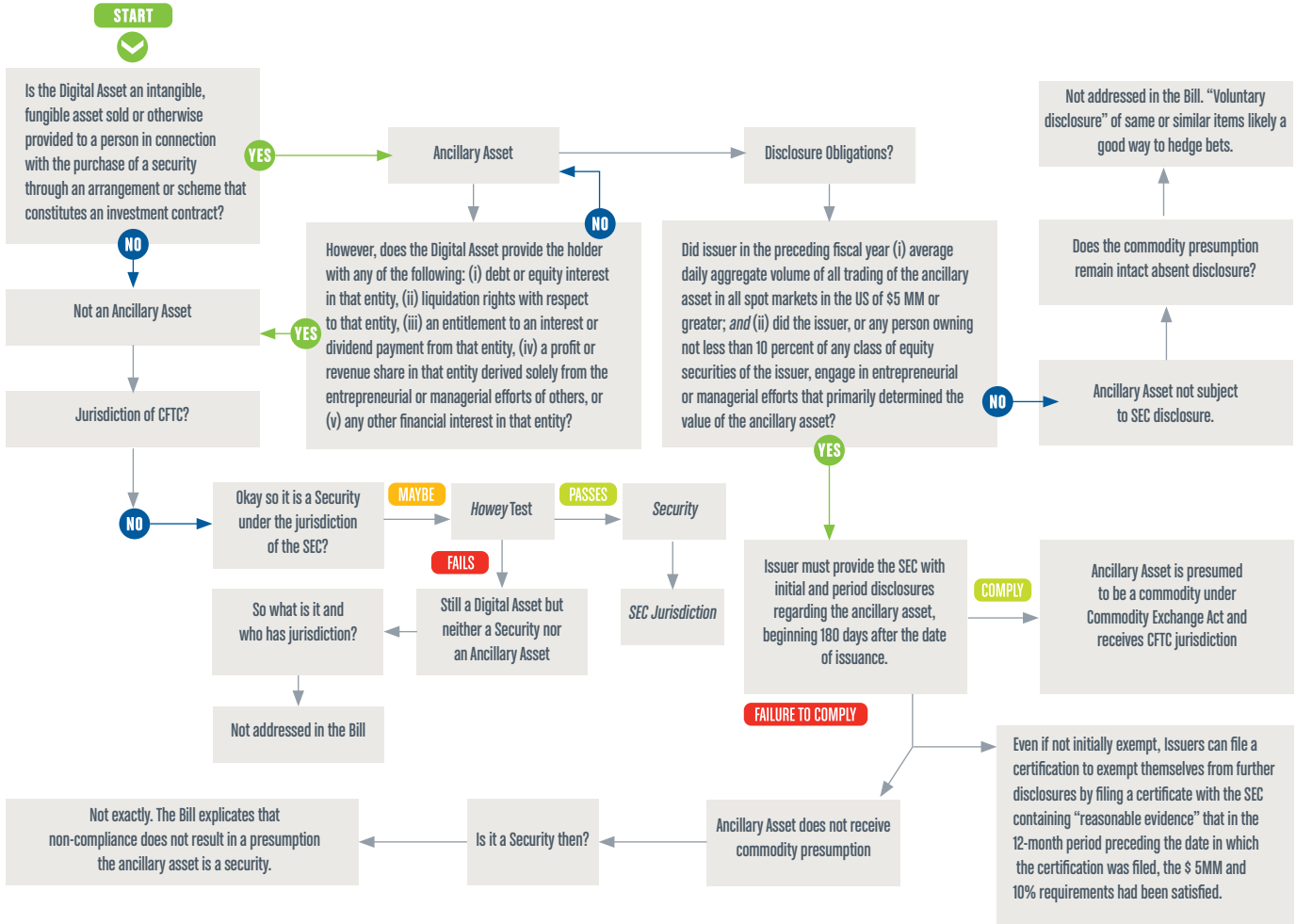
Key among these new tax provisions include the introduction of a safe harbor allowing individuals to make small purchases of goods and services without triggering tax (similar to using foreign currencies), narrowing the scope of intermediaries subject to tax reporting obligations, providing certainty for the tax classification of DAOs, deferring the taxation of mining and staking rewards until disposition, and enabling qualifying digital assets to be treated similar to securities and commodities for purposes of the existing (and taxpayer-favorable) lending and trading safe harbor regimes.⁴⁷ The Bill also instructs Treasury to issue guidance on a number of specific items, including the classification of forks and air drops as taxable only upon affirmative claim and disposition, although the Bill does not amend or identify statutes relevant to this mandate.⁴⁸

TIMELINE/NEXT STEPS OVERVIEW



THRESHOLD QUESTIONS

Is the Digital Asset an Ancillary Asset?



ENDNOTES

- 1 Lummis-Gillibrand Responsible Financial Innovation Act, S. 4356, 117th Cong., § 101(a) (2022) (proposed 31 U.S.C. § 9801(2)).
- 2 *d.* § 101(a) (proposed 31 U.S.C. § 9801(3)).
- 3 *Id.* § 203(a) (proposed 26 U.S.C. § 864(b)(C)).
- 4 *Id.* § 401 (amending 7 U.S.C. § 1a).
- 5 Kate Rooney, “SEC chief says agency won’t change securities laws to cater to cryptocurrencies,” CNBC (June 6, 2018).
- 6 See, e.g., *In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 5535736, at * 2 (Sept. 17, 2015) (stating that bitcoin is properly defined as a commodity within the meaning of the CEA).
- 7 *In re BFXNA INC. d/b/a BITFINEX*, CFTC Docket No. 16-19 (June 2, 2016).
- 8 Daniel Kuhn, “SEC’s Gensler Reiterates Bitcoin Alone Is a Commodity. Is He Right?,” Yahoo (June 28, 2022).
- 9 See Chair Gary Gensler, U.S. Sec. & Exch. Comm’n, [Speech at Penn Law Capital Mkts. Ass’n Annual Conference](#) (April 4, 2022).
- 10 See [Letter from Chair Gary Gensler](#), U.S. Sec. & Exch. Comm’n, to Sen. Elizabeth Warren (Aug. 5, 2021).
- 11 S. 4356, § 401(2) (amending 7 U.S.C. § 1a); § 403(a)(1)(B) (amending 7 U.S.C. § 2(c)(2)).
- 12 *Id.* § 301 (amending 15 U.S.C. § 78a et seq.).
- 13 *Id.*
- 14 *Id.* § 403(a)(1)(B) (amending 7 U.S.C. § 2(c)(2)).
- 15 *Id.* § 404 (amending 7 U.S.C. § 1 et seq.).
- 16 Thomas Franck, “Bipartisan crypto regulatory overhaul would treat most digital assets as commodities under CFTC oversight,” CNBC (June 7, 2022).
- 17 *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).
- 18 Lummis-Gillibrand Responsible Financial Innovation Act, [Section-by-Section Overview](#), 2 (June 7, 2022).
- 19 *Id.*
- 20 S. 4356, § 301 (amending 15 U.S.C. § 78a et seq.).
- 21 *W. Virginia et al. v. EPA*, 142 S. Ct. 2587, 2614 (2022) (holding that an agency must point to “clear congressional authorization” to exercise regulatory authority in extraordinary cases involving statutes that confer authority upon an administrative agency).
- 22 S. 4356, § 404 (amending 7 U.S.C. § 1 et seq.).
- 23 *Id.* § 403 (amending 7 U.S.C. § 2(c)(2)(F)(i)(II)).
- 24 *Id.*
- 25 This is currently allowed, but takes some looking around the CEA and CFTC regulations to figure out. See [Public Comment from Joshua Sterling](#), Jones Day, to Christopher Kirkpatrick, Secretary, Commodity Futures Trading Comm’n (Mar. 17, 2022).
- 26 S. 4356, § 404(a) (amending 7 U.S.C. § 1 et seq.).
- 27 *Id.* § 403(b) (amending 7 U.S.C. § 6d).
- 28 *Id.* § 403(b) (amending 7 U.S.C. § 6d); § 404(a) (amending 7 U.S.C. § 1 et seq.).
- 29 *Id.* § 404(a) (amending 7 U.S.C. § 1 et seq.).
- 30 *Id.*
- 31 *Id.* § 601 (proposed 12 U.S.C. § 4810(j)).
- 32 *Id.* § 601 (proposed 12 U.S.C. § 4810(j)).
- 33 *Id.*
- 34 *Id.* § 601 (proposed 12 U.S.C. § 4810(j)).
- 35 *Id.* § 601 (proposed 12 U.S.C. § 4810(b)).
- 36 *Id.* § 604 (amending 12 U.S.C. § 5169).
- 37 *Id.* § 601 (proposed 12 U.S.C. § 4810(c)).
- 38 *Id.*
- 39 *Id.*
- 40 *Id.* § 601 (proposed 12 U.S.C. § 4810(l)); § 604 (amending 12 U.S.C. § 5169).
- 41 *Id.* § 601 (proposed 12 U.S.C. § 4810(i)).
- 42 *Id.* § 501 (proposed 31 U.S.C. § 9802(a)).
- 43 *Id.* § 501 (proposed 31 U.S.C. § 9802(b)).
- 44 *Id.* § 501 (proposed 31 U.S.C. § 9802(c)).
- 45 *Id.* § 501 (proposed 31 U.S.C. § 9802(e)).
- 46 *Id.* § 501 (proposed 31 U.S.C. § 9802(d)).
- 47 *Id.* § 201 (proposed 26 U.S.C. § 139J).
- 48 *Id.* § 206.



DIGITAL ASSETS DEFINED: CONSUMER PROTECTION AND CYBERSECURITY ENTER THE STAGE

SEPTEMBER 2022 WHITE PAPER

In this latest *White Paper* on our [Bill analysis](#), we underscore headline proposals in the Lummis-Gillibrand Responsible Financial Innovation Act (the “Bill”) regarding consumer protection standards (Title V) and cybersecurity standards (Title VIII, Section 808). As for consumer protection standards, the Bill lays out the notices and disclosures that digital asset service providers must give customers, and the subjects that customer agreements must address. The Bill also covers rules for managing the accrual of gains to digital assets, the implementation of source code changes to digital assets, the enforcement of the standards laid out in the title, and customers’ rights to individual management of their digital assets. As for cybersecurity standards, the Bill requires the Commodity Futures Trading Commission (“CFTC”) and the Securities and Exchange Commission (“SEC”) to develop guidance related to cybersecurity for digital asset intermediaries ([as described in our previous White Paper](#)).

We conclude this *White Paper* by highlighting important unresolved questions that should be the focus of future stakeholder efforts to refine the Bill before it—or aspects of it—becomes law.

CONSUMER PROTECTION STANDARDS FOR DIGITAL ASSETS

Scope of Permissible Transactions

A digital asset service provider, defined in the Bill as set forth below, must ensure that the scope of permissible transactions that it may undertake with its customers’ digital assets is clearly disclosed in a customer agreement. Unlike other requirements for digital asset service providers in Title V, this requirement applies to both “persons” and “protocols” providing digital asset services. Under the Bill, a “person who provides digital asset services” includes: (i) a digital asset intermediary; (ii) a financial institution as defined in section 1a of the Commodity Exchange Act; and

(iii) any other person conducting digital asset activities pursuant to a federal or state charter, license, registration, or other similar authorization, or a person who is required by law to hold such a license, registration, or other similar authorization. The Bill does not define “protocol,” but based on the Bill’s other references to protocols, it likely means decentralized applications such as decentralized finance (“DeFi”) protocols.

Required Notices to Customers

A digital asset service provider must give clear notice to each customer, and obtain the customer’s acknowledgment, of any “material” changes to the source code version of a digital asset involved in the parties’ contractual

relationship.² Under the Bill, “source code version” means the source code version comprising a digital asset, and does not include the software used to manage or facilitate transactions in a digital asset.

The provider must generally give the required notice and obtain the required acknowledgement before the provider implements any material source code change. Notice and acknowledgement are not required in emergencies, however, such as when security vulnerabilities exist that require immediate changes to a source code version. It is unclear as to whether, in an emergency, notice and acknowledgement would be required *after* a source code version change is implemented. However, as laid out elsewhere in the Bill (see “Source Code Version of Digital Assets,” *below*), a provider may specify that different standards for implementing source code version changes apply in emergencies, which could include giving notice and obtaining acknowledgement after a source code change is implemented.

In addition, a digital asset service provider must provide clear notice to each customer, and require the customer’s acknowledgement, of the following:

- Whether the customer’s digital assets are segregated from other customers’ assets, and the manner of segregation.
- How the customer’s assets would be treated in a bankruptcy or insolvency scenario, and the risks of loss (note that Title IV, Section 407 of the Bill, which will be discussed in a future Jones Day *White Paper*, enacts new requirements related to the bankruptcy treatment of digital assets).
- The time period and the manner in which the provider must return the customer’s digital assets to the customer upon the customer’s request.
- Any fees that apply to the contractual relationship between the provider and the customer (such fees could include transaction fees, or a monthly fee for custodial digital assets).
- The provider’s dispute resolution process for any disputes that arise between the provider and the customer.

Subsidiary Proceeds

Except as otherwise specified in a customer agreement, all “ancillary or subsidiary proceeds” related to digital asset services provided by a digital asset service provider accrue to the customer’s benefit. “Subsidiary proceeds” are defined to include proceeds arising from forks,³ airdrops,⁴ staking,⁵ and other gains that accrue to a digital asset through market transactions, use as a financial asset, or being held in custody or safekeeping by a digital asset service provider. The use of “ancillary” appears to be redundant here, since

there is no separate definition for “ancillary proceeds,” and “ancillary” and “subsidiary” are related concepts. A digital asset service provider may elect not to collect certain subsidiary proceeds, if the election is disclosed in a customer agreement.

Assuming a digital asset service provider elects to collect subsidiary proceeds, a customer may withdraw its digital assets from the provider in a method that permits the collection of subsidiary proceeds. Further, if a customer desires, a digital asset service provider must enter into a customer agreement regarding the manner in which to invest subsidiary proceeds or other gains attributable to the customer’s digital assets.

As used here in connection with “subsidiary proceeds,” an “agreement” includes the digital asset service provider’s standard terms of service. Thus, to the extent these standards on subsidiary proceeds require something to be disclosed in or agreed to through a customer agreement, it may be disclosed in or agreed to through the provider’s standard terms of service.

Lending Arrangements

Digital asset service providers must ensure that any lending arrangements they have with customers related to digital assets are clearly disclosed to customers before any lending services take place, and that their customers consent to such arrangements.

Providers must also ensure that any lending arrangements with customers are accompanied by a wide variety of disclosures. Specifically, such arrangements must be accompanied by:

- Full disclosures of applicable terms (such as the loan’s repayment period, monthly payments, and interest rate) and risk, yield, and the manner in which the yield is calculated.
- “Appropriate disclosures” related to collateral requirements and policies, including: (i) haircuts and overcollateralization;⁶ (ii) collateral the provider accepts when calling for additional collateral from a customer, including collateral substitution; (iii) whether customer collateral is comingled with other customers’ collateral or the provider’s collateral; and (iv) how customer collateral is invested, and whether the yield belongs to the customer or the provider. The term “appropriate disclosures” is not defined here.
- Disclosures of mark-to-market and monitoring arrangements,⁷ including: (i) the frequency of mark-to-market monitoring and how frequently the provider will call for additional collateral from a customer; (ii) the time period in which the customer must supply additional collateral to the provider after a collateral call; and (iii) whether the

provider permits failures to deliver additional collateral, and if so, the period of time in which a customer must cure the failure before the customer's position is closed.

Further, providers must ensure that lending arrangements with customers are “fully enforceable as a matter of commercial law” and compliant with all applicable federal and state laws. In general, for a contract to be legally enforceable, there must be an offer, an acceptance, consideration, capacity to contract, and legality of purpose. Certain laws apply to lending arrangements in particular, including the Equal Credit Opportunity Act, which prohibits lenders from discriminating against borrowers on the basis of any protected class; the Truth in Lending Act, which requires lenders to disclose loan cost information to borrowers; and state usury laws, which prohibit lenders from charging unreasonable or predatory interest rates. Requiring providers to ensure that their lending arrangements with customers are “fully enforceable as a matter of commercial law” and compliant with federal and state lending laws could have a profound impact on DeFi protocols and decentralized autonomous organizations (“DAOs”), many of which employ smart contracts to effectuate loan transactions. Questions regarding the enforceability of the “agreements” underlying smart contracts—such as what source code controls and who the contracting parties are—have circulated for years without clear answers. Because it does not address these questions directly, the Bill, as written, would require DeFi protocols and DAOs to continue to answer these questions for themselves, and to incorporate the requirements of contract law in general, and lending laws in particular, into the smart contracts and related documents used for loan transactions.

Rehypothecation

Before a rehypothecating a customer's digital asset—that is, before pledging to a third party as collateral for a financial transaction a digital asset that a customer has pledged to the provider as collateral for a loan—a digital asset service provider must clearly disclose its policies on rehypothecation to customers, including a clear definition of “rehypothecation” that is accessible to consumers. The terms “clearly disclose,” “clear definition,” and “accessible” are not defined here. A provider must also obtain affirmative consent from a customer to rehypothecate that customer's digital asset.

In addition, when deciding to rehypothecate a customer's digital asset, a provider must consider the following factors to appropriately mitigate risk relating to rehypothecation:

- The liquidity and volatility of the digital asset.
- Past failures to deliver the digital asset.
- The concentration risk of the digital asset.⁸
- Whether an issuer or lender of last resort relating to the digital asset exists, including for virtual currency with a finite supply.⁹
- The provider's capital, leverage, and market position.
- The provider's legal obligations to customers and other digital asset service providers.

Source Code Version of Digital Assets

At the beginning of their contractual relationship, a digital asset service provider and its customer must agree in writing on what source code version will apply to each digital asset involved in that relationship, including for purposes of legal treatment. This agreement must include the treatment of each digital asset under securities laws and commodities laws, as well as under the Uniform Commercial Code (“UCC”) applicable to the transaction.

A digital asset service provider may periodically implement a digital asset source code version that uses validation rules different from those of the source code version specified in the customer agreement. The term “validation rules” is not defined, but most likely refers to block-level validation rules (or “consensus rules”), which define what is permitted to be included in a block on a blockchain and require non-conforming transactions to be rejected from the chain.

A provider may implement a digital asset source code version with different validation rules even when it is not possible to predict in advance whether using the different source code will be in the “best interests” of the customer. However, this discretion leaves open the possibility that providers must consider how a source code change will affect customers' best interests if it is possible to do so. The “best interests” of the customer are not defined; what is in a customer's “best interests” could range from ensuring the maximum possible value of a digital asset, to ensuring the maximum possible liquidity of the digital asset, to ensuring that the digital asset can be used in future transactions.

A digital asset service provider must consider the nature of any proposed changes to the source code versions of a digital asset. Specifically, the provider must consider whether any proposed changes by third-party actors—such as within a DAO—could create different source code versions resulting in new networks that could create “economic value” for customers. The term “economic value” is not pegged to any particular standard here; perhaps it could be determined by the digital asset's price in the securities or commodities markets, or by the asset's liquidity and risk.

Although a digital asset service provider is allowed to implement a digital asset source code version that uses different validation rules, it is not required to support digital assets and source code versions that it has not agreed with customers to support. This issue may arise if customers

are expecting or pressing a provider to change the source code version of a digital asset. At the same time, a digital asset service provider must not “capriciously” redefine a digital asset or corresponding source code or alter customer agreements as they relate to digital asset source codes. The term “capriciously” is not defined here.

A digital asset service provider must adopt and maintain standards for implementing digital asset source code versions with different validation rules from those of the source code version specified in a customer agreement. These standards must include customer notice and approval “as appropriate based on the circumstances”; this rule is not explained, and will likely be based on a fact-intensive inquiry and subject to court interpretation. Providers may specify that different standards for implementing source code version changes apply in emergencies, such as when security vulnerabilities exist that require immediate changes to a source code version.

Settlement Finality

Digital asset service providers and their customers must agree on the terms of settlement finality for all transactions between them. That agreement must address the conditions under which a digital asset may be deemed fully transferred as a matter of law. These legal conditions may be different from the operational conditions under which digital assets are considered transferred based on the distributed and probabilistic nature of digital assets. Therefore, digital asset service providers and their customers can choose to consider a digital asset as fully transferred as a matter of law, even if different from when it would be considered fully transferred in operation.

The agreement between provider and customer on settlement finality terms must also address the exact moment of transfer of a digital asset, the discharge of any obligations upon transfer of a digital asset, and conformity to applicable provisions of the UCC. Provisions of the UCC that relate to settlement finality include Article 2, Parts 3-5 (transfer obligations related to contracts for the sale of goods); Article 4, Part 2 (transfer obligations related to bank deposits and collections); Article 4A, Parts 2-4 (transfer obligations related to funds transfers between banks); Article 8, Part 3 (transfer obligations related to investment securities); and Article 9, Part 2 (attachment obligations related to secured transactions).

Standards of Customer Notice and Enforcement of Consumer Protection Standards

When providing disclosures and carrying out other duties under 31 U.S.C. Subtitle VI, Chapter 98 (a new chapter created by the Bill), a person who provides digital asset services in or affecting interstate commerce must provide

“higher” standards of customer notice and acknowledgment if there is likely to be a “material” impact on the “economic value” of a customer’s digital asset. Again, the terms “higher” and “material” are not defined here. And, again, the term “economic value” is not pegged to any particular standard.

The Bill also instructs that the “standards” under 31 U.S.C. Subtitle VI, Chapter 98 shall be enforced “in an appropriate manner,” commensurate with other consumer protection standards. Given the reference to “other consumer protection standards,” the term “standards” most likely refers to the “consumer protection standards” laid out in Title V of the Bill. “[A]n appropriate manner” will most likely depend on how authorities would enforce consumer protection standards in other contexts. “Commensurate with” also indicates that enforcing authorities must not treat the consumer protection standards applicable to digital assets any differently from the consumer protection standards applicable to other types of goods or services.

The consumer protection standards under Title V applicable to digital asset intermediaries will be enforced by the federal or state licensing, registration, or chartering authority of the intermediary, while the standards applicable to depository institutions or other financial institutions will be enforced by the appropriate federal or state banking supervisor.

Right to Individual Management of Digital Assets

“[E]xcept as otherwise required by law,” no person is required to use an intermediary for the safekeeping of digital assets that the person legally owns and either possesses or controls. An example of a law that requires a person to use an intermediary for the safekeeping of assets that the person legally owns and either possesses or controls is 17 CFR § 227.100, which requires a securities issuer to use an intermediary when relying on the crowdfunding exemption to securities registration requirements.

The Bill states it should not be interpreted as allowing a person to engage in market activity for which authorization is required under federal or state law. In other words, the fact that a person is not required to use an intermediary to safekeep that person’s digital assets does not mean that person can use those digital assets for a market activity without being authorized to do so, if such authorization is required by federal or state law.

The Bill also states that it should not be interpreted as preventing a person from freely entering into an agreement for digital asset services with a third party. In other words, the fact that a person is not required to use an intermediary to safekeep that person’s digital assets does not mean that person is prohibited from making an agreement to do so if desired.

Undefined Terms

As evident from the above discussion, the Bill's proposals related to consumer protection standards leave several crucial terms undefined. The meanings ultimately assigned to these undefined terms will likely be based on fact-intensive inquiries and subject to interpretation by courts and by a number of federal and state agencies. Some terms—such as “material” and “best interests”—may be interpreted consistently with their meanings in other contexts, such as whether there has been a misrepresentation or omission of “material” information to investors in the securities fraud context, and whether a broker-dealer's recommendation of a securities transaction or investment strategy involving securities is in the “best interests” of a retail customer. Other terms have no corollaries to reference, and will present issues of first impression.

It is also likely that some or all of the federal and state regulators responsible for enforcing the Bill's consumer protection standards (see “Standards of Customer Notice and Enforcement of Consumer Protection Standards,” *above*) will promulgate rules or guidance interpreting these undefined terms in the future. Indeed, Title VIII of the Bill expressly contemplates that the CFTC and the SEC, among other federal financial regulators, will issue “individualized interpretative guidance” on the application of statutes, rules, or policies under their jurisdiction.

CYBERSECURITY STANDARDS FOR DIGITAL ASSET INTERMEDIARIES

On the topic of cybersecurity, the Bill requires the CFTC and the SEC, in consultation with the Secretary of the Treasury and the Director of the National Institute of Standards and Technology, to “develop comprehensive, principles-based guidance relating to cybersecurity” for digital asset intermediaries. This guidance must account for:

- The internal governance and organizational culture of the digital asset intermediary's cybersecurity program;
- The security operations of the digital asset intermediary, including threat identification, incident response, and mitigation;
- Any risk identification and measurement by the digital asset intermediary;
- The mitigation of risk by the digital asset intermediary, including policies of the digital asset intermediary, controls implemented by the digital asset intermediary, change management with respect to the digital asset intermediary, and the supply-chain integrity of the digital asset intermediary;
- Any assurance provided by, and testing conducted by, the digital asset intermediary, including penetration testing and independent audits so conducted; and
- The potential for digital asset intermediaries to be used to facilitate illicit activities including sanctions avoidance.

This guidance must be “developed,” according to the Bill, no later than 18 months after the Bill is enacted.

CLOSING THOUGHTS

All told, the Bill sets out a thorough framework for regulating—or developing rules for regulating—important consumer protection and cybersecurity issues in the digital assets space. These include foundational matters such as customer notices, subsidiary proceeds, lending arrangements, and source code controls. At the same time, the Bill relies on key terms and concepts that it does not define, such as “material” changes to source code, “higher” standards of customer notice and acknowledgement, and “best interests” of the customer, to name just a few. Thus, in order for the proposed framework to be implemented in a manner that provides clarity for market participants, the Bill will have to become more specific, or agencies and courts may be left to fill in the blanks.

ENDNOTES

- 1 The Bill does not define the term “material.”
- 2 “Source code” refers to a set of instructions, written in programming language, directing a computer program how to function.
- 3 “Forks” are changes to a blockchain's protocol that cause the chain to split and produce an additional chain.
- 4 An “airdrop” is the delivery of a cryptocurrency, token, non-fungible token (“NFT”), or other type of digital asset to customers at no cost, generally as part of a promotion.
- 5 “Staking” is pledging digital assets to a platform for use in the proof-of-stake process for validating blockchain transactions in a proof-of-stake ecosystem, e.g., Ethereum.
- 6 A “haircut” refers to valuing a collateral asset as less than its fair market value, while “overcollateralization” refers to pledging a collateral asset worth more than the loan amount.
- 7 “Mark to market” is a method of measuring, based on current market conditions, the fair value of an account that can fluctuate over time.
- 8 “Concentration risk” is the risk of loss that may occur from a customer “concentrating” its investments in the digital asset, compared to the customer's overall portfolio.
- 9 A “lender of last resort” provides liquidity to a lender that urgently needs funding and has exhausted all its other options.



DIGITAL ASSETS DEFINED: SEC, CFTC, AND ANCILLARY (ILLUSORY?) ASSETS

AUGUST 2022 WHITE PAPER

In “Digital Assets Defined: How Lummis-Gillibrand Will Shape the Coming Fintech Debate,” we provided a high-level overview of the Responsible Financial Innovation Act (the “Bill”) and examined some of its significant takeaways. We then explored how the Bill would [shore up stablecoins](#).

In this latest installment, we take a closer look at the Bill’s contemplated regulatory jurisdiction as between the Securities and Exchange Commission (“SEC”) and the Commodity Futures Trading Commission (“CFTC”) in the digital assets space. In doing so, we will summarize the commissions’ respective regulatory roles, and we will highlight the critical importance of the defined term “ancillary asset” in determining where regulatory authority over a particular digital asset would lie.

THE SECURITIES AND EXCHANGE COMMISSION’S EXPANDED JURISDICTION OVER “ANCILLARY ASSETS”

Title III of the Bill is devoted to addressing the SEC’s jurisdiction. Its centerpiece is the defined term “ancillary asset,” which can, in certain circumstances, trigger a set of conditional disclosure requirements. Importantly, if an issuer of an ancillary asset complies with those disclosure requirements, then the Bill states that the ancillary asset “shall be presumed to be” a commodity, and not a security under various laws.

The Bill describes “ancillary asset” as follows:

The term ‘ancillary asset’ means an intangible, fungible asset that is offered, sold, or otherwise provided to a person in connection with the purchase and sale of a security through an arrangement or scheme that constitutes an investment contract, as that term is used in section 2(a)(1) of the Securities Act of 1933 (15 U.S.C. 77b(a)(1)).¹

Excluded from the definition are assets with the following characteristics:

[A]n asset that provides the holder of the asset with any of the following rights in a business entity:

- “(i) A debt or equity interest in that entity.
- “(ii) Liquidation rights with respect to that entity.
- “(iii) An entitlement to an interest or dividend payment from that entity.
- “(iv) A profit or revenue share in that entity derived solely from the entrepreneurial or managerial efforts of others.
- “(v) Any other financial interest in that entity.”²

If an asset is an ancillary asset, the Bill establishes a set of conditional initial and ongoing disclosure requirements for certain issuers that provide or propose to provide the ancillary asset in conjunction with a securities offering:

[A]n issuer engaged in business in or affecting interstate commerce, or that is organized outside of the United States and is not a foreign private issuer, that offers, sells, or otherwise provides a security through an arrangement or scheme that constitutes an investment contract, as that term is used in section 2(a)(1) of the Securities Act of 1933 (15 U.S.C. 77b(a)(1)), and that provides or proposes to provide any holder of the security with an ancillary asset, shall be subject to the periodic disclosure requirements under subsection (c)...³

The conditions relate to whether, during prescribed time frames: (i) the average daily trading volume of the ancillary asset in spot markets exceeded \$5,000,000; and (ii) “the issuer, or any person owning not less than 10 percent of any class of equity securities of the issuer, engaged in entrepreneurial or managerial efforts that primarily determined the value of the ancillary asset.”⁴ The initial compliance time frames shift depending on whether the digital asset was either issued prior to the time the provision goes into effect or the digital asset is being issued for the first time after the provision has gone into effect. The ongoing compliance time frames are the same—the issuer’s preceding fiscal year—regardless of the timing of the digital asset’s issuance.

If the aforementioned conditions are met, then the issuer must furnish, or cause the relevant affiliate to furnish, to the SEC, on a semi-annual basis: (i) corporate information regarding the issuer; and (ii) information concerning the ancillary asset. The former category consists of at least a dozen separately identified topics covering a range of matters such as the issuer’s board composition, promotional activities, ancillary asset ownership, purchases and sales, and a going-concern statement signed under penalty of perjury.⁵ The latter category also consists of at least a dozen wide-ranging topics relating to the ancillary asset’s underlying technology, risk factors, airdrops, source code audits, average daily price, the issuer’s plans to continue or discontinue supporting the ancillary asset, and so on.⁶ An issuer can terminate its disclosure obligations by providing to the SEC a certification, supported by reasonable evidence, that the relevant conditions are no longer met.⁷

To be sure, these disclosure requirements are substantial, and would require significant investments in time and money to prepare twice per year. However, the proposed disclosures would be less onerous than those associated with publicly traded securities. And, if an issuer complies with them,⁸ the ancillary asset “shall be presumed to be a commodity . . . and not to be a security” under various enumerated laws, including the Securities Act and the Exchange Act.⁹ Thus, the ancillary asset would not need to be traded through an SEC-registered broker-dealer, or on an SEC-registered exchange. Instead, pursuant to

the provisions in the Bill concerning the CFTC, the ancillary asset would be eligible for trading (assuming the satisfaction of other relevant conditions) on newly defined digital asset exchanges registered with and regulated by the CFTC.

The SEC can, however, challenge the commodity presumption through litigation in a court of competent jurisdiction, and the presumption can be overcome if the court finds that there is not a “substantial basis” for its application to a specific asset.¹⁰ Although it is an open question to what extent the SEC would plan to litigate under this exception to challenge a commodity presumption, its ability to do so cannot be overlooked. In addition, because the definition of “ancillary asset” presumes that the asset has been offered or sold to a person in connection with an investment contract, which would continue to be a “security,” there is a nonzero chance the SEC could take a position that the federal securities laws apply to the investment contract as a whole (including the digital assets).

THE COMMODITY FUTURES TRADING COMMISSION

Title IV of the Bill is devoted to addressing the CFTC’s jurisdiction. Its centerpiece is a provision providing the CFTC with “exclusive jurisdiction over any agreement, contract, or transaction involving a contract of sale of a digital asset in interstate commerce, including ancillary assets (consistent with section 41(b)(4) of the Securities Exchange Act of 1934).”¹¹

The Bill includes a fungibility requirement, however, thereby excluding typical nonfungible tokens, or NFTs.¹²

To facilitate trading in approved digital assets, the Bill articulates a framework for registering and overseeing digital asset exchanges. The definition of a “digital asset exchange” is straightforward: “a trading facility that lists for trading at least 1 digital asset.”¹³ And the definition of “digital asset” is that used throughout the Bill, with one significant exclusion.¹⁴ The Bill defines a “digital asset” as a natively electronic asset that confers economic, proprietary, or access rights or power, and is recorded using cryptographically secured distributed ledger technology.¹⁵ This definition includes virtual currency, ancillary assets, payment stablecoins, and *other securities and commodities*.¹⁶ But in the title pertaining to the CFTC, the Bill expressly excludes from the definition any digital assets that would not qualify as ancillary assets due to the digital assets being interests in a business entity.¹⁷ As a result, the Bill effectively excludes digital asset securities from trading on CFTC-registered digital asset exchanges. And there is still the risk that the SEC (or a private litigant) could attempt to characterize a

digital asset as a security rather than as a commodity/ancillary asset.

Digital asset exchanges would be required to comply with a set of “Core Principles” similar to those for existing CFTC-registered entities.¹⁸ These principles address fundamental matters such as establishing and complying with exchange rules, treatment of customer assets, monitoring of trading and trade processing, reporting requirements, recordkeeping, financial resources, governance fitness standards, and system safeguards.¹⁹ The Bill includes provisions concerning the segregation of digital assets that are similar to those applicable to registered futures commission merchants.²⁰

Of note, digital asset exchanges would be permitted to list and transact in digital assets that are not readily susceptible to manipulation only.²¹ Considerations relevant to that topic include the creation or release process, the consensus mechanism, the governance structure, and “any other factors required by the Commission.”²² These provisions appear to be directed to concerns that digital assets purporting to be traded within a distributed autonomous organization (“DAO”) are not truly “distributed” to a satisfactory degree, such that the organization is not truly autonomous. The Bill would permit digital asset exchanges to leverage the self-certification process in the Commodities Exchange Act to self-certify that a digital asset not previously listed for trading on another registered entity meets this requirement.²³ But, consistent with that process, the Commission could stay the certification while it analyzed the digital asset, and could ultimately deny the certification outright. The Bill would provide the Commission with extended time frames to conduct such inquiries,²⁴ which would likely focus on the extent to which a digital asset is distributed among unaffiliated persons and entities.

Also of note, the “Core Principles” indicate that digital asset exchanges would be permitted to hold customer money, assets, and property directly, without the involvement of a futures commission merchant or derivatives clearing organization.²⁵ As a result, a digital asset exchange would be able to independently execute and settle margined, leveraged, and financed digital asset transactions. This disintermediated approach to digital asset trading would further reduce costs and friction in the digital assets market.

ANCILLARY ASSET OR SECURITY?

Within this proposed paradigm, the fundamental question for any digital asset is as follows: Is it an ancillary asset or not?²⁶ A digital asset that qualifies as an ancillary asset is eligible for comparatively reduced SEC reporting and disclosure requirements, presumed treatment as a commodity, and trading on CFTC-regulated digital asset exchanges. A digital asset that does not qualify as an

ancillary asset—and has not been previously classified as a commodity—presumably receives treatment as a security, and remains entirely within the domain of the SEC and the requirements associated with the federal securities laws. As a result, the ramifications associated with a digital asset’s ultimate classification are not insubstantial.

To better understand the ancillary-assets issue, it is useful to consider its likely origins. Discussing the application of federal securities law to initial coin offerings (“ICO”) at the end of 2018, former SEC Chairman Jay Clayton analogized the sale of crypto “coins” to fund a blockchain protocol to the advanced sale of tickets to fund a Broadway production.²⁷ Chairman Clayton explained that, in the Broadway context, the advanced sale of tickets was a fundraising scheme and the tickets were securities. And similarly, in the ICO context, the advanced sale of tokens was the fundraising scheme and the tokens were the securities. In articulating this analogy, Chairman Clayton helped highlight the difference between a fundraising scheme and its object—a crucial distinction that the Bill aims to address with its novel legal concept “ancillary asset.”

Viewed objectively, the Bill appears to contemplate that even where tokens are offered as part of a fundraising scheme, they would be presumed to be commodities as long as the ancillary-asset disclosure requirements were met. The “ancillary asset” concept, then, reflects a regulatory compromise: The digital assets sold (or promised) in conjunction with the scheme receive reduced disclosure requirements and access to trading on CFTC exchanges; the SEC gets regulatory authority over the former, and the CFTC gets regulatory authority over the latter.

Based on this construct and the Bill’s broad definition of “digital asset,” most digital assets would *appear* to qualify for treatment as commodities. But appearances can be deceiving. In this case, that is attributable to the Bill’s ancillary-asset exclusions, which have the potential to effectively negate the concept in its entirety. As noted above, these relate to whether the digital asset grants the holder certain rights in a business entity. In one sense, the exclusions represent a second application of the *Howey* test. The Bill suggests that this test is first applied to determine whether a token was “offered, sold, or otherwise provided to a person in connection with the purchase and sale of a security through an arrangement or scheme that constitutes an investment contract.” By considering the token holder’s rights in a business entity, and the managerial and entrepreneurial efforts of others with respect to that entity, the test is then applied *again* to ascertain—in part—whether the tokens themselves are, nonetheless, securities.²⁸

This *Howey* double-dose could pose problems. In the current market, many decentralized finance, or DeFi, companies mint their own crypto-assets called “governance

tokens” and award them to users of their smart contract platforms. Doing so incentivizes the use of these platforms by providing a return above and beyond the fees generated from being a liquidity provider.²⁹ These tokens often include various rights associated with the protocols in which they are intended to operate, such as the right to vote on protocol changes, to receive a portion of the protocol’s proceeds, etc. Considering the Bill’s ancillary-asset exclusions, the Bill’s failure to state whether “[a]ny other financial interest” in a “business entity” includes governance tokens capable of altering equity structure or redemption rights of a protocol through voting rights in on-chain governance is an unfortunate omission. Ancillary assets are presumed to be commodities under the Bill, but there is no express presumption that governance tokens are presumed to be ancillary assets.

Whether governance tokens are ancillary assets would seem to turn on what one considers to be a “business entity,” which is a requirement in every ancillary-assets exclusion. Many governance tokens provide holders with a right to interest or dividend payments from the protocol, to profit or revenue payments from the protocol, or to other financial interests in the protocol. Consequently, if a DAO or a smart contract protocol is construed to be a “business entity”—or is registered as a business entity under a state law such as Wyoming’s DAO statute—then, despite the Bill’s apparent intent, many of these governance tokens would not appear to qualify as ancillary assets presumed to be commodities after all. Given the present realities in the digital assets space, and the features associated with many tokens in the space, the entire ancillary-asset construct would appear to be directed at something that does not exist or, if it does, exists in a very limited sense.

Although it is conceivable that regulators might not consider a DAO or smart contract protocol to be a “business entity,” that is unlikely given the SEC’s track record.³⁰ SEC Chairman Gensler has repeatedly insisted that most digital assets are securities. That is abundantly clear in the SEC’s insider trading case against individuals at a prominent

crypto exchange, which alleges that 9 different crypto-assets are, in fact, securities.³¹ This risk exists alongside the already extant risk that the SEC would consider a DAO or smart contract protocol to be a “person” under the Investment Company Act.³²

Furthermore, one must also consider the potential consequences associated with taking the position that a DAO or smart contract protocol is *not* a “business entity,” or with deciding not to register a DAO or smart contract as a business entity in the form of a limited-liability company or partnership. A possible outcome is that the DAO or smart contract protocol would be viewed as a general partnership, thereby exposing its participants to unlimited liability.³³

Given these consequential and unresolved issues, current and prospective token issuers would be right to question whether the Bill’s ancillary-assets provisions really provide a workable path to reduced reporting obligations and trading on CFTC-registered exchanges. As a result, the Bill—or future legislation that embraces the ancillary-asset concept—would benefit from greater clarity around the ancillary-asset concept, especially its exclusions. For instance, is a “protocol,” a term the Bill utilizes in other provisions, a “business entity” for the purpose of the ancillary-asset exclusions? Similarly, is a DAO, which the Bill expressly designates as a business entity within the context of the Internal Revenue Code, also a business entity in the context of ancillary assets? Also, do voting rights in a protocol or DAO qualify as “any other financial interest” in an entity?

Until these and other bedrock questions are answered, the utility of, and ramifications associated with, the Bill will remain unclear, and the digital assets market will continue its long wait for much-needed guidance and certainty.

ENDNOTES

- 1 § 301 (Proposing a new Exchange Act Section 41(a), which would be 15 U.S.C. § 78(a)).
- 2 *Id.*
- 3 § 301 (Proposing a new Exchange Act Section 41(b)).
- 4 *Id.*
- 5 § 301 (Proposing a new Exchange Act Section 41(c)(1)).
- 6 § 301 (Proposing a new Exchange Act Section 41(c)(2)).
- 7 § 302 (Proposing a new Exchange Act Section 41(i)).
- 8 Although the Bill is somewhat unclear on this point, presumably an ancillary asset would receive the “commodity” presumption even if the issuer was *not required to comply* with the disclosure requirements, because the asset’s average daily trading volumes did not exceed the established thresholds for the given time frame, and/or the asset’s value was not primarily determined by the entrepreneurial or managerial efforts of the issuer or any person owning not less than 10% of any class of equity securities of the issuer. Such a presumption would seem to be supported by the fact that under the Bill, the CFTC’s jurisdiction is not limited to commodity interests but is extended to digital assets—including ancillary assets. § 403 (Proposing a new 7 U.S.C. 2(c)(2)(F), CEA § 2(c)(2)(F)).
- 9 § 301 (Proposing a new Exchange Act Section 41(b)(4)(A)).
- 10 § 301 (Proposing a new Exchange Act Section 41(b)(4)(C)).
- 11 § 403 (Proposing a new 7 U.S.C. 2(c)(2)(F), CEA § 2(c)(2)(F)).
- 12 *Id.*
- 13 § 401 (Proposing a new 7 U.S.C. 1a(15B), CEA § 1a(15B)).
- 14 § 401 (Proposing a new 7 U.S.C. 1a(15A), CEA § 1a(15A)).
- 15 § 101 (Proposing a new 31 U.S.C. 9801(2)).
- 16 *Id.*
- 17 § 401 (Proposing a new 7 U.S.C. 1a(15A)(B), CEA § 1a(15B)).
- 18 Compare § 404 (Proposing a new 7 U.S.C. 7b-4, CEA § 1a(15B)) to 7 U.S.C. 7(d), CEA § 5d, and 7 U.S.C. 7b-3(f), CEA § 5h.
- 19 *Id.*
- 20 Compare § 403 (Proposing a new 7 U.S.C. 6d(i), CEA § 4d) to 17 C.F.R. § 1.20.
- 21 § 404 (Proposing a new 7 U.S.C. 7b-4(c), CEA § 5i).
- 22 § 404 (Proposing a new 7 U.S.C. 7b-4(d)(3)(C), CEA § 5i).
- 23 § 403 (Proposing a new 7 U.S.C. 7a-2(c)(5)(D), CEA § 5c).
- 24 *Id.*
- 25 § 404 (Proposing a new 7 U.S.C. 7b-4(d)(4), CEA § 5i).
- 26 § 404 (Proposing a new 7 U.S.C. 7b-4(d)(4), CEA § 5i). Both the SEC and the CFTC have issued statements or enforcement actions classifying Bitcoin and Ether as commodities, but one should be cautious about regarding those actions as representing the final word on the matter.
- 27 Zack Seward, “SEC Chairman Jay Clayton’s Full Consensus: Invest Interview,” Coindesk (Nov. 28, 2018, 10:13 p.m.).
- 28 Notably, because the exclusions are dependent on whether the asset bestows the holder with certain rights in “a” business entity, each of the participants in the associated network ecosystem (e.g., sponsors, protocol creators, platform hosts, technology providers, developers, etc.) would need to be considered. Also, while the exclusions refer to “a business entity,” the Bill’s periodic disclosure requirements, discussed above, relate to the “issuer” of the ancillary asset.
- 29 Gemini, “[Defi Governance in Action](#),” Cryptopedia (Mar. 10, 2022).
- 30 See Section C of [the SEC’s DAO report from 2017](#), pp. 15-16. The definition of “issuer” is broadly defined to include “every person who issues or proposes to issue any security,” and “person” includes “any unincorporated organization.” 15 U.S.C. § 77b(a)(4). The term “issuer” is flexibly construed in the Section 5 context “as issuers devise new ways to issue their securities and the definition of a security itself expands.” *Doran v. Petroleum Mgmt. Corp.*, 545 F.2d 893, 909 (5th Cir. 1977); *accord SEC v. Murphy*, 626 F.2d 633, 644 (9th Cir. 1980) (“[W]hen a person [or entity] organizes or sponsors the organization of limited partnerships and is primarily responsible for the success or failure of the venture for which the partnership is formed, he will be considered an issuer. . .”). The DAO, an unincorporated organization, was an issuer of securities, and information about the DAO was “crucial” to the DAO Token holders’ investment decision. See *Murphy*, 626 F.2d at 643 (“Here there is no company issuing stock, but instead, a group of individuals investing funds in an enterprise for profit, and receiving in return an entitlement to a percentage of the proceeds of the enterprise.”) (citation omitted). The DAO was “responsible for the success or failure of the enterprise” and, accordingly, was the entity about which the investors needed information material to their investment decision. *Id.* at 643-44.
- 31 *Securities and Exchange Commission v. Wahi et al.*, Case No. 2:22-cv-01009 (W.D. Was.), ¶¶ 95-206.
- 32 15 U.S.C. § 78c(a)(9).
- 33 See, e.g., *Sarcuni, et al., v. bZx DAO et al.*, No. 22-cv-618, *Complaint* at 3 (S.D. Cal. May 2, 2022) (bringing suit against defendants asserting joint and several liability due to negligence in protocol hack on the theory that DAOs are most analogous to “another phrase in American law. . .[the] general partnership” where two or more individuals carry on as co-owners of a business and agree to share profits or losses.)



DIGITAL ASSETS DEFINED: HOW LUMMIS-GILLIBRAND WILL SHORE UP STABLECOINS

AUGUST 2022 WHITE PAPER

In this latest *White Paper* on our [Bill analysis](#), we underscore headline proposals in the Lummis-Gillibrand Responsible Financial Innovation Act (the “Bill”) regarding the issuance and regulation of a “payment stablecoin,” which the Bill defines as a digital asset issued by a business entity that is “redeemable on demand” for legal tender, “backed by 1 or more financial assets,” and is “intended to be used as a medium of exchange.”¹ Stablecoin regulation has received renewed attention after the collapse of the algorithmic stablecoin TerraUSD, which was not fully backed with cash or assets.

We finish this *White Paper* by highlighting unresolved questions that should be the focus of future stakeholder efforts to refine the Bill before aspects of it become law.

FEDERAL PREEMPTION TO ISSUE PAYMENT STABLECOINS

The Bill grants state- and federally chartered depository institutions the right to “issue, redeem, and conduct all incidental activities relating to payment stablecoins,” notwithstanding state regulations to the contrary.² Federal preemption conveys significant benefits for all depository institutions. The term “incidental activities” is defined broadly to include “management of required payment stablecoin assets,” market making, custodial services, settlement and clearing, and post-trade services, and “[a]ll other activities consistent with a safe and sound operation.”³

Absent these provisions or other sources of federal preemption, depository institutions wishing to issue payment stablecoins would face the prospect of complying with the laws of all 50 states, an onerous and potentially impossible regulatory burden depending on the overlap or conflict among state controls. By extending a federal right to issue payment stablecoins and conduct all “incidental activities” that attend such commercial activity, the Bill nips state protectionist forces in the bud and offers a welcomed and

much-needed degree of uniformity. It is notable, though not unprecedented, that the Bill, a federal statute, would preempt state law applicable to state-chartered banks in order to *expand* the powers of those state-chartered banks, underscoring that the Bill is intended to increase uniformity nationwide.

NON-BANKS MAY ISSUE AND REDEEM PAYMENT STABLECOINS AND ACCESS FEDERAL RESERVE SERVICES

The Bill also allows non-depository institutions to issue and redeem payment stablecoins and conduct all “incidental activities,” “consistent with a safe and sound operation, as determined by the appropriate regulator of the entity.”⁴ It also defines a path for payment stablecoin issuers to obtain national charters from the Office of the Comptroller of the Currency if they are exclusively engaged in: issuing payment stablecoins; providing safekeeping, trust, or custodian services; or activities incidental to the foregoing.⁵

Controversially, the Bill also contemplates extending Federal Reserve payment, clearing, and settlement services to these newly chartered stablecoin-only entities.⁶ Some have argued that extending Federal Reserve services to entities that do not comply with the same regulatory standards as traditional banks is unfair and exposes the Federal Reserve to unnecessary risks.⁷ Others argue that extending Federal Reserve services to all stablecoin issuers fosters competition and lends security and stability to these digital assets, which is one of the Bill's key objectives. Perhaps a compromise can be reached that includes further oversight for all Federal Reserve master account holders.

PAYMENT STABLECOINS MUST BE FULLY BACKED BY RESERVES

The Bill requires payment stablecoin issuers to maintain “high-quality liquid assets . . . equal to not less than 100 percent of the face amount of the . . . payment stablecoins.”⁸ Such assets include U.S. currency and other legal tender,⁹ demand deposits, balances held at the Federal Reserve bank, short-term Treasury securities, or “[a]ny other high-quality, liquid asset determined to be consistent with safe and sound banking practices, as determined by the appropriate Federal banking agency or State bank supervisor.”¹⁰

These provisions aim to mitigate the systemic risks associated with stablecoins that led to the collapse of TerraUSD. But to the extent the Bill creates payment stablecoins that function like traditional bank deposits but does not deem them to be such for fractional banking purposes, then a 100% backing requirement will all but eliminate any money-multiplier associated with those stablecoins. In other words, as traditional bank deposits migrate into segregated stablecoin reserve accounts held by the central bank, the deposit-backed funding for credit will be reduced.¹¹

This 100% backing requirement may eventually relax once lawmakers, regulators, and industry participants better understand stablecoin. The broad definition of “high-quality liquid assets” also leaves a fair amount of discretion and work to be done for federal and state regulators. The Bill does not, for example, adopt the detailed, three-tier definition of “high-quality liquid assets” employed by the federal banking agencies for purposes of the liquidity coverage ratio rule.¹²

ISSUERS MUST REQUEST PERMISSION AND PLAN FOR CONTINGENCIES

A depository institution desiring to issue a payment stablecoin must apply for permission from the appropriate federal or state banking agency not less than six months before the intended stablecoin issuance date.¹³ The application must include a tailored recovery and resolution plan, a flow

of funds explanation, a robust information technology plan, and operational design of the payment stablecoin, among other things. To prevent bottlenecks, the Bill compels the responsible government entity to make a reasoned decision on each application within four months and limits the grounds for denial to defined criteria.¹⁴

RECOVERY AND RESOLUTION PLANS FOR STABLECOIN ISSUERS

The Bill requires issuers to have “tailored recovery and resolution plans” in the event of distress, whether by resuming ordinary safe and sound operations or by winding down the issuer, as well as a plan for the redemption of all outstanding payment stablecoins.¹⁵ The Bill allows the Federal Deposit Insurance Corporation to be appointed as receiver of a covered depository institution, including a specially chartered stablecoin entity. If an issuer goes into receivership, stablecoin holders have a priority claim on reserve assets over all other claims on the institution with respect to any required payment stablecoin.¹⁶

SUPERVISION OF PAYMENT STABLECOIN ISSUER HOLDING COMPANIES

The Bill also adds a new Section 15 to the Bank Holding Company Act (“BHCA”) that would establish a “lighter-touch” regulatory framework for entities that control payment stablecoin issuers than the currently existing set of requirements for bank holding companies. The Bill clarifies that such stablecoin issuers are not “banks” for purposes of the BHCA and therefore that entities controlling them are not bank holding companies,¹⁷ yet commercial firms are prohibited from obtaining controlling interests in payment stablecoin issuers.¹⁸ The “controlling interest” definition is consistent with the existing definition of “control” under the BHCA, and is defined as either the ability to vote 25% or more of any class of voting securities, control of the election of a majority of directors, or the power to exercise a controlling influence over bank management or policies.¹⁹ Those with controlling interests must submit annual audited financial statements and descriptions of all affiliated or parent entities, among other things.

If the appropriate banking supervisor finds that it is in the public interest and has reasonable cause to believe it is necessary to protect customers of a depository institution, then the supervisor may conduct an examination of the controlling entity and force it to divest or sever their relationship with the stablecoin issuer, “if necessary to maintain safety and soundness.”²⁰ Certain other elements of the existing regulatory regime for banks and their affiliates within a bank holding company structure would also apply. For example, existing restrictions on transactions between

banks and their affiliates apply to payment stablecoin issuers pursuant to the Bill.²¹

MANY QUESTIONS LEFT UNANSWERED

Although the Lummis-Gillibrand Bill addresses many challenges in the stablecoin sector, it leaves important questions unanswered. Some of these open issues can be addressed through incremental regulation, but many can be addressed now (and probably should).

- Some non-banks that have issued stablecoins already may struggle to amass sufficient cash and other assets to comply with the Bill's 100% backing threshold. Will such entities be grandfathered into the system?
- State and federal definitions and enforcement of the requirement to hold "high-quality liquid assets" may strongly favor capital-rich depository institutions over non-depository entities. If that is the case, the Bill may strongly incentivize non-banks to become depository institutions. This may be undesirable or nonfeasible for many non-banks because it could require fundamental business changes, which could result in significant market exit. The Bill should provide more guidance to regulators regarding what types of assets are sufficiently "high quality" or "liquid." Will cryptocurrencies or other digital assets suffice? If so, under what circumstances? Will the sufficiency of the assets held in reserve to back the stablecoins be evaluated on a case-by-case basis, taking into account the financial strength of the issuer itself?
- The Bill requires stablecoin issuers to comply with the data privacy provisions of the Gramm-Leach-Bliley Act. That law requires covered banks to give customers the ability to opt out of having their nonpublic personal information shared with nonaffiliated companies.²² But the pseudonymous and yet public nature of blockchains could cause stablecoin issuers to inadvertently violate this aspect of Gramm-Leach-Bliley. For example, an issuer of a stablecoin compatible with public blockchains will have issues complying with Gramm-Leach-Bliley's opt-out requirement because nonaffiliated third parties can easily see a consumer's information whether or not they have opted out. Are there any carveouts to potential liability under these provisions? If preexisting stablecoin issuers apply for charters under Lummis-Gillibrand, will they still be required to comply with Gramm-Leach-Bliley?
- The Bill contemplates certain "national security threats" as per se "valid reason[s]" for terminating a Federal Reserve account.²³ However, the proposed language is vague, allowing a Federal banking agency to terminate an account if it believes "a specific customer or group of customers is, or [is] acting as a conduit for, an entity which . . . poses a threat to national security."²⁴ Certain senators have already introduced a bill to prohibit app stores from hosting apps that enable transactions using China's Digital Yuan.²⁵ The bill's sponsors argue that the Digital Yuan will be used to spy on its users, control and access users' financial lives, and infiltrate the American economy. These arguments are a preview of how stablecoin issuers utilizing foreign central bank digital currencies might be portrayed as threatening national security, regardless of whether the risks pointed to are real or substantial.

The Bill sets out a 100% reserve requirement for stablecoin issuances and requires banks to make monthly public disclosures that include a summary description of reserve assets, the value of such assets, and the number of total outstanding payment stablecoins.²⁶ It further provides that the applicable state or federal banking agency must verify the composition of the assets and the accuracy of the summary description.²⁷ Several potential issues flow from this requirement. First, it bears consideration whether a bank could have an account terminated if it submits what is deemed to be an inaccurate summary description (perhaps on multiple occasions). Second, if so, the Bill does not provide for any cure period, and it would be an open question as to how this may impact the account termination process. Third, would a depository institution's disclosure of any instances in which it failed to comply with any portion of the reserve requirements—as required by the Bill—be considered an admission for purposes of account termination and perhaps other regulatory actions?

ENDNOTES

- 1 § 101(a)(5).
- 2 See § 601 (creating a new 12 U.S.C. 4810(a)).
- 3 § 601 (creating a new 12 U.S.C. 4810(j)).
- 4 § 601(l).
- 5 § 604. While the question of whether the OCC can charter a non-depository fintech on its own authority remains unsettled, there is precedent for Congress to grant authority to the OCC to charter special-purpose national banks, including non-depository entities. See, e.g., 12 U.S.C. §§ 27(b) (bankers' banks); 92a (non-depository trust companies).
- 6 § 702.
- 7 See Kyle Campbell, "The Lummis-Gillibrand Crypto Bill Provision That Has Banks on Edge," *American Banker* (June 7, 2022).
- 8 § 601 (creating a new 12 U.S.C. 4810(b)).
- 9 Section 4810(b)(1) of the Bill includes "any other instrument defined as legal tender (as defined by 31 U.S.C. 5103)" as eligible high-quality liquid assets. Currently, 31 U.S.C. 5103 includes only "coins or currency," but this provision accounts for the Federal Reserve's and Treasury's ongoing consideration of issuing official U.S. digital currencies. The Bill is thus drafted to automatically include such U.S. digital currencies if they eventually come into being.
- 10 § 601 (creating a new 12 U.S.C. 4810(b)(7)).
- 11 See "[Stablecoins: Growth Potential and Impact on Banking](#)" at 12–13, Federal Reserve (Jan. 2022).
- 12 12 C.F.R. §§ 50.20 (OCC), 249.20 (Federal Reserve), 329.20 (FDIC).
- 13 § 601 (creating a new 12 U.S.C. 4810(e)).
- 14 § 601 (creating a new 12 U.S.C. 4810(e)). The Bill does not subject payment stablecoin issuers to existing resolution plan requirements for large banks pursuant to Section 165 of the Dodd-Frank Act; rather, it requires the OCC to establish new, "tailored," resolution plan requirements.
- 15 § 601 (creating a new 12 U.S.C. 4810(e)).
- 16 § 601 (creating a new 12 U.S.C. 4810(i)).
- 17 § 605(2).
- 18 § 605(2) (amending 12 U.S.C. 1841 with a Section 15(d)).
- 19 § 605 (amending 12 U.S.C. 1841 with a Section 15(a)(2)).
- 20 § 605 (amending 12 U.S.C. 1841 with a Section 15(e)).
- 21 § 604(2); see 12 C.F.R. Part 223 (Regulation W).
- 22 § 601 (creating a new 12 U.S.C. 4810(h)).
- 23 § 707(c).
- 24 § 707(c)(1).
- 25 *Defending Americans from Authoritarian Digital Currencies Act*, S. 4313, 117th Cong. (2022).
- 26 § 601 (creating a new 12 U.S.C. 4810(c)).
- 27 § 601 (creating a new 12 U.S.C. 4810(c)).



OCTOBER 2022 WHITE PAPER

In June 2022, Senators Kirsten Gillibrand (D-NY) and Cynthia Lummis (R-WY) introduced the [Responsible Financial Innovation Act](#) (the “Bill”), one of most comprehensive responses by Congress to date with respect to digital assets and their increasingly significant role in the U.S. economy. The legislation proposed a governance and definitional framework for digital assets across numerous areas of law, including taxation. While it is unlikely this Bill will be passed given the limited time remaining for the 117th Congress, the Bill’s support of positions endorsed by the cryptocurrency industry is welcome. And it is widely anticipated that aspects of this bipartisan Bill will be incorporated in subsequent legislation, and are likely to shape the debate in future Congressional sessions.

In this *White Paper*, we discuss some of the Bill’s most significant tax proposals.

SAFE HARBOR FOR DE MINIMIS TRANSACTIONS

The use of virtual currency to purchase goods and services is generally a taxable event to the purchaser under current law, and the resulting gain or loss is reportable to the U.S. Internal Revenue Service. The Bill would provide a long-sought-after de minimis exception to this rule by excluding from a taxpayer’s income any gain or loss recognized on certain “personal” (i.e., non-business, non-investment) transactions up to \$200. The intent of this proposal is to relieve taxpayers from onerous calculations and reporting obligations in situations where virtual currency is being used to make small purchases. While the sorts of “personal transactions” contemplated by the Bill include the use of virtual currency for transactions such as buying a cup of coffee, they would not include transactions in which virtual currency is sold or exchanged for cash, other digital assets, or securities or commodities.

Helpfully, the \$200 threshold would be subject to an annual inflation adjustment so the rule’s usefulness would not be eroded over time. In determining whether this threshold has been exceeded, all dispositions of virtual currency that are part of the same transaction or series of related transactions would be aggregated together. In other words, transactions in excess of \$200 could not be broken into smaller transactions in order to avoid tax reporting.

If a de minimis exception such as this were adopted, it would remove some of the practical barriers to the regular use of virtual currency by casual users. Notably, however, taxpayers coming within the scope of this exception would be unable to take advantage of losses triggered by such transactions.

Similar de minimis exclusions have been proposed. For example, the Virtual Currency Tax Fairness Act, proposed in July 2022 by Pat Toomey (R-PA) and Kyrsten Sinema (D-AZ), would provide an exclusion for gains of less than \$50 on similar transactions (although apparently would not also exclude losses triggered by such transactions).

RELAXATION OF TAX REPORTING REQUIREMENTS

The 2021 Infrastructure Investment and Jobs Act (the “IIJA”) created new tax reporting obligations related to digital assets beginning for 2023, as well as expanded the definition of “brokers” that are subject to the rules. Under these new rules, a broker is “any person who (for consideration) is responsible for regularly providing any service effectuating transfers of digital assets on behalf of another person.”¹

The Bill would clarify—and narrow—the definition of “broker” for reporting purposes to “any person who (for consideration) stands ready in the ordinary course of a trade or business to effect sales of digital assets at the direction of their customers.” Critically, this revised definition appears to answer the industry’s call to exclude persons presumably not intended to be swept within the definition of “broker”—including miners, stakers, and certain software and hardware vendors—as these persons typically would not have access to the relevant taxpayer information required to comply with such reporting obligations.

The definition of “broker” introduced by the IIJA has been widely criticized as overbroad and the subject of numerous Congressional proposals attempting to narrow it in a fashion similar to the amendment contained in the Bill. One of the most recent such proposals, Senate Bill 4751, was also cosponsored by Senator Lummis.

EXPANSION OF THE SECURITIES AND COMMODITIES TRADING SAFE HARBOR

A critical threshold question for foreign persons investing in the United States is whether they are considered “engaged in a U.S. trade or business” for U.S. income tax purposes—a question that does not always have an obvious answer. This answer, however, will determine whether the investor may be subject to U.S. income tax. Current law contains an important safe harbor that generally insulates foreign investors from U.S. income taxation for qualifying securities and commodities trading activities.²

The Bill would extend that safe harbor to expressly cover qualifying digital asset trading activities by foreign investors. Eligibility would require satisfying several technical conditions, including that the digital assets be of a kind customarily traded on a digital asset exchange. Intended to encourage foreign investment in the growing U.S. digital asset markets, the expansion of this taxpayer-favorable safe harbor would be a welcome development that would provide more tax certainty to investors and put the trading of digital assets on par with U.S. securities and commodities.

TAX-FREE LENDING OF DIGITAL ASSETS

Under current law, securities loans that satisfy certain requirements are generally tax-free.³ Loans of digital assets, however, generally are not covered by this statutory rule, which applies only to “securities” (as specifically defined for purposes of this rule).⁴ The Bill would extend the application of this existing rule to qualifying digital asset lending transactions. Accordingly, if this proposal were enacted, no gain or loss would be recognized upon either the loan or repayment of digital assets under this statutory rule (as long as the various technical requirements were met).

This proposal would be welcomed by the fintech and financial sectors and is similar to a proposal made by the Biden administration in March 2022 in its 2023 Fiscal Year Budget.

MINING AND STAKING INCOME

Finally, the Bill would require that Treasury publish formal guidance providing that digital assets obtained from mining and staking activities not be included in a taxpayer’s income until the year in which those digital assets are disposed of. Currently, the IRS takes the position that when a person successfully mines virtual currency, the fair market value of any reward received is taxable income as of the date of receipt. There is more uncertainty as to the current tax treatment of staking awards,⁵ so such a taxpayer-favorable clarification would be particularly welcomed by the industry and their tax advisors.

ENDNOTES

- 1 Internal Revenue Code Section 6045(c)(1)(D).
- 2 Internal Revenue Code Section 864(b)(2).
- 3 Internal Revenue Code Section 1058(a).
- 4 Internal Revenue Code Sections 1058(a) and 1236(c).
- 5 See *Jarrett et al. v. United States*, Docket No. 3:21-cv-00419 (M.D. Tenn. May 26, 2021).

REPRINT

WHAT THE FEDERAL GOVERNMENT IS DOING ABOUT STABLECOINS

AUGUST 2022 REPRINT (EXTERNAL PUBLICATION)

Over the weekend of May 7–8, 2022, Terraform Lab’s TerraUSD stablecoin (aka “UST”)—which was one of the top-three largest stablecoins by market share—plummeted to mere pennies from its previous \$1 peg. The damage was done by the following Monday. Investors had lost over \$18 billion invested (aka “locked”) into TerraUSD. Make that over \$40 billion when combined with the value of Luna, Terra’s native token.

While the future of TerraUSD and other cryptocurrencies hang in the balance, there is one thing readers can take to the bank: stablecoin regulation is coming. And at least some stablecoin issuers appear to welcome it.

HOW STABLECOINS WORK

TerraUSD’s crash wasn’t supposed to happen. Stablecoins are designed to be just that—stable. As an asset class, they are intended to shield holders from price volatility by pegging to a certain fiat currency like the U.S. Dollar. Most stablecoins do this by maintaining reserves in the form of “safe” assets such as cash, Treasury securities, or commercial paper. Issuers of stablecoins like Tether, USDC, and Binance USD maintain one-to-one reserves comprised of high-quality assets, allowing full redemption at \$1 to every holder in the event of a run.

As a prime example of the stability this can offer, following TerraUSD’s crash, Chief Technology Officer of Tether (issuer of the world’s most widely held stablecoin) reportedly tweeted that around 300 million Tether tokens were withdrawn in 24 hours “without a sweat drop.” Algorithmic stablecoins like TerraUSD, by contrast, are significantly under-collateralized and instead rely on demand-side arbitrage to stabilize the price.

Here’s how TerraUSD’s algorithm works: in the Terra ecosystem, users can swap \$1 of TerraUSD for \$1 of newly minted Luna (Terra’s native token), regardless of the market price of either token. If the price of TerraUSD falls below \$1, traders can “burn” their TerraUSD (i.e., permanently remove the token from circulation) in exchange for newly minted Luna. This allows users to capture the risk-free profit in an arbitrage-like transaction. As the number of TerraUSD in circulation decreases, the corresponding value should increase (theoretically) until it reaches equilibrium. The converse is also true where traders can burn Luna to mint more TerraUSD if the value of TerraUSD climbs above peg.

TerraUSD lost its peg a year prior in May 2021 when the value fell around 10% before quickly correcting as designed.

A common criticism of algorithmic stablecoins like TerraUSD is that they present greater risks compared to reserve-based stablecoins, in part due to reliance on human behavior and underlying user confidence that the algorithm will return the stablecoin to its peg. In this case, TerraUSD’s de-pegging began with several large withdrawals from Anchor Protocol (a decentralized savings, lending, and borrowing platform created by Terraform Labs that runs on the Terra blockchain). But rather than burning TerraUSD in exchange for newly minted Luna to arbitrage it back to peg, a panic ensued that resulted in a sustained, large-scale selloff that triggered a so-called “death spiral” for the algorithm. In other words, no one wanted Luna because everyone lost confidence in the algorithm.

CONGRESS IS CONSIDERING THE RULES OF THE GAME

Following TerraUSD’s precipitous crash, Treasury Secretary Janet Yellen reiterated her call for swift stablecoin regulation during her testimony during a Senate Banking Committee hearing. Secretary Yellen had already expressed her concern previously that stablecoins were subject to “inconsistent and fragmented oversight” and offered little actual assurance that the obligated entity had the ability to meet its redemption liabilities. “In times of stress,” Yellen warned, “this uncertainty could lead to a run.” As fate would have it, that is exactly what happened to TerraUSD. Secretary Yellen said it was “highly appropriate” to pass legislation addressing stablecoins and that “we really need a consistent federal framework.”

Even though legislative proposals have varied in approach, we have some idea of what this framework might look like. Multiple proposals have hit the congressional floor, and there are likely many more to come. The Lummis-Gillibrand Responsible Innovation Act, for example, takes a sweeping approach, and among many other things attempts to distinguish digital assets that are commodities (probably most stablecoins), which would be overseen by the CFTC, from digital assets that are securities to be overseen by the SEC. Other bills have taken aim at bolstering reserves and restricting stablecoin issuance.

Yet another proposal is reportedly in the works from the bipartisan duo of Representative Waters and Representative McHenry, who have neared a deal that would deliver tougher rules for the crypto industry generally. Consideration of this proposal has been met with some resistance from certain factions, resulting in more delay. Treasury Secretary Yellen is said to have raised concerns with Waters over how the proposal would address digital assets held in custody on behalf of consumers, specifically that Treasury wanted changes that would require digital wallet providers to segregate assets in order to ensure preservation in the event of the provider's bankruptcy.

THE BIG QUESTION: SHOULD STABLECOIN ISSUERS BE LIMITED TO BANKS?

One of the biggest sticking points for stablecoin legislation is whether issuers should be limited to traditional banking institutions—or at least subject to bank-like oversight and regulation. Several proposals look to the Office of the Comptroller of the Currency (OCC) as the regulating authority to issue a special license or bank charter to certain entities for the exclusive purpose of issuing stablecoins and performing incidental activities.

The possibility that the OCC would provide a license or charter to non-banks to issue stablecoins appears inconsistent on its face with the views set out in a November 2021 report on stablecoins published by the President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation (FDIC), and the OCC. To guard against "stablecoin runs" in particular, that report recommended that any legislation "should require stablecoin issuers to be insured depository institutions."

The legislative proposal being considered by Representatives Waters and McHenry supposedly would treat issuers more like banks.

THE EXECUTIVE BRANCH HAS ALREADY BEGUN ANALYZING STABLECOIN POLICY

While Congress puts chisel to slab, the executive branch and various federal agencies have already begun evaluating how best to regulate digital assets and crypto-related activities. On March 9, 2022, President Biden issued an Executive Order on Digital Assets (the "EO") outlining a first-ever, "whole-of-government strategy" for "addressing the risks and harnessing the potential benefits of digital assets and their underlying technology." Among many other reports and studies, the EO requested a report within 180 days (or by September 5, 2022) from the Secretary of the Treasury, in consultation with the FDIC and others, on the "implications of developments and adoption of digital assets." The report is to include specific policy recommendations including for "potential regulatory and legislative actions."

From the OCC's perspective, Acting Comptroller Michael J. Hsu agreed that "[g]etting stablecoins right from a regulatory policy perspective is important." In remarks delivered in spring 2022, Hsu compared the \$23 trillion U.S. economy—which is supported by \$2.4 trillion of capital circulating in the banking system—to the roughly \$2 trillion worth of crypto assets resting atop \$180 billion of stablecoins. Hsu said the relationship can be depicted by an upside-down pyramid where instability at the bottom can cause the entire structure to destabilize.

Hsu also echoed the conclusion in the President's Working Group report that a run risk is the leading risk to stablecoins. He discussed two approaches to mitigate run risk under our current regulatory framework. The first is based on money market regulation, which requires disclosure and sets asset holding requirements; the second is based on bank regulation and supervision.

If stablecoins were investments, then a money market approach could serve as "a starting point," Hsu remarked. But given the "notable limits" of money market regulation to prevent runs, as seen during the 2008 financial crises, "[a] banking approach would be more effective." To address the criticism that a banking approach would be inefficient and unduly burdensome to many would-be issuers, Hsu said that:

[i]f a stablecoin entity were tightly limited to just issuing stablecoins and holding reserves to meet redemptions, I would agree that the full application of all bank regulatory and supervisory requirements would be overly burdensome. Provided that the activities and risk profile of a stablecoin issuing bank could be narrowly prescribed, a tailored set of bank regulatory and supervisory requirements could balance stability with efficiency.

Hsu's "tailored" approach above is probably consistent with a licensing regime or limited charter structure with attending restrictions on a non-bank stablecoin issuer's activities. Yet Hsu has warned that a lower bar would make it "more likely [that] a risky issuer blows itself up sparking contagion across peers."

In a significant first step for the FDIC following the EO, the agency issued a letter to all its supervised institutions requesting notice of their intent prior to engaging in, or if currently engaged in, a "crypto-related activity." The FDIC defined "crypto-related activity" broadly and non-exhaustively to include the following: acting as a crypto-asset custodian, maintaining stablecoin reserves, issuing crypto and other digital assets, acting as market makers or exchange or redemption agents, and participating in distributed-ledger based settlement and payment systems. The agency said these activities are "known existing or proposed crypto-related activities engaged in by FDIC-supervised institutions." The FDIC hypothesized that a disruption in a crypto-related asset could result in a "run" on that asset that could "create a self-reinforcing cycle of redemptions and fire sales of financial assets, which, in turn, could disrupt critical funding markets . . . [and] have a destabilizing effect on the insured depository institutions engaging in such activities."

The SEC staff have also weighed in on accounting standards for digital assets. Most legislative proposals so far exclude stablecoins from the ambit of securities laws. Even still, the SEC staff expressed their views in Staff Accounting Bulletin No. 121 concerning entities that safeguard crypto assets for users. Those entities most report a liability on their balance sheet for the fair value of those assets, so says the SEC. Before this guidance, an entity generally would not report safeguarded digital assets on its balance sheet unless it controlled those assets. Several GOP lawmakers responded to this staff bulletin by sending a letter to the SEC arguing it amounts to improper rulemaking and makes crypto custody by banks "economically infeasible."

GOVERNMENT AND INDUSTRY MULL OVER A U.S. CENTRAL BANK-BACKED STABLECOIN

The United States has also begun exploring the potential role for a United States Central Bank Digital Currency (CBDC). Secretary Yellen has said that a CBDC could contribute to a more efficient payment system and may have the potential to mitigate some of the risks posed by "private" stablecoins. Biden's EO placed the "highest urgency on research and development efforts into the potential design and deployment options of a United States CBDC." Yellen said that a CBDC would present a "major design and engineering challenge that would require years of development, not months."

Beyond the massive technical feat, CBDCs face other hurdles including skepticism from some quarters of the banking industry. For example, in May 2022, the American Bankers Association (ABA) and Bank Policy Institute submitted separate letters arguing that the risks of a CBDC outweigh the potential benefits. These industry groups were responding to a January 2022 discussion paper on CBDCs from the Federal Reserve.

The Fed's paper discussed, among other things, the potential disintermediating effect a CBDC could have on traditional banks, which play a critical role in credit provision and other essential financial services. The Fed also raised the possibility, however, that this effect could be mitigated by designing a CBDC that is slightly less attractive than nondigital money by limiting interest-bearing capability or capping the amount an "end user" can hold. Assuming holdings were capped at \$5,000/\$10,000 per end user, the ABA's response letter estimated that even a non-interest-bearing CBDC would cause deposit losses upwards of \$720 billion/\$1.08 trillion—a large enough scale to destabilize the financial system.

In June 2022, Fed Chair Powell spoke of a U.S. CBDC in a positive light, stating that it could "potentially help maintain the dollar's international standing." Fed Vice Chair Brainard has also made the case for a CBDC with certain limitations; Fed Governor Waller has made the case against. The Office of Financial Research released a working paper concluding that "a well-designed CBDC may decrease rather than increase financial fragility."

This article first appeared in RealClearMarkets (RCM) and is reprinted with permission from RCM.



CFPB TO INVOKE “DORMANT AUTHORITY” TO SUPERVISE NONBANK FINTECH COMPANIES

APRIL 2022 ALERT

On Monday, April 25, 2022, the Consumer Financial Protection Bureau (“CFPB”) issued a [press release](#) announcing its intent to utilize a “dormant authority” under the Dodd-Frank Act to examine nonbank “fintechs” that the agency determines pose risks to consumers. This “largely unused legal provision” is found in 12 CFR 1091, a “procedural rule” finalized in 2013. The rule established a process by which nonbanks are given notice of a CFPB determination that they present risks to consumers and an opportunity to respond, after which the CFPB may determine the nonbank to be within the CFPB’s supervisory authority. In tandem, the CFPB announced a new procedural rule “to increase the transparency of [that] process” by “authoriz[ing] the release of certain information about any final determinations.”

The CFPB’s release cites familiar UDAAP principles as examples of risky conduct that can subject a fintech to supervision, stating that it may rely on, *inter alia*, complaints it receives, judicial opinions, administrative decisions, whistleblower complaints, state or federal partner information, or news reports to establish the necessary reasonable cause for action. The CFPB specifically points to its authority “to use traditional law enforcement,” including the possibility of “adversarial litigation.” And the CFPB notes its powers to conduct “supervisory examinations [to] review the books and records of regulated entities.”

The announcement comes weeks after the White House’s [March 9 Executive Order](#) (“EO”) touting a “whole-of-government” approach to assessing risks and benefits of digital asset technologies. Our prior [Alert](#), “[White House Issues Executive Order Calling for Inter-Agency Study of Digital Assets](#),” noted that the EO specifically highlights consumer and investor protection as a focus point for further research by relevant federal agencies (including the CFPB) over the coming months. The CFPB’s announcement signals its intent to take a more active role in the digital asset and broader fintech space, and to root itself firmly within the “whole-of-government” approach advanced by the Biden administration.

REPRINT

THE \$YEAR OF THE RUG PULL
(REAL CLEAR MARKETS)

MARCH 2022 REPRINT (EXTERNAL PUBLICATION)

Writing for Real Clear Markets, partner James Burnham and Coinbase Associate General Counsel Sumeet Chugani discuss a new type of fintech scam.

Writing for Real Clear Markets, partner James Burnham and Coinbase Associate General Counsel Sumeet Chugani discuss a new type of fintech scam.

Fraudsters have been at it since Ancient Greece. In 300 B.C., a Greek merchant named Hegestratos committed the first documented insurance fraud. He took out a large insurance policy on a grain-filled boat that would supposedly transport grain from Syracuse to Athens. But Hegestratos actually planned to set sail with no grain, sink his boat, and recover a hefty payout for both the (sunk) boat and the (nonexistent) grain. Unfortunately for Hegestratos, the boat's crew uncovered the scam and confronted him. Hegestratos ended up jumping overboard and drowned to his death.

Technology has changed dramatically since 300 B.C., but humanity has not. And as technology evolves, new opportunities for fraud arise. The invention of the telephone gave rise to telemarketer scams, while the adoption of email enabled phishing scams and instant notification of “foreign lottery winnings” across the globe. So it is with the explosion of innovation in cryptocurrency and decentralized finance, which has given rise to the increasingly common “Rug Pull.” The techniques are new, but the fraud is timeless—a promoter lies about a product, gets investor buy-in on the product's potential, dupes people into investing, and then abandons the project and rides into the sunset with investor funds.

A majority of rug pulls begin with anonymous developers creating new cryptocurrency projects—tokens or non-fungible tokens (“NFTs”)—and hyping that new creation to investors. For token offerings, fraudsters typically pair their new token with a leading cryptocurrency like Ethereum, and ask investors to swap that leading cryptocurrency for the token. The project's creators may even inject substantial amounts of the leading cryptocurrency into their project pool to bolster investor confidence and initially boost their newly created token's value. The fraudsters then promote the fraudulent offering through Discord, Reddit, and other social media. They may even create a website that sets forth certain indicia of a legitimate offering—such as a roadmap or white paper that purports to describe the token offering and where the project is headed.

To capitalize on investor enthusiasm and the modern phenomenon of meme investing, fraudsters will often link their projects to pop culture—a recent Squid Game rug pull

being a prime example—and generate buzz that their token is the next Dogecoin. Investors then rush to get a piece before the price skyrockets. And in a market where fortunes are sometimes made in minutes, FOMO can eclipse rationality. That is a recipe for fraud.

There are several types of rug pulls. One version is basically theft—promoters induce investors to put leading cryptocurrencies into liquidity pools, and then yank all the liquidity at once, generally using backdoors coded into the exchange. Another is basically fraud—developers hype a new token with false promises about its functionality or other features, then drive up the token's price and dump all of their tokens, making off with the profits. A third version is another species of fraud—developers hype a token and induce people to buy believing they can resell the token later, only to discover that the developer has made it impossible to sell—rendering it, for example, a one-way transaction. These scams are also sometimes accompanied by additional sorts of theft—such as when a developer connects to a recipient's wallet, obtains unlimited access, and drains all the funds along with any valuable NFTs.

One rug pull rang in the new year. Purporting to model itself after the SOS airdrop for high-volume users of OpenSea, \$Year tokens were airdropped to individuals on New Year's Eve based on how many Ethereum transactions they had completed over 2021 as a year-in-review “reward.” Using Etherscan to review the Ethereum smart contracts, each user verified the \$Year smart contract—hoping to not only receive rewards, but to increase the value of the reward token they had just received.

On the surface, everything looked legitimate. \$Year provided transparency into the code being executed at user interaction and there were no obvious red flags associated with the contract—no apparent, malicious code. But it turned out that a function titled “`_burnMechanism`” was actually a hidden weapon that allowed the creator to revoke ownership of the contract, make the new owner UniSwap V2, and prevent further sale of the token—allowing only token purchases. This limitation of transactions to purchases created an artificial price spike on decentralized exchange charts, causing even more people to buy. But then, immediately after the spike, the owner drained the pool of over 30 Ethereum and zeroed out the token.

* * *

Rug pulls are a new type of scam, but their fundamentals are not unique. For victims, current law thus provides potential options.

Depending on the specific facts and circumstances, victims could try to sue as a group using the class action rules that apply in federal court—typically the best forum for pursuing far-flung (and possibly overseas) fraudsters. The sorts of claims that victims might be able to bring are straightforward:

Common Law Fraud. Common law fraud is a claim that enables recovery when one is defrauded. It generally requires showing nine things, all of which are likely present in many rug pulls: (1) a representation of fact; (2) its falsity; (3) its materiality; (4) the representer’s knowledge of its falsity or ignorance of its truth; (5) the representer’s intent that it should be acted upon by the person in the manner reasonably contemplated; (6) the injured party’s ignorance of its falsity; (7) the injured party’s reliance on its truth; (8) the injured party’s right to rely thereon; and (9) the injured party’s consequent and proximate injury.

Conversion. Conversion is a civil claim for theft. It generally requires showing that someone took property without a right to do so or the owner’s permission to do so.

Fraud in the Inducement. Fraud in the inducement is basically a civil claim for taking property through lies. It generally occurs when a person tricks another person into signing an agreement to that person’s disadvantage by using fraudulent statements and representations.

Fraudulent and negligent misrepresentation. Fraudulent and negligent misrepresentation are claims that are basically about lying in connection with contracts—which could sometimes be present in a rug pull. Establishing a fraudulent misrepresentation generally requires proving that someone has knowingly said something false to induce a contract. Establishing a negligent misrepresentation generally requires proving (1) that someone said something false and (2) that the person making the representation had a relationship with the other person that required special care to ensure the representation was accurate.

Fraudulent concealment. Fraudulent concealment is another claim that exists in cases with a contract, where a party can show that the other party to the contract (1) concealed a material fact about the bargain, (2) while knowing about the material fact, and (3) that this fact is not something the victim could have readily discovered.

Unjust Enrichment. Unjust enrichment is a claim by someone who has conferred a benefit on someone else without receiving the restitution required by law. This claim usually arises when the claimant fulfills his or her obligations under a contract and the counter-party refuses to fulfill theirs. Depending on the facts and circumstances of a rug pull, this claim might be available, too.

* * *

Anywhere there is value, there is fraud and theft. Blockchain technology provides unique safeguards for digital assets—users can track the flow of value across the blockchain, they can scrutinize the code underlying their investments, and they have some ability to protect themselves. But sometimes bad things happen. The good news is that there are civil tools to deal with it. Victims need only deploy them.

Sumeet Chugani is an Associate General Counsel at Coinbase and James Burnham is a partner at Jones Day in Washington, D.C. The views expressed herein are the personal views of the authors alone.

Reproduced with permission. Published February 18, 2022. Copyright 2022 by Real Clear Markets.



MARCH 2022 ALERT

President Biden's executive order calls for "whole-of-government" approach to studying risks and harnessing potential benefits of digital asset technologies.

On Wednesday, March 9, 2022 President Biden signed a first-of-its-kind [executive order](#) (the "Order") addressing regulation of cryptocurrencies and digital assets in the United States. Without making any explicit policy changes, the Order establishes six areas of focus for further research and examination by relevant federal agencies in the coming months:

1. Consumer and investor protection;
2. Promoting financial stability;
3. Preventing illicit finance;
4. Advancing U.S. leadership in the global financial system;
5. Promoting financial inclusion and economic competitiveness; and
6. Encouraging responsible innovation within the digital asset space.

The Order calls for a coordinated, interagency process headed by the White House National Security Advisor and the Assistant to the President for Economic Policy. The broad array of federal regulatory agencies tasked with studying these issues and reporting on their findings signals that the Biden administration intends to provide clarity regarding the role of digital assets within the existing regulatory framework of traditional finance. The Order directs that initial reports from the Department of Treasury, the Financial Stability Oversight Council and the Department of Commerce are due in 180 days, with a final comprehensive report set for completion by March 9, 2023.

Notably, the Order instructs the Treasury Department and Federal Reserve to evaluate the design and potential deployment of a U.S.-issued Central Bank Digital Currency ("CBDC") as part of studying "the future of money" and ways in which the current financial system may fail to meet consumer needs. That evaluation will include whether legislative changes would be necessary for the United States to issue a CBDC. While a U.S. CBDC does not appear imminent, the fact the Administration "places the highest urgency on research and development efforts" regarding a CBDC means this is something to track closely in the coming months.

Overall, the Order suggests that the "all of government" approach to be taken will be measured and thorough, while pursuing a broad set of ambitions, including the potential for a "digital dollar" to be issued as official U.S. legal tender. The Order suggests a willingness to engage with industry stakeholders in crafting legislation and regulatory changes that will foster responsible innovation with the ambition of keeping the United States as the primary financial power. Of course, the promise of a deliberate and thorough process does not guarantee a light touch, but the terms of debate that have been set are promising compared to earlier political rhetoric. We will continue to monitor developments and share our thoughts with clients and friends as more concrete steps are taken in this process.



MARCH 2022 COMMENTARY

IN SHORT

The Situation: The U.S. Securities and Exchange Commission (“SEC”) has taken the position that many digital assets are securities subject to regulation under the U.S. federal securities laws, and has sought to make that position clear through the use of enforcement actions. In 2021, Ripple Labs, Inc. (“Ripple”) asserted that the SEC had not provided “fair notice” that the digital asset XRP was a security subject to regulation under the federal securities laws, and two Ripple executives challenged the SEC’s claims against them on extraterritoriality grounds.

The Result: On March 11, 2022, the U.S. District Court for the Southern District of New York denied the SEC’s motion to strike Ripple’s “fair notice” defense and rejected the SEC’s arguments regarding its viability. In a separate order, the court denied the individual defendants’ motions to dismiss, concluding that their offers and sales of XRP were sufficiently domestic for the U.S. federal securities laws to apply, and that the SEC had adequately pled its aiding and abetting claims.

Looking Ahead: The court’s rulings were preliminary in nature, and the SEC will still have to survive summary judgment and prove its claims at trial (absent a settlement). However, the court’s denial of the SEC’s motion to strike Ripple’s “fair notice” defense is significant, as it preserves a potential path to victory for Ripple and will, in some sense, allow Ripple to put the SEC’s efforts to regulate digital assets like XRP on trial. In addition, the court’s findings regarding the territorial reach of Section 5 provide some guidance to companies involved in the creation, marketing and sale of digital assets.

THE SEC'S ENFORCEMENT ACTION AGAINST RIPPLE

In December 2020, the SEC commenced an enforcement action against Ripple and two of its senior executives alleging that the defendants violated Section 5 of the Securities Act of 1933 through the unregistered offering and sale of XRP. Ripple argued that XRP is not a security subject to SEC regulation, and that even if it is, the SEC failed to provide Ripple with “fair notice” that its unregistered sales of XRP violated federal law. The SEC moved to prevent Ripple from asserting this “fair notice” defense. Separately, the individual defendants moved to dismiss the SEC’s claims, arguing that their offers and sales of XRP occurred abroad and were beyond the reach of the U.S. federal securities laws, and that the SEC failed to adequately plead its aiding and abetting claims.

The digital assets community was watching this case closely to see if the court would provide guidance on whether digital assets such as XRP are securities subject to regulation under the federal securities laws, and whether the SEC adequately put market participants on notice that they could be subject to potential claims. Market participants were also closely monitoring the individual defendants’ extraterritoriality argument, as the court’s decision had the potential to provide guidance on the criteria that should be used to determine whether the federal securities laws can be applied to offers and sales of digital assets, which often have significant foreign contacts.

RIPPLE’S “FAIR NOTICE” DEFENSE

Ripple asserts that it did not have fair notice that its distribution of XRP violated U.S. securities laws. Ripple points to, among other things, the SEC’s lack of action in 2015 when Ripple reached a settlement with the U.S. Department of Justice and the Financial Crimes Enforcement Network (“FinCEN”) that described XRP as a “convertible virtual currency,” and permitted future sales of XRP subject to the laws and regulations applicable to money services businesses. The SEC moved to strike this defense, arguing, among other things, that it was not required to provide specific notice of the illegality of Ripple’s conduct prior to commencing an enforcement action, and even if it was, the defendants had actual notice that their conduct violated the federal securities laws.

The court denied the SEC’s motion to strike, concluding that Ripple had raised serious legal questions as to whether it had “fair notice” that XRP was considered an “investment contract” subject to regulation under the federal securities laws (including because Ripple alleged that XRP was not sold as an investment and that its price was not tied to Ripple’s activities). The court also rejected the SEC’s argument that it would suffer undue prejudice if the defense was

permitted to proceed. The court concluded that Ripple had raised the defense in a timely fashion, and that it should therefore be permitted to proceed.

THE TERRITORIAL REACH OF SECTION 5 OF THE SECURITIES ACT

In their motions to dismiss the SEC’s claims that they engaged in unregistered offers and sales of securities in violation of Section 5, the individual defendants argued that their sales of XRP did not occur on domestic exchanges (but rather on digital asset trading platforms with worldwide operations) and that irrevocable liability for those sales was not incurred in the United States. The individual defendants argued that their offers and sales were therefore foreign (or at least “predominantly foreign”), and thus beyond the reach of the federal securities laws under the Supreme Court’s decision in *Morrison v. National Australia Bank Ltd* and its progeny (including the Second Circuit’s decisions in *Absolute Activist Value Master Fund Ltd. v. Ficeto* and *Parkcentral Glob. Hub Ltd. v. Porsche Auto. Holdings SE*). The SEC, on the other hand, argued that the individual defendants’ offers and sales did not qualify as “foreign” under Regulation S, or “predominantly foreign” under *Parkcentral*, and that Section 5 could therefore be applied.

In denying the individual defendants’ motions, the court used two different tests to analyze whether the SEC’s Section 5 claims were impermissibly extraterritorial. First, the court used the transactional test established by the Supreme Court in *Morrison* (rather than the criteria set forth in Regulation S as advocated by the SEC) to analyze whether the individual defendants’ “sales” of XRP were sufficiently domestic for Section 5(a) to apply. The court determined that the SEC adequately alleged that irrevocable liability for at least some of the sales was incurred in the U.S., as those sales purportedly occurred on trading platforms incorporated and based in the U.S., and that Section 5 could therefore be applied consistent with *Morrison*.

Second, the court applied a different test focused on the “location of the offerors” to analyze whether the defendants’ “offers” were sufficiently domestic to impose Section 5(c) liability. The court concluded that the SEC plausibly alleged that the individual defendants offered XRP in the U.S. because they resided in California when the offers were made and utilized a trading firm with an office in the U.S. to place their offers. Thus, the individual defendants’ offers were also sufficiently domestic for Section 5 to be applied.

The court also rejected the individual defendants’ argument that their offers and sales were so “predominately foreign” as to be outside the reach of the federal securities laws. The court concluded that since the offers and sales were made by U.S. residents and in some instances involved U.S.-based trading platforms and U.S. purchasers, applying

Section 5 would “enhance confidence in U.S. securities markets [and] protect U.S. investors” (quoting *Cavello Bay Reins. Ltd. v. Shubin Stein*).

The SEC’s Aiding and Abetting Claims

The court also denied the individual defendants’ motion to dismiss the SEC’s aiding and abetting claims. In doing so, the court rejected the individual defendants’ arguments that the SEC was required to plead that they knew Ripple’s conduct was illegal or improper. The court concluded that the SEC was only required to plead that the individual defendants knew the facts underlying Ripple’s alleged misconduct, not the legal implications of those facts. The court also explained that the SEC’s civil aiding and abetting claim did not require a showing of willfulness, and that reading a willfulness requirement into the statute would be inconsistent with the Dodd-Frank Act (which expanded rather than contracted aiding and abetting liability).

THREE KEY TAKEAWAYS

1. The court’s decision to deny the SEC’s motion to strike Ripple’s “fair notice” defense was a significant victory for Ripple; it will allow Ripple to place the SEC’s own conduct and statements regarding digital assets at issue later in the case. Market participants should watch for further developments on this defense as the case proceeds.
2. The court’s decision provides some indication of how Section 5 of the Securities Act may be applied to offers and sales of digital assets, which often have significant foreign components. If applied in other cases, the court’s reasoning could expose individuals affiliated with other unregistered digital assets to potential liability where their offers to sell emanate from the United States. Market participants should consider the court’s conclusions in structuring future marketing efforts.
3. While the court concluded that the individual defendants’ offers and sales were sufficiently domestic for the federal securities laws to apply, the court’s rejection of the SEC’s argument that Regulation S (rather than *Morrison*’s transactional test) should govern the extraterritoriality analysis for Section 5 claims was nonetheless a setback for the commission.



FINCEN WARNS INSTITUTIONS OF SANCTIONS EVASION RISKS

MARCH 2022 ALERT

As the U.S. government's economic sanctions against Russia continue to grow, regulators are calling on financial institutions to help detect and prevent attempts to evade these measures through the use of convertible virtual currencies (“CVC”) and other means.

The United States responded to the Russian military action in Ukraine by imposing extensive sanctions against Russia and Belarus. On March 7, 2022, the Treasury Department’s Financial Crimes Enforcement Network (“FinCEN”) issued an alert (“Alert”) urging financial institutions to be “vigilant” in preventing attempts to evade these sanctions. As the Alert explains, illicit actors will likely attempt to circumvent sanctions by concealing their identities via shell companies, transacting with presently unsanctioned banks, and utilizing CVCs to blur chains of custody. These types of alerts often serve as the basis for future enforcement actions.

RED FLAGS

FinCEN encourages firms to review traditional indicators of sanctions evasion and to share information under the USA PATRIOT Act. The Alert also advises financial institutions to consider context-specific red flags related to the Russia sanctions, including:

- Jurisdictions previously associated with Russian financial flows evincing a notable recent increase in new company formations.
- New accounts attempting to send or receive funds from a sanctioned institution or an institution removed from the Society for Worldwide Interbank Financial Telecommunication (“SWIFT”).

- Non-routine foreign exchange transactions indirectly linked to sanctioned Russian entities. For example, Russia’s Central Bank could engage import or export companies to conduct foreign exchange transactions on its behalf and obfuscate its involvement.

CVC CONCERNS

Although FinCEN recognizes that a direct governmental effort to utilize CVCs is unlikely, it notes that sanctioned individuals may attempt to move or conceal assets via CVC anonymizing tools and segmented transactions. FinCEN reminds financial institutions that CVCs trigger the same compliance obligations as fiat currencies. Red flags specific to CVCs include transactions linked to IP addresses in Russia and Belarus and the use of CVC exchangers in high-risk jurisdictions. Financial institutions should also remain alert to Russia-related ransomware campaigns.

The Alert reminds financial institutions of their obligations to file Suspicious Activity Reports when they detect activity designed to evade sanctions. Further, financial institutions should ensure their due diligence procedures address the sanctions-related risks linked to foreign “politically exposed persons” and their networks. Financial institutions should actively monitor the evolving sanctions situation and incorporate the above guidance into their risk-based compliance program.



FEBRUARY 2022 COMMENTARY

IN SHORT

The Situation: The U.S. Securities and Exchange Commission (“SEC” or “Commission”) has proposed amendments to Rule 3b-16 under the Exchange Act that would dramatically expand the definition of an “exchange” and eliminate the exemption provided under Regulation ATS for systems that exclusively trade government securities. It also has proposed related changes to various filing and operational requirements for Alternative Trading Systems (“ATSs”).

The Issue: By including systems using “communication protocols” and including systems that display and match non-firm indications relating to securities in the definition of an “exchange,” the proposed amendments, if adopted, would require many more systems, not currently subject to registration, to either register as an exchange or register as a broker-dealer and comply with Regulation ATS, thereby materially increasing the scope of systems subject to agency oversight.

Looking Ahead: If the amendments are adopted, systems previously excluded from exchange registration because they did not meet the definition in Rule 3b-16 and/or were not required to register as broker-dealers pursuant to SEC Staff no-action letters, including many fintech platforms, may no longer be able to avoid registration in some capacity.

THE SEC'S PROPOSAL

On January 26, 2022, the SEC released a [rulemaking proposal](#) that, among other things, would expand the definition of “exchange” under Rule 3b-16 of the Exchange Act. Under the current rule, which further defines some of the terms in the Exchange Act’s definition of “exchange” in Section 3(a)(1) of the Act, an organization or group of persons will be considered to be or provide an exchange if it: “(1) Brings together the orders for securities of multiple buyers and sellers; and (2) Uses established, non-discretionary methods (whether by providing a trading facility or by setting rules) under which such orders interact with each other, and the buyers and sellers entering such orders agree to the terms of a trade.” An entity or system that meets this definition must either register with the SEC as an exchange or register as a broker-dealer and comply with Regulation ATS. As the markets and the use of technology in them have changed significantly since the rule was first adopted in 1998, the SEC has proposed to amend this definition to encompass many of the types of platforms used today by market participants to facilitate trading in a variety of instruments.

While the current rule requires that, to be an exchange, a system must bring together “orders,” the proposed amended rule would require only that the system bring together “trading interest,” which would include both orders and non-firm indications of a willingness to buy or sell a security. Similarly, while the current rule provides that an exchange’s “established, non-discretionary methods” can be established by either providing a trading facility or by setting rules, the proposed amendment would include “communication protocols” as a means for meeting this part of the definitional requirement. Consequently, conditional order systems, Request for Quote (“RFQ”) systems, negotiated orders initiated via OMS/EMS scraping systems, and “stream axes” (IOI or firm, negotiated or auto-ex) could therefore all constitute an “exchange” under the amended rule. According to Commissioner Crenshaw, this would “remove a potential loophole” whereby system providers might label as non-firm trading interest orders that are actually firm in practice in order to avoid registration requirements or complying with Regulation ATS.

The proposal also would eliminate the current exemption provided under Regulation ATS for systems that exclusively trade government securities as defined under Section 3(a)(42) of the Exchange Act, in addition to those that trade repurchase and reverse repurchase agreements on government securities. ATSs trading government securities are not currently required to file public disclosures, nor are they subject to the operational transparency rules that apply to ATSs that trade NMS stocks, Regulation ATS’s Fair Access Rule (Rule 301(b)(5)) or the requirements of Regulation SCI. The proposed amendments not only would make all such government securities ATSs comply with these various

requirements, including filing a revised Form ATS-N, but also would, among other things, require all ATSs trading government securities or NMS stocks to make disclosures about the ATS’s interaction with related markets, liquidity providers, and activities the ATS undertakes to surveil and monitor its market, as well as make a new type of filing regarding their fees. Finally, the proposal would broaden the application of the Fair Access Rule for all ATSs by aggregating, for purposes of the transaction volume thresholds for application of the rule, the average transaction volumes of all ATSs operated by a common broker-dealer or by affiliated broker-dealers. For those ATSs meeting those thresholds, the SEC has proposed minimum standards for providing Fair Access.

IMPACT: REGULATORY OVERSIGHT, PRIOR GUIDANCE, AND BLOCKCHAIN IMPLICATIONS

The proposed amendments would significantly broaden the definition of what constitutes an “exchange” for purposes of SEC registration and oversight. For instance, changing “orders” to “trading interest”—which includes not only orders but also “any non-firm indication of a willingness to buy or sell a security that identifies at least the security and either quantity, direction (buy or sell), or price”—essentially covers all indications of interest (“IOIs”) submitted to any system, since the submission of a message that only identified the security and nothing else would be practically useless. (In fact, this proposed definition is even more broad than the definition of “actionable indication of interest” in Rule 600(b)(1) of Regulation NMS, which requires each of symbol, side, price equal to or better than the NBBO and a size at least equal to a round lot.) Consequently, any system to which IOIs are submitted could fall within the definition of “exchange” if it meets the other conditions of the proposed rule.

Expanding the means by which “established, non-discretionary methods” can be demonstrated to include “communication protocols” similarly will bring numerous previously excepted systems within the SEC’s jurisdiction. In the SEC’s view, “communication protocols . . . generally use non-firm trading interest as opposed to orders to prompt and guide buyers and sellers to communicate, negotiate, and agree to the terms of the trade. For example, if an entity makes available a chat feature, which requires certain information to be included in a chat message (e.g., price, quantity) and sets parameters and structure designed for participants to communicate about buying or selling securities, the system would have established communication protocols.” The SEC will take a broad view of “communications protocols,” which will include, but not be limited to: setting minimum criteria for what messages must contain; setting time periods under which buyers and sellers must respond to messages; restricting the number of persons a message can

be sent to; limiting the types of securities about which buyers and sellers can communicate; setting minimums on the size of the trading interest to be negotiated; or organizing the presentation of trading interest, whether firm or non-firm, to participants. Even if those communication protocol systems do not match counterparty trading interest, buyers and sellers using them can be brought together to interact and agree upon the terms of the trade. (This latter condition—agreeing to the terms of a trade—must still be met for a system to be considered an “exchange.”)

Other proposed changes to the rule, however, could operate to bring systems that do not match counterparties or enable them to agree to trade terms on the system within the “exchange” definition. In this regard, the proposed amendments would change the word “uses” established non-discretionary methods with “makes available” such methods. The SEC believes that this change is needed to capture Communication Protocol Systems within the rule because such systems take a more passive role in providing to their participants the means and protocols to interact, negotiate, and come to an agreement. It also believes the term “makes available” will make clear that, in the event that a party other than entity/group performing exchange functions performs any exchange function, the function performed by that party would still be captured for purposes of determining whether Rule 3b-16 applies to the entity/group. This essentially means that if an entity/group arranges with a third party to provide a trading facility or communications protocols, the third party’s activities will be considered to be part of the group’s activities for purposes of determining exchange status. Thus, there is an increased likelihood that a collection of entities providing disparate services connected in some way, even tenuously, to an eventual securities transaction could be considered part of a group constituting an “exchange.”

Perhaps most significantly, the inclusion of “communications protocol systems” within the definition of “exchange” may also bring platforms facilitating blockchain and digital asset transactions within the regulatory ambit of the SEC. If the system using a communications protocol “makes available” (such as by routing to) a platform through which parties can agree to the terms of a trade, this arguably could constitute an “exchange” under the amended rule. Pursuant to this expansive new definition, providing information concerning AMM contracts or participating as a liquidity provider with respect to a particular AMM pool may constitute a communication protocol subject to registration and reporting obligations.

Because Bitcoin does not appear to be considered a security, this expansive proposal likely does not interfere with the current Bitcoin ecosystem. But any attempt to regulate communication protocols that interact with Bitcoin could elicit legal challenges on many bases. These include challenges grounded in administrative law, as well as ones

potentially invoking the associational and expressional freedoms of the First Amendment.

Finally, the proposed rulemaking—particularly the “makes available” change—also may impact the validity of previously granted SEC no-action letters, including those relied upon by systems that operate in conjunction with registered broker-dealers and platforms. To the extent a system (collectively) falls under the new proposed definition of “exchange,” any prior relief excepting the system from having to register as an exchange or a broker-dealer may no longer apply. This could require matching systems, and potentially even some bulletin board systems, relying on existing no-action letters to seek updated guidance with respect to their potential registration obligations.

PUBLIC REACTION AND SHORT COMMENT PERIOD

Broadly speaking, the proposed amendments would appear to bring under the SEC’s exchange/ATS registration regime almost any electronic system that involves communications relating to any interest to ultimately enter into a trade. As such, the proposal is likely to face resistance from those who view them as jurisdictional overreach by the SEC. There has already been much criticism of the proposal in the press. Likewise, if enacted as proposed, the federal judiciary will almost certainly be tasked with fielding a litany of legal challenges. Given the Supreme Court’s increasing proclivity toward agency restraint and deference to the clear mandates of Congress, courts may be hesitant to permit the Commission to stretch the statutory limits of its power too far beyond the bounds of the Exchange Act.

Finally, despite the complexity of the proposal—the version on the SEC’s website is more than 650 pages long and contains more than 220 separate requests for comment on a variety of issues—the Commission has provided a short 30-day period for public comment on the proposed amendments. This could be particularly burdensome for those market participants who also are interested in other significant SEC rule proposals that have already been published or have been announced in the [agency’s regulatory agenda](#) and are likely to be proposed in the near future. While the short comment period led to a public spat between Commissioner Peirce and Chair Gensler at the open meeting at which the rulemaking was considered, Chair Gensler noted that the 30-day period would start upon publication in the *Federal Register*, which he said currently has a publication backlog ranging between six to eight weeks. Consequently, he suggested interested persons should start the comment process now, so that they could have a *de facto* comment period of closer to two months or more.

FOUR KEY TAKEAWAYS

1. The SEC's proposed amendments to Exchange Act Rule 3b-16 would ultimately lower the threshold of what constitutes an exchange and significantly increase the scope of systems subject to agency oversight, through registration as an exchange or through registering as a broker-dealer and complying with Regulation ATS.
2. The inclusion of "communications protocol systems" within the definition of "exchange" may bring platforms facilitating digital asset transactions within the regulatory ambit of the SEC, thereby subjecting them to new registration and reporting obligations.
3. Matching and trading systems relying on prior no-action letters may need to seek updated guidance with respect to their registration obligations, since the final rule may supersede or otherwise render moot prior agency guidance.
4. Because this proposal is so broad, and dramatically expands the Exchange Act's definition of "exchange," the proposal could face robust political and legal opposition from those who perceive these amendments as jurisdictional overreach by the SEC.

REPRINT

THE LEGAL REVOLUTION THAT MIGHT SAVE
CRYPTOCURRENCY

JANUARY 2022 REPRINT

The future of digital asset regulation is being written right now and we can all hope collaboration carries the day. But for those who believe that peace is best achieved through strength, contingent battle plans must be readied. And that means understanding the legal terrain on which any conflict would unfold. For now, opponents of regulatory overreach hold the high ground.

Over several years and three Supreme Court Justices, the law of federal regulation has changed dramatically and for the better. In a series of decisions about everything from veterans benefits to a nationwide eviction moratorium, the Supreme Court has curtailed the power of federal regulators in major ways. Here are two:

Major Questions are for Congress. The era of unelected administrators resolving major policy questions is over. Time and again, the Court has rejected attempts by agencies to do big things based on novel interpretations of old laws. Consider last summer's decision invalidating the CDC's so-called eviction moratorium in *Alabama Association of Realtors v. HHS* (2021). There, the Court rejected the CDC's unprecedented claim that an antiquated phrase from a decades-old health law empowered the agency to shut down the rental housing market nationwide. In the Court's words: "We expect Congress to speak clearly when authorizing an agency to exercise powers of 'vast economic and political significance.'"

Judges Decide the Law. Once upon a time, administrative agencies had broad latitude to interpret laws and regulations according to their preferred policy views. No longer. In a pair of recent decisions—*Kisor v. Wilkie* (2019) and *Niz-Chavez v. Garland* (2021)—the Supreme Court has made clear that judges must apply laws as Congress wrote them, according to "their ordinary meaning at the time Congress adopted them." Courts must confine agencies to their statutory limits rather than reflexively "defer to some conflicting reading the government might advance."

These principles weigh against interpreting old statutes to invest unelected agencies with broad authority over digital assets. Whether and how to regulate a \$2 trillion (and growing) industry poised to revolutionize the internet is plainly a major economic and political question. And Congress has not addressed—much less clearly addressed—digital asset regulation. Rather, digital assets do not fit cleanly within any existing statutory regime, which is no surprise with laws that largely date to the Great Depression.

The Securities and Exchange Commission illustrates how these principles might apply on the ground. Under the Securities Act of 1933 and the Securities Exchange Act of 1934, the SEC has jurisdiction to regulate "securities." Federal law defines the word "security" with a laundry list of terms (e.g., "stock," "bond," "debenture"), and the vague, catch-all term "investment contract."

Whether the SEC has jurisdiction over a digital asset typically turns on whether the asset falls within the catch-all—whether it represents an "investment contract." Federal law does not define "investment contract." But in a 1946 case called *SEC v. W.J. Howey Co.*—arising from people buying land in Florida while leasing it back to the seller for operation as a profit-generating orange grove—the Supreme Court defined the term "investment contract" as any "contract, transaction or scheme whereby a person [1] invests his money in [2] a common enterprise and is led to [3] expect profits [4] solely from the efforts of the promoter or a third party."

Under *Howey*, an investor therefore must (among other things) expect to reap profits "solely from the efforts of the promoter or a third party" for an "investment contract" to arise. Taken literally, that is a very strict requirement—profits must derive "solely" from someone else's work.

Perhaps unsurprisingly, then, lower federal courts have held that "solely" cannot be taken literally, reading that passage from *Howey* to require only that profits derive "predominantly," "primarily," "substantially," etc. from the efforts of a third party. The SEC, for its part, has embraced the broad view of the U.S. Court of Appeals for the Ninth Circuit that an "investment contract" exists whenever profits depend on "undeniably significant" efforts from management. The Supreme Court has never endorsed these expansive glosses, though it has advised that "form should be disregarded for substance and the emphasis should be on economic reality" in construing the securities laws.

The Supreme Court's recent shifts in administrative law support taking *Howey's* terms seriously—even if not literally. If major questions are for Congress and courts must apply the laws as written rather than leave agencies to fill the gaps, then it makes sense to interpret *Howey* narrowly in the context of digital assets. Limiting current law to arrangements where profits come "predominantly" or even "nearly solely" from another's efforts—rather than expanding it to all arrangements in which another's efforts play an "undeniably

significant” role—would restrict the SEC’s domain in a novel area and let Congress take the lead in creating new regulatory schemes.

The word “solely” might seem like an esoteric basis for reining in the SEC, but here is why it matters. Bitcoin and Ethereum—the two largest cryptocurrencies in the world—are likely not “securities” under a stricter view of Howey and should thus be exempt from SEC oversight. Both currencies operate on largely “decentralized” networks that do not depend on a small group of developers to function. So when someone buys Bitcoin or Ethereum, the purchaser stands to profit mainly from market forces (like when one buys gold). Bitcoin and Ethereum investors are not expecting profits “solely” (or predominantly, or substantially) from the efforts of others.

Perhaps that’s an easy case, so consider a harder one. Many tokens derive some value from the “efforts of others.” Investors often buy tokens for a variety of reasons: because the tokens have intrinsic value; because they think others will want the tokens later; because the token supplies a stake in some broader organization; and because the token’s creator is going to keep improving the network, enhancing the token’s value. Taking Howey seriously, the relevance of intrinsic value, market forces, or purchaser participation in enhancing a token’s value could prevent that token from being a “security”—even if the token’s creator plays an “undeniably significant” role in returning profits to investors.

Similar arguments could be made about each of the acronym agencies currently circling digital assets. Statutes need not fossilize in a fast-changing world, but they cannot mutate either. As the Supreme Court has repeatedly reaffirmed, the choice about whether and how to regulate new innovations is one that Congress has to make. Should the administrative state come for digital assets without clear statutory authority to do so, it will be charging up a steep hill indeed.

*Reproduced with permission. Published Jan. 13, 2022.
Copyright 2022 RealClearMarkets.com (202) 644-8780.*

REPRINT

THE BREWING TURF WAR IN CRYPTO REGULATION (COINDESKTV)

JANUARY 2022 REPRINT (EXTERNAL PUBLICATION)

Amid a growing influence of digital assets on Capitol Hill, partner James Burnham joined the hosts of CoinDesk TV's "First Mover" to discuss the potential problems of a crypto turf war brewing between U.S. enforcement entities. "Regulators can't just do whatever they want using statutes from the Great Depression that would include vague language that might arguably be applied to digital assets," he said. Mr. Burnham also explained why the SEC might be the most effective in offering regulatory clarity.

[WATCH THE FULL INTERVIEW BELOW.](#)





U.S. FEDERAL BANKING REGULATORS ANNOUNCE PLAN FOR CRYPTO-ASSET POLICY INITIATIVE

NOVEMBER 2022 ALERT

The interagency “policy sprints” are designed to give banks guidance on how to navigate crypto-assets moving forward.

On November 23, 2021, the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency issued a joint statement concerning the interagency crypto “policy sprints” that were first announced in May 2021. The stated purpose of the “policy sprints” is to develop and provide clarity on how banks can engage with crypto-assets.

The statement noted that through these “sprints,” agency staff with relevant subject matter expertise conducted preliminary analysis on certain issues:

- Developing a common vocabulary for the use of crypto-assets by banking organizations;
- Identifying and assessing risks in safety and soundness, consumer protections, compliance, and legal permissibility of potential crypto-asset activities; and
- Analyzing application of existing regulations and guidelines and identifying areas where additional clarification is necessary.

Based on their analysis, the agencies developed a regulatory roadmap for navigating activities involving crypto-assets, about which they intend to provide further information throughout 2022. The purpose of the roadmap is to provide clarity and guidance on the legality, expectations for safety, consumer protection, and compliance with regulations required for banking activities related to crypto-assets. The statement identified particular areas the agencies expect to provide guidance:

- Crypto-asset safekeeping and traditional custody services;
- Ancillary custody services;
- Facilitation of customer purchases and sales of crypto-assets;
- Loans collateralized by crypto-assets;
- Issuance and distribution of stablecoins, i.e., digital assets that are designed to maintain a stable value relative to a national currency or other reference assets;
- Activities involving the holding of crypto-assets on balance sheet; and
- Application of bank capital and liquidity standards to crypto-assets.

The statement does not indicate whether the “policy sprint” teams have completed preliminary analysis concerning any of the identified topics. Nor does the statement provide specific dates in 2022 by when the agencies expect to issue guidance. The statement follows recent remarks by Acting Comptroller Michael Hsu at the American Fintech Council’s Fintech Policy Summit 2021 concerning the regulatory framework for fintechs. The Acting Comptroller referenced the “policy sprints” as part of a broader set of forthcoming pronouncements—also to include chartering decisions and interpretive letters—concerning the “regulatory perimeter” for fintech.

The next steps stemming from the sprint will lay the foundation for how traditional and new finance interact. It remains unclear whether regulators, in allowing traditional finance to adapt to fintech, will impede development of fintech that goes beyond—and ultimately may supplant—core elements of traditional finance. In this sense, the policy statement marks “the end of the beginning” in what will be a pivotal time for crypto-assets and broader fintech.



REGULATING THE ETHER: LESSONS FOR THE MENA DIGITAL ASSET INDUSTRY FROM U.S. ENFORCEMENT ACTIONS

OCTOBER 2021 COMMENTARY

IN SHORT

The Situation: Regulators worldwide have taken varying approaches to define and shape the legal and regulatory landscape for digital assets. The United States has thus far largely relied on enforcement actions within its existing regulatory framework, and it has focused its attention on cryptocurrencies. The impact of U.S. enforcement ensnares people and organizations globally.

The Result: Regulatory gaps, the spectrum of approaches taken by global regulators, and the overlapping jurisdiction of enforcement agencies create a regulatory landscape that is complex and subject to constant change. Entities that have purposefully sought to avoid U.S. jurisdiction have nonetheless been subjected to U.S. enforcement action.

Looking Ahead: As the commercial prominence of digital assets increases, regulators will pay increasing attention to them. Market participants should expect an uptick in related enforcement actions, despite regulators' lack of clear or consistent messaging, and should glean what lessons they can from the United States' eight-year history of cryptocurrency-related enforcement actions to avoid some of the common pitfalls.

As the global digital asset industry continues to grow, regulators worldwide have increased efforts to define and shape the legal landscape through various approaches. In the UAE, for example, the Financial Services Regulatory Authority issued [guidance](#) in 2018 on regulating cryptoasset activities in the Abu Dhabi Global Market, and the Dubai Financial Services Authority announced in its 2021–2022 [business plan](#) that it would develop a regulatory regime for digital assets (including cryptocurrencies) in the Dubai International Financial Center. In 2019, Singapore passed the [Payment Services Act](#), which brings “digital payment token services” (also called “cryptocurrency dealing or

exchange services”) under the regulation of the Monetary Authority of Singapore. In 2020, the European Union proposed a regulation on [Markets in Crypto-Assets](#), which seeks to create a regulatory framework for cryptocurrency, among other things. And just last month, China [declared](#) all cryptocurrency transactions illegal.

The United States has thus far used enforcement actions under existing regulatory frameworks to address digital assets. Proponents of this approach argue that existing U.S. laws are already broad and clear enough to capture many digital assets. For example, under the U.S. Supreme Court

case *S.E.C. v. W.J. Howey Co.*, the term “security” includes an “investment contract” component, which exists if there is “[a] scheme involv[ing] an investment of money in a common enterprise with profits to come solely from the efforts of others.” Proponents argue this definition is broad enough to encompass many digital assets. Others argue that U.S. law is ill-suited to regulate the developing digital asset marketplace, and that legal gap-filling through legislation-by-enforcement does not set clear expectations on the front end.

Irrespective of the spectrum of approaches, it is not always easy to predict which regulator or regulators will assert their enforcement powers. In the United States, the SEC, which enforces federal securities laws, has been the most active U.S. regulator in bringing digital asset-related enforcement actions. But other U.S. enforcement agencies have also been active in this regard, including the U.S. Commodity Futures Trading Commission (“CFTC”), the U.S. Department of the Treasury’s Financial Crimes Enforcement Network (“FinCEN”), and the U.S. Department of Justice (“DOJ”), which involves itself when enforcement matters are alleged to be criminal violations of federal law.

As evidenced by its enforcement action against Ripple Labs, Inc. (“Ripple”), discussed in more detail below, the SEC is particularly unapologetic about its lack of front-end clarity regarding cryptocurrency regulation. Recent letters between SEC Chair Gary Gensler and members of the U.S. Congress further demonstrate the SEC’s awareness that current rules do not lead to a clear application of law for cryptocurrency and that there is a need to legislate a solution to fill in regulatory gaps. Indeed, Gensler has recently analogized the cryptocurrency market to the “Wild West,” calling for increased regulatory and enforcement scrutiny. Yet it is unclear whether the United States’ current practice of rule-making-through-enforcement will continue. U.S. regulators are expected to launch reports on the digital asset market, with proposed rules likely to follow on their heels. The role of future enforcement efforts may evolve if a more proactive regulatory regime begins to take shape.

Given the uncertainty created by the overlapping jurisdiction of enforcement agencies that define the regulatory landscape, market participants should glean what lessons they can from the cryptocurrency-related enforcement actions initiated within the eight years since the SEC’s first such action. This *Commentary* therefore offers five lessons based on recent digital asset-related U.S. enforcement actions. For market participants in the MENA region, these lessons may be particularly pertinent given: (i) the potential extraterritorial reach of certain U.S. regulators (read our recent *Jones Day Commentary* on this topic); and (ii) regional legislators may take cues from the United States’ approach as the local regulatory landscape develops.

LESSON #1: THE SEC MAY WELL CONSIDER YOUR DIGITAL ASSET A SECURITY

While the SEC has previously determined that Bitcoin is a cryptocurrency, some of its more recent actions make clear that the SEC applies securities registration requirements to certain other digital assets. In 2017, the SEC issued a report on its investigation of the DAO, a “decentralized autonomous organization” or “virtual” organization embodied in computer code and executed on a distributed ledger or blockchain. The SEC concluded that “DAO Tokens”—the DAO’s cryptocurrency offering—were “investment contracts,” and therefore securities, pursuant to *Howey*. The SEC noted that, unless an exemption applies, securities registration requirements apply to every entity that offers or sell securities in the United States, regardless of whether it is decentralized or relies on the automation of certain functions through a distributed ledger or blockchain.

The SEC has, perhaps most notably, demonstrated its willingness to define cryptocurrencies as securities rather than currencies in its ongoing enforcement action against Ripple. Despite vigorous counterargument by Ripple, the SEC has argued extensively that XRP—Ripple’s digital asset offering—was not currency because it did not qualify as “currency” under the federal securities laws, had not been designated as legal tender in any jurisdiction, and was never offered or sold by Ripple as “currency.” Rather, the SEC argued, XRP was an “investment contract,” and thus a security, under *Howey*.

Alternatively, other U.S. regulators may consider a digital asset to be subject to their jurisdiction. In 2020, the CFTC brought an enforcement action against a trading platform offering derivatives on certain digital assets. The CFTC claimed that the platform was subject to CFTC jurisdiction because those digital assets are “commodities” under federal statute. The CFTC also charged the platform with failing to register as a futures commission merchant (“FCM”) and violating CFTC regulations requiring FCMs to comply with federal anti-money laundering and know-your-customer obligations. The platform’s alleged violations led to charges by FinCEN and the DOJ as well.

LESSON #2: REGULATORS WILL CONTINUE PURSUING DIGITAL ASSET-RELATED ENFORCEMENT ACTIONS DESPITE LACKING CONSISTENT MESSAGING

U.S. regulators have been vigorously pursuing digital asset-related enforcement actions despite lacking consistent guidance. For example, a pillar of Ripple’s defense is the lack of contemporaneous, clear guidance from the SEC concerning when digital assets constitute securities. The SEC has responded that it was not required to issue clear

guidance on this issue before suing Ripple, and that in any event its report on the DAO placed Ripple on notice that XRP was a security. Ripple began selling XRP in 2013, and the SEC's report on the DAO was not issued until 2017. Thus, even if its report on the DAO created notice, the SEC is enforcing for conduct that predates the report.

The SEC is not the only U.S. regulator vigorously pursuing digital asset-related enforcement actions despite lacking consistent guidance. In 2020, the CFTC issued a [final rule](#) that, among other things, adopted a new definition of “U.S. Person” that is narrower in scope and eliminates certain look-through requirements for collective investment vehicles. However, the CFTC charged the above-mentioned derivatives trading platform even though its parent company was organized in the Seychelles and it had policies to prevent U.S. residents from trading. These charges demonstrate the CFTC's conviction that derivatives are subject to CFTC enforcement, even if the platform on which they are traded is operated from outside the United States and ostensibly takes measures to exclude U.S. residents.

LESSON #3: ACT CONSISTENTLY WITH YOUR DISCLOSURES

The SEC has been using enforcement actions to target trading platforms that make materially false and misleading statements about their business. For example, this year, the SEC [charged](#) DeFi Money Market (“DMM”), a platform that exchanged investors' Ether for redeemable tokens. DMM told investors that it would use their Ether to purchase and own collateralized loans generating a certain minimum interest, which investors could redeem based on the amount of their principal. DMM, however, did not actually own these loans—a corporate affiliate did. While investors ultimately did not suffer any loss and were paid their promised interest, the SEC sued DMM anyway, premised largely on the allegation that DMM did not act consistently with what it represented.

Also this year, the SEC [charged](#) BitConnect, a cryptocurrency lending platform, with defrauding retail investors through an unregistered offering. To attract investors, BitConnect represented that it would deploy a “trading bot” that would use investor funds to generate returns of as high as 40% a month. It also represented that investors could trade “BitConnect Coin” (“BCC”) for Bitcoin (and vice versa) on the “BitConnect Exchange” through peer-to-peer transactions. In reality, BitConnect siphoned off investors' money for its own benefit, engaged in a Ponzi scheme with investors' funds, and retained custody of most BCC tokens traded on its exchange. BitConnect also failed to tell investors that it had two types of commission for promoters, both of which were paid from investor funds. The SEC thus charged BitConnect for both alleged unfulfilled promises and alleged omissions of material information.

LESSON #4: BE TRANSPARENT AND REALISTIC ABOUT COMMERCIAL RISKS ASSOCIATED WITH DIGITAL ASSETS

U.S. regulators generally consider it incumbent upon participants to assess and disclose commercial risks to investors. For example, in its action against BitConnect, the SEC alleged that BitConnect advertised extraordinary returns through its “Lending Program” of up to 2% daily, with no negative returns for any day, and an average daily return of approximately 1%, or approximately 3700% on an annualized basis.

Similarly, in its case against DMM, the SEC alleged that DMM did not account for or disclose risks that fluctuations in the tokens' principal (Ether) would be realized as gains or losses when the tokens were redeemed. Instead, DMM used new investments to, among other things, offset the redemptions, rather than buying new collateralized assets as represented to investors.

LESSON #5: MIND YOUR GEOGRAPHY

The SEC has increasingly been willing to conduct digital asset-related enforcement actions against companies and persons with non-U.S. bases of operation and focus, even if they enact measures against selling products to U.S. residents. In the case of DMM, a Cayman Islands company, DMM's website was used to advertise DMM's initial coin offering (“ICO”), but the website was publicly available and not geographically restricted. DMM also expressly invited U.S. residents to participate in the first stage of the ICO. It attempted to limit the second stage of the ICO to non-U.S. residents by using an IP blocker, but that failed to work.

Likewise, BitConnect was an unincorporated organization that registered several companies in the United Kingdom, and its founder was an Indian national. To support jurisdiction, the SEC's complaint referenced the acts of BitConnect's worldwide network of promoters and their activities in the United States, which included soliciting new accounts from U.S. residents via social media and BitConnect's sponsoring of promotional events in the United States.

In the case of the above-referenced derivatives trading platform, the platform's parent company was registered in the Seychelles and the platform enacted measures—albeit ineffective—to prevent doing business with U.S. residents. One of the platform's cofounders was a U.K. citizen and Hong Kong resident, indicating the CFTC's, FinCEN's, and the DOJ's willingness to prosecute foreign nationals whose businesses engage with U.S. residents. These regulators cite several instances where the platform's cofounders sought to circumvent U.S. regulations, including by organizing the platform's parent company in the Seychelles where

it was allegedly easier to bribe regulators, asking U.S.-based trading firms to incorporate offshore entities to open trading accounts on the platform, and lying in depositions about tracking the platform's activities within the United States.

THREE KEY TAKEAWAYS

1. While it is difficult to predict whether local legislators and regulators will adopt the U.S. regulators' approaches to digital assets, market participants in MENA should engage with their advisors and regulators from an early stage to ensure they have—or at least can demonstrate that they sought to obtain—the appropriate level of guidance regarding the requirements applicable to their digital assets.
2. Until more consistent messaging evolves and is issued by the U.S. and global regulators, those operating in MENA should be cognizant of both local regulatory regimes as well as any international laws and regulations that may have extraterritorial effect on their enterprise.
3. If MENA-based market participants make inaccurate disclosures in connection with digital assets, whether by misleading statement or omission, they expose themselves to enforcement risk, even if investors do not actually suffer a loss.



OFAC ISSUES ADDITIONAL RANSOMWARE GUIDANCE AND DESIGNATES VIRTUAL CURRENCY EXCHANGE

SEPTEMBER 2021 ALERT

The U.S. Treasury Department has issued an updated ransomware advisory that highlights sanctions risks associated with ransomware payments and details proactive steps companies can take to mitigate these risks.

On September 21, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") took several [actions](#) relating to ransomware, including designating an exchange and issuing guidance. Last October, OFAC issued an [Advisory](#) highlighting the sanctions risks faced by parties that make or facilitate ransom payments to malicious cyber actors. OFAC's new [Advisory](#) supersedes its earlier guidance and reiterates these risks, emphasizing that facilitating ransomware payments on behalf of a victim may violate OFAC regulations, and provides guidance for ransomware victims.

For the first time, OFAC designated a virtual currency exchange for complicit financial services. OFAC noted that SUEX OTC, S.R.O. ("SUEX") facilitated transactions involving proceeds from roughly eight ransomware variants and that more than 40% of SUEX's "known transaction history is associated with illicit actors." OFAC indicated that it would continue to use its authorities to "disrupt financial nodes tied to ransomware payments. ..."

Under its updated guidance, OFAC underscored that companies that unknowingly make or facilitate a payment to a threat actor that is on or has a substantial nexus to an entity on the sanction list may be liable for a sanctions violation. OFAC stated that it will consider, in deciding whether to take enforcement action, whether a company has taken "meaningful steps" to reduce the risk of extortion through improving or adopting cybersecurity practices, specifically those highlighted in the Cybersecurity and Infrastructure Security Agency's ("CISA") September 2020 Ransomware

Guide. Meaningful steps include developing incident response plans, maintaining offline backups of data, and employing authentication protocols. OFAC noted that such efforts could be a "significant mitigating factor" in enforcement responses.

OFAC also explained that for ransomware payments that may have a sanctions nexus, it will consider a complete voluntary report of an attack to law enforcement or other relevant U.S. government agencies (including CISA or Treasury's Office of Cybersecurity and Critical Infrastructure Protection), "made as soon as possible after discovery of an attack, to be a voluntary self-disclosure and a significant mitigating factor" in enforcement responses. OFAC indicated that such a report and cooperation during an investigation would result in the agency being more likely to resolve an apparent violation with a nonpublic response.

OFAC's announced actions are part of a broader counter-ransomware strategy that focuses on the need for collaboration between the public and private sectors and close relationships with international allies.

The Agencies will begin examining financial institutions' BSA compliance programs to assess how well they integrate the AML/CFT Priorities once the new regulations incorporating the priorities become final. In the meantime, financial institutions should evaluate the related risks of the customers they serve, the products and services they offer, the activities they engage in, and the geographies where they operate to understand how they will incorporate the AML/CFT Priorities into their BSA compliance programs.

FinCEN's announcement aligns with President Biden's [National Security Study Memorandum](#), issued on June 3, 2021, [making anticorruption efforts a core national security interest](#), and indicating that domestic and foreign corrupt actors and their financial facilitators seek to take advantage of vulnerabilities in the U.S. financial system to launder their assets and obscure the proceeds of crime. For example, FinCEN's announcement highlights the sophistication of Mexican and Colombian drug cartels' reliance on professional money laundering networks in Asia (primarily China) that facilitate currency exchanges of Chinese and U.S. currency or serve as money brokers in trade-based money laundering, trafficking drugs, and laundering money in the United States. Accordingly, financial institutions' BSA programs should reflect heightened AML/CFT risks, including those posed by drug trafficking organizations, transnational criminal organizations, fraud, and corruption. Financial institutions should also ensure that their current policies concerning politically exposed persons and senior foreign officials are up-to-date. Moreover, FinCEN's particular mention of Russia and other nations believed to have facilitated cybercrime in, or against, the United States indicates that financial institutions should closely review and revise their policies and practices to ensure vigilance against malicious cyber actors.

The [Biden administration](#) and FinCEN have expressed heightened concerns about cyber-enabled financial crime, ransomware attacks, and use of virtual assets to undermine innovation and launder illicit proceeds. According to FinCEN, convertible virtual currencies ("CVC") are becoming "the currency of preference in a wide variety of online illicit activity," many of which have targeted financial institutions. Financial institutions should evaluate the typologies and red flags FinCEN has issued with regard to cybercrime and take steps to combat [ransomware](#) by identifying and reporting suspicious activity concerning how criminals and bad actors exploit [CVCs](#).

Additionally, because financial activity from human trafficking, human smuggling, and child exploitation may intersect at any point in the legal financial system, FinCEN has stated it is imperative for financial institutions to detect and report suspicious transactions by understanding the [current methodologies](#) that traffickers and facilitators use. Financial institutions should recognize the financial and behavioral

red flags associated with these activities in order to identify and report suspicious transactions, and may share information about the proceeds of one or more specified unlawful activities in reliance on the safe harbor protection from civil liability in the USA Patriot Act.

FOUR KEY TAKEAWAYS

1. FinCEN and federal and state financial institution regulators have stated they will issue new regulations within the next six months to implement the national AML/CFT Priorities. Those regulations will require financial institutions to integrate into their BSA compliance programs the novel and long-standing threats to the U.S. financial system and national security identified in the AML/CFT Priorities.
2. Financial institutions' compliance programs should reflect heightened AML/CFT risks, including those posed by drug trafficking organizations, transnational criminal organizations, fraud, and corruption.
3. Financial institutions should evaluate the typologies and red flags FinCEN has issued with regard to cybercrime and take steps to combat ransomware by identifying and reporting suspicious activity concerning how criminals and bad actors exploit convertible virtual currencies, which FinCEN views as "the currency of preference in a wide variety of online illicit activity."
4. Financial institutions should recognize the financial and behavioral red flags associated with human trafficking, human smuggling, and child exploitation in order to identify and report suspicious transactions.



SEC CHAIRMAN SIGNALS INTENSIFIED ENFORCEMENT AND REGULATORY SCRUTINY OF CRYPTO AND DEFI

AUGUST 2021 ALERT

SEC Chairman Gary Gensler suggests SEC will aggressively police crypto assets and decentralized finance (“DeFi”) platforms while seeking expanded authority to regulate these fast-growing industries.

SEC Chairman Gary Gensler took aim at a host of crypto-related topics in a recent [speech](#), signaling his agency will continue leveraging existing authorities to regulate digital assets while calling for expanded powers.

The SEC has long targeted digital assets, mostly through enforcement actions involving unregistered initial coin offerings. Gensler endorsed these efforts but acknowledged regulators have been hampered by their limited authority. Decrying a “Wild West” environment that undermines investor protection and national security, Gensler signaled the SEC would “take our authorities as far as they go” while also asking Congress for additional tools to regulate the crypto and DeFi industries.

Gensler also sent warning signals on a number of crypto-related topics:

- Echoing his predecessor, Gensler noted that “many [digital] tokens may be unregistered securities” and signaled the SEC would continue to police unregistered token offerings while also targeting derivative-like “crypto tokens . . . priced off of the value of securities.”
- Gensler explained that this may create registration obligations for platforms that support crypto trading and lending.
- He singled out “stablecoins,” which he suggested “may be securities and investment companies,” and indicated the SEC would “apply the full investor protections . . . of the federal securities laws to these products.”

While Gensler has spoken previously on crypto-related topics, market participants should pay close attention to these remarks, which are the clearest sign yet that the SEC will intensify and expand scrutiny of this developing industry under its new Chairman.

Though an increased SEC role may be welcomed by some, the CFTC has also staked a significant position regulating crypto. Indeed, Gensler’s remarks drew an immediate challenge from CFTC Commissioner Brian Quintenz, foreshadowing a potential inter-agency clash and highlighting the need for cooperation to ensure the agencies do not stymie innovation or undermine certainty.

Despite Gensler’s calls for new authorities, his reputation as an aggressive enforcer suggests the SEC is unlikely to wait on Congress to take action. Going forward, market participants should prepare for close scrutiny of the crypto and DeFi industries by the Enforcement Division, including in new areas the SEC has not targeted to date. Those who ignore Gensler’s warnings may find themselves facing an enforcement action in the years ahead. Indeed, just days after Gensler’s speech, the SEC announced its first-ever enforcement action involving DeFi technology and another involving an unregistered digital asset trading platform, emphasizing the Enforcement Division’s intent to actively police this space.



FINCEN ISSUES FIRST U.S. PRIORITIES FOR ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING

JULY 2021 COMMENTARY

The Situation: The U.S. Department of the Treasury's Office of Financial Crimes Enforcement Network ("FinCEN") issued the first national policy priorities for anti-money laundering and countering the financing of terrorism ("AML/CFT Priorities").

The Result: FinCEN and federal and state financial institution regulators (the "Agencies") have stated they will issue revised regulations within the next six months addressing how to integrate the national policy priorities into risk-based Bank Secrecy Act ("BSA") and AML/CFT compliance programs.

Looking Ahead: To prepare for implementing regulations, financial institutions should evaluate risks related to the AML/CFT Priorities connected to the customers they serve, the products and services they offer, and the geographies where they operate.

On June 30, 2021, FinCEN [announced](#) the first set of government-wide AML/CFT Priorities, as required by the Anti-Money Laundering Act of 2020 ("AML Act"). Consistent with the [National Strategy for Combating Terrorist and Other Illicit Financing](#), the AML/CFT Priorities reflect a mix of new and long-standing threats to the U.S. financial system and national security. These threats involve attempts to exploit perceived legal, regulatory, supervisory, or enforcement [vulnerabilities](#) in the U.S. financial system that may be associated with a particular product, service, activity, or jurisdiction.

The national AML/CFT Priorities FinCEN identified are, in no specific order: (1) Corruption; (2) Cybercrime, including cybersecurity and virtual currencies; (3) Foreign and domestic terrorist financing; (4) Fraud; (5) Transnational criminal organization activity; (6) Drug trafficking organization activity; (7) Human trafficking and human smuggling; and (8) Proliferation financing. In identifying these AML/CFT Priorities, FinCEN consulted the Department of

the Treasury's Office of Terrorist Financing and Financial Crimes, Office of Foreign Assets Control, and Office of Intelligence and Analysis, as well as the U.S. attorney general, federal and state financial regulators, law enforcement, and national security agencies.

Concurrent with the announcement of the AML/CFT Priorities, the Agencies issued an [interagency statement](#) explaining that the AML/CFT Priorities do not create any immediate changes to BSA requirements or supervisory expectations. Rather, the Agencies will revise their BSA regulations within six months to clarify how financial institutions should integrate the AML/CFT Priorities into their risk-based BSA programs. Financial institutions are not required to incorporate the AML/CFT Priorities into their risk-based BSA compliance programs until the effective date of these new regulations.



OCC VICTORY IN SECOND CIRCUIT NOT A CLEAR VICTORY FOR FINTECH CHARTERS

JUNE 2021 COMMENTARY

IN SHORT

The Situation: The Court of Appeals for the Second Circuit reversed the [judgment](#) of the Southern District of New York (“SDNY”) in [Lacewell v. Office of the Comptroller of the Currency](#). The Second Circuit ruled in favor of the Office of the Comptroller of the Currency (“OCC”), reversing on procedural grounds the SDNY’s decision enjoining the OCC from issuing special purpose national bank (“SPNB”) charters to nondepository financial technology (“fintech”) firms.

The Result: The Second Circuit did not rule on the merits of the challenge by the New York State Department of Financial Services (“NYDFS”), New York’s banking regulator, to the OCC fintech charter. The Second Circuit chose not to take a position on whether the “business of banking” under the National Bank Act (“NBA”) requires the acceptance of deposits as a condition to eligibility for an OCC charter. Instead, the Second Circuit dismissed the case without prejudice after deciding that the NYDFS lacked standing and that its claims were not constitutionally ripe.

Looking Ahead: The Second Circuit’s dismissal of the case on standing and ripeness grounds all but guarantees further litigation in the event the OCC grants a SPNB charter to a fintech company. However, both the NYDFS and the OCC have publicly announced their willingness to cooperate to address consumer protection, safety and soundness, and fairness issues. In the meantime, a fintech company applying for a SPNB charter should be aware that the OCC’s authority to issue such charters has not been decided by the courts, and any charter granted by the OCC will likely result in further litigation by state regulators.

On June 3, 2021, the Court of Appeals for the Second Circuit issued a decision in the OCC's appeal of the SDNY decision in *Lacewell v. Office of the Comptroller of the Currency* in which the NYDFS had successfully challenged the OCC's authority to grant SPNB charters to nondepository fintech companies. The Second Circuit reversed the SDNY's judgment and ordered dismissal of the NYDFS's complaint without prejudice. While this may appear to be a victory for the OCC, the reality is more complicated.

CHALLENGES TO THE OCC FINTECH CHARTER

The underlying dispute in *Lacewell* began in July 2018 when, in order to address business questions raised by the Second Circuit's decision in *Madden v. Midland Funding LLC*, the OCC announced its plan to issue fintech charters to nondepository fintech companies. The OCC's decision to issue fintech charters was in response to the fact that the *Madden* decision limited the ability of nonbank debt purchasers to benefit from the NBA's preemption of state usury law, which is key to the business models adopted by many fintech companies that are not themselves nationally chartered banks and which oftentimes partner with banks to originate loans, which are immediately sold to the fintech company. For an in-depth look at the background and significance of the complaint filed by the NYDFS in the SDNY, as well as the significance of the SDNY's judgment in favor of the NYDFS, see Jones Day's January 2020 *Commentary OCC Fintech Charter Headed to the Second Circuit*.

The OCC's fintech charter rules were almost immediately challenged by state government regulators in both New York, in *Lacewell*, and in Washington, D.C., in *Conference of State Bank Supervisors v. Office of the Comptroller of the Currency*. While the Washington, D.C., case was dismissed twice for lack of standing and ripeness, the NYDFS prevailed in the SDNY in *Lacewell*. In *Lacewell*, the SDNY held that the NYDFS's allegations that fintech charters would "lead to the preemption of state law and thereby reduce [the NYDFS's] regulatory power, to the detriment of New York consumers" and that the NYDFS "faces the prospect of losing revenue from assessments it currently levies against nondepository fintechs, which may opt to convert to a federal SPNB charter" were sufficient to confer Article III standing upon the NYDFS. *Lacewell*, Case No. 19-4271 at 8.

The SDNY further held that the NYDFS claims were ripe for review because the NYDFS "had sufficiently alleged that the OCC's execution of the fintech charter decision was imminent and that there was a substantial risk that the OCC could grant an SPNB charter to a nondepository fintech at any time, thereby injuring [the NYDFS]." *Lacewell*, Case No. 19-4271 at 5. Finally, the SDNY concluded that the term the "business of banking" in the NBA unambiguously requires federally chartered institutions to accept deposits. *Id.*

Following the SDNY judgment, the Conference of State Bank Supervisors ("CSBS") again filed a [complaint](#) against the OCC in the District Court for the District of Columbia seeking declaratory and injunctive relief, arguing that the OCC lacks the authority to issue fintech charters.

OCC APPEAL TO THE SECOND CIRCUIT

The OCC appealed the SDNY judgment, arguing, *inter alia*, that the SDNY erred in holding both (i) that the NYDFS had Article III standing and that the claims pursued by the NYDFS were constitutionally ripe and (ii) that the "business of banking" under the NBA unambiguously requires the receipt of deposits.

Finding in favor of the OCC, the Second Circuit held that the alleged risk of preemption of New York state law was too speculative to meet the requirements to confer Article III standing on the NYDFS because no nondepository fintech company had yet applied for a fintech charter (let alone been granted one), and therefore no state laws or regulations were preempted. The Second Circuit held the NYDFS claims were not constitutionally ripe for adjudication for similar reasons.

Further, the Second Circuit found no evidence that the OCC intended to grant any fintech charters imminently. The Second Circuit was similarly unpersuaded by the NYDFS's allegation that it faced a substantial risk of loss of revenue, holding that "until a nondepository fintech that [the NYDFS] currently regulates—or would otherwise regulate—decides to apply for an SPNB charter, this alleged assessment loss will remain purely conjectural or hypothetical, rather than imminent as the Constitution requires." *Lacewell*, Case No. 19-4271 at 11. Finding that the NYDFS lacked Article III standing, the Second Circuit did not address whether the "business of banking" under the NBA requires the receipt of deposits. (Nonetheless, the question of what constitutes the business of banking is increasingly being litigated in a variety of contexts. For example, on June 1, 2021, in *MoneyGram Int'l, Inc. v. Commissioner of Internal Revenue*, Case No. 20-60146, the United States Court of Appeals for the Fifth Circuit reiterated that for an institution to be considered a bank under the U.S. tax code, it must "be a bank under the common understanding of that term" and therefore must "recei[ve] deposits from the general public, repayable to the depositors on demand or at a fixed time.")

The Second Circuit's decision is a victory for the OCC but only with regard to the standing and ripeness questions that were decided. In practical terms, the decision can be viewed as a victory for the NYDFS, as it is hard to imagine any fintech companies seeking a fintech charter given the uncertainty because the court ruled for the OCC on procedural grounds only.

The Second Circuit's decision does not address the substantive question of the OCC's legal authority to grant a fintech charter to a company that does not take deposits. While the Second Circuit reversed the SDNY's judgment, the *Lacewell* decision provides insight into how the SDNY may decide future similar legal challenges if the standing and ripeness requirements are met. Likely, because of the possibility of further litigation on this substantive question, no fintech company has yet applied for a fintech charter.

Following the Second Circuit's decision in *Lacewell*, and likely as a direct result of that decision and the probability its complaint would again be dismissed for lack of standing, the CSBS filed an unopposed motion to stay its litigation in Washington, D.C. *Conference of State Bank Supervisors v. Office of the Comptroller of the Currency*, Case No. 1:20-cv-03797 [ECF 15].

THE REGULATORY HORIZON

Although the future of the fintech charter is not yet settled in the courts, recent public announcements by the Superintendent of the NYDFS and the Acting Comptroller of the Currency suggest that the regulators may coordinate and work together to address the financial needs of consumers, recognizing the need to address consumer protection, safety and soundness, and fairness.

In a [statement](#) issued on the day of the Second Circuit's decision, the Superintendent promised that the NYDFS would continue to “guard[] against any encroachment on the state regulatory system which is traditionally more consumer protective,” saying, “States are the vanguards of consumer protection which is more important now than ever given the global pandemic and resulting economic crisis which has disproportionately adversely affected communities of color and women.”

The Superintendent's statement looked to the new leadership at the OCC to work together with the states to address both safety and soundness and consumer protection, stating:

With new leadership at the OCC, we urge them to reconsider this ill-advised [fintech charter] program. It is incumbent upon us to work together in our dual state-federal financial system to ensure both safety and soundness of industry and protection of the consumers who rely on financial products and services.

On his first day in office, and before the Second Circuit decision was handed down, the Acting Comptroller of the Currency [announced](#) a review of key regulatory standards and matters that are pending before the OCC. The Acting Comptroller indicated that the OCC would take into account the full range of internal and external views: “I want to make sure that we distinguish the forest from the trees, that

changed circumstances due to the pandemic are considered, and that all alternatives are evaluated.”

In subsequent [testimony](#) before the U.S. House Financial Service Committee on May 19, 2021, the Acting Comptroller shared his perspective on licensing and charters, addressing fintech charters specifically, and indicating that the OCC must coordinate with the states and other federal financial regulators to find a way to consider how fintech charters fit into the banking system:

... Denying a [fintech] charter will not make the problem go away, just as granting a [fintech] charter will not automatically make a fintech safe, sound, and fair. I will expect any fintechs that the OCC charters to address the financial needs of consumers and businesses in a fair and equitable manner and support the important goal of promoting the availability of credit. Recognizing the OCC's unique authority to grant charters, we must find a way to consider how fintechs and payments platforms fit into the banking system, and we must do it in coordination with the FDIC, Federal Reserve, and the states.

For its part, the CSBS Executive Vice President has made clear that the CSBS is “confident that the courts will ultimately determine that Congress has not given the OCC [the] authority” to grant fintech charters and “encourage[d] the OCC to abandon its pursuit of the chartering of uninsured national banks.”

THREE KEY TAKEAWAYS

1. Any nondepository company that is granted a fintech charter by the OCC is very likely to face renewed litigation challenges brought by state regulatory agencies against the company and/or the OCC that will take time to resolve.
2. Because the Second Circuit did not address the underlying legal question as to whether the OCC has the authority to grant fintech charters to companies that do not take deposits, a fintech company cannot rely on obtaining a fintech charter to avoid the interest rate preemption effects of the Second Circuit's 2015 decision in *Madden v. Midland Funding LLC*.
3. Based upon recent public announcements, the future regulatory horizon for Fintech companies appears to be poised for greater focus on coordination and cooperation among the OCC, other federal financial regulators, and the states to address the financial needs of consumers, recognizing the goals to address consumer protection, safety and soundness, and fairness. But it remains to be seen whether the regulators can find a way, outside the courts, to consider how fintech charters fit into the banking system.



JUNE 2021 COMMENTARY

The surging interest in cryptocurrency continues to raise new legal challenges for market participants and interested parties. This is largely uncharted territory, so there's comparatively little case law. However, a recent federal court's decision in *United American v. Bitmain* provided some insight as to how courts would apply antitrust laws to cryptocurrency.

Jones Day partners Craig Waldman, Mark Rasmussen, and Chris Pace talk about the key takeaways from the court's decision and discuss the other potential types of crypto asset antitrust claims we might see in the months and years ahead.

[LISTEN TO THE PODCAST](#)



DEFI IDENTIFIED AS POTENTIAL FOCUS FOR CFTC ENFORCEMENT ACTION

JUNE 2021 ALERT

CFTC Commissioner asserts that Decentralized Finance (“DeFi”) likely violates the Commodity Exchange Act (“CEA”) and that the regulator should respond accordingly.

DeFi is an umbrella term encompassing a range of blockchain financial markets designed to offer financial services through a distributed platform that does not involve traditional financial intermediaries such as banks, exchanges, and brokerages. DeFi proponents argue that removing these intermediaries increases efficiency and grants consumers more control over their investments and trading activities. This is especially so in the cryptocurrency space. For example, over \$20 billion in cryptocurrency was traded using DeFi as of January 2021—a twenty-fold increase from the prior year. In response to this demand growth, DeFi platforms are quickly proliferating.

Perhaps because the DeFi floodgates are opening further, CFTC Commissioner Dan Berkovitz recently expressed significant reservations about DeFi platforms—even going so far as to say that those platforms, by their very nature, may violate the CEA.

In a [June 8 speech](#), the Commissioner stressed that the CEA requires derivatives like futures and options to be traded on CFTC licensed markets. Since DeFi platforms are unlicensed, the Commissioner could “not see how they are legal.”

Moreover, the Commissioner asserted that the unregulated platforms raise customer protection concerns. He emphasized that financial market intermediaries monitor for fraud, prevent money laundering, and safeguard deposits. He cautioned that in a pure DeFi system, none of these safeguards exist.

Commissioner Berkovitz also seemingly signaled that enforcement actions in the DeFi space may be imminent. He urged that financial regulators “not permit DeFi to become an unregulated shadow financial market in direct competition with regulated markets,” and that the “CFTC, together with other regulators, need to focus more attention to this growing area of concern and address regulatory violations appropriately.”

The CFTC’s actions follow the March 2021 publication by the Financial Action Task Force of its “[Draft updated Guidance for a risk-based approach to virtual assets and VASPs](#),” which adds proposed definitions for decentralized exchanges and decentralized finance and specifies who might be held liable for enforcing KYC requirements for DeFi platforms.

While “regulation by enforcement action” is far from ideal, any cases that do come will begin to rough out some parameters in the DeFi space for what may be out-of-bounds under the current rule sets. Further rulemaking will ultimately be necessary to get to a better fit. For the time being, market participants exploring DeFi should consider the opportunities before them with a particular focus on how well or poorly they fit within existing regulatory frameworks for banking, securities, and commodities.



CRYPTOCURRENCY TAX UPDATE: IMPACT OF NEW IRS GUIDANCE AND PROPOSED U.S. TAX RATE INCREASE

MAY 2021 ALERT

New Internal Revenue Service guidance on hard forks and a proposed tax rate increase on capital gains could significantly impact cryptocurrency holders.

The IRS recently clarified its position on the U.S. income tax treatment of a hard fork. A hard fork occurs when protocols on a blockchain change, causing a “fork” or splintering of the existing blockchain into two distinct ledgers. In 2019, the IRS asserted in Revenue Ruling 2019-24 that any unit of cryptocurrency received as a result of a hard fork and obtained via an airdrop was taxable to the recipient. As relevant here, an airdrop generally refers to the gratuitous, en masse distribution of (new) cryptocurrency units to existing holders. This combination of events is rare, however, and some holders may have taken a position based on the 2019 revenue ruling that a hard fork was not taxable in the absence of a corresponding air drop.

The recently released IRS Chief Counsel Advice 202114020 takes aim at that argument, stating that the receipt of new cryptocurrency units as a result of a hard fork is taxable to the recipient at applicable (individual or corporate) rates, regardless of how the new units are distributed or otherwise made available.

Another relevant tax development for certain cryptocurrency holders pertains to the IRS’s position that most cryptocurrencies are considered property—not currency—for income tax purposes. A key consequence of this position is that any purchase made with cryptocurrency is taxable to the purchaser to the extent of any gain in the cryptocurrency used for payment. In contrast, a purchase using cash is not taxable to the purchaser. This can lead to unexpected results for U.S. taxpayers. If the relevant cryptocurrency has

been held for at least one year, the gain is currently taxed at 23.8% for most individuals (regardless if held directly or through certain investment vehicles).

The Biden administration has recently proposed increasing the rate on capital gains for individuals from 23.8% to 43.4% for those making more than \$1 million. This increase would mean significantly higher tax bills for affected holders each time cryptocurrency is used as payment (as well as converted into another digital or fiat currency or otherwise disposed of in a taxable transaction), thus raising the stakes for taxpayers.

To date, the only published guidance on the U.S. tax treatment of cryptocurrencies and other digital assets is subregulatory.



MARCH 2021 ALERT

On February 26, 2021, the SEC's Division of Examinations released a Risk Alert to make digital asset market participants aware of recurring issues that have arisen in the course of recent examinations, and provide notice of the areas of focus for future Division examinations.

The Securities and Exchange Commission's ("SEC") Division of Examinations (the "Division") issued a [Risk Alert](#) on February 26, 2021, to identify recurring issues that Division staff have observed during past examinations of market participants in the digital asset industry. The Alert also provides guidance about what the Division will focus on for future examinations relating to digital assets. Because such Risk Alerts often presage enforcement actions, broker-dealers, investment advisers, and others engaging in digital asset securities transactions should review the Alert and, if needed, amend their supervisory and compliance systems to take the Division's guidance into account.

The Division highlighted six areas of primary risk for investment advisers, derived from examinations of investment advisers managing digital asset securities for clients both directly and through pooled vehicles:

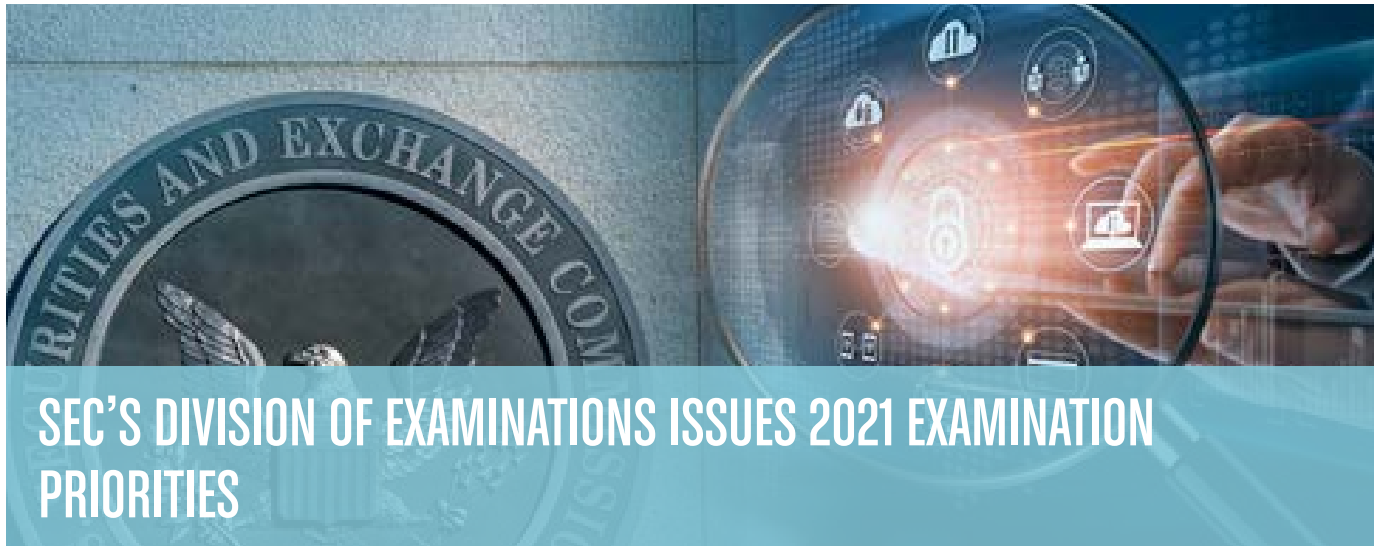
- Portfolio management (including whether digital assets are securities, and whether the adviser is fulfilling its related duties to clients);
- Books and records;
- Custody issues (including safekeeping and unauthorized transactions);
- Disclosures regarding the unique nature of risks associated with digital assets;
- Pricing client portfolios, including volatile digital assets; and
- Registration issues (especially calculating regulatory assets under management).

For broker-dealers, the Division pointed to six rather different areas of regulatory and compliance risk to consider:

- Safekeeping funds and operations (including custody);
- Registration requirements (e.g., for affiliates effecting transactions in digital asset securities);
- Anti-money laundering (especially tied to "pseudonymous aspects of distributed ledger technology");
- Offerings disclosure and diligence;
- Disclosing conflicts (e.g., a broker-dealer operates in multiple capacities); and
- Outside business activities of registered representatives that potentially should be overseen by the broker-dealer employer.

Additionally, the Division reinforced that operators of trading platforms should determine whether registration as a national securities exchange or alternative trading system ("ATS") is required. If they are an ATS, the Division will examine compliance with Regulation ATS. Further, transfer agents servicing digital asset securities are reminded of the need to comply with applicable transfer agent rules in the digital securities environment.

Acknowledging the rapid pace of financial innovation, the Division encourages market participants to speak with the agency's Strategic Hub for Innovation Technology about applicable regulations. The Division also encourages market participants to review their policies and procedures related to digital asset securities and to consider any necessary improvements to their supervisory and compliance programs.



MARCH 2021 COMMENTARY

IN SHORT

The Situation: The U.S. Securities and Exchange Commission's ("SEC") Division of Examinations (the "Division") issued its 2021 examination priorities ("2021 Exam Priorities").

The Result: The 2021 Exam Priorities set forth a non-exhaustive list of key areas where the Division intends to concentrate its resources in 2021.

Looking Ahead: SEC registrants, including broker-dealers and registered investment advisers, should use the 2021 Exam Priorities as a resource in administering and improving compliance programs, and expect Division examinations to include the 2021 Exam Priorities.

On March 3, 2021, the U.S. Securities and Exchange Commission's ("SEC") Division of Examinations (the "Division"), formerly the Office of Compliance Inspections and Examinations, issued its [2021 Examination Priorities \(the "2021 Exam Priorities"\)](#), detailing the nonexclusive areas on which it intends to focus its resources for examinations in the coming year. As in previous years, the 2021 Exam Priorities contain the broad thematic categories of retail investors, market infrastructure, the activities of the Financial Industry Regulatory Authority ("FINRA") and the Municipal Securities Rulemaking Board ("MSRB"), cybersecurity, and anti-money laundering ("AML") programs. This year, however, some areas of focus changed or were reorganized to highlight or expand upon particular areas the Division intends to target, including: (i) compliance with the newly implemented Regulation Best Interest ("Reg BI"); (ii) unique compliance issues related to the COVID-19 pandemic; (iii) operational resiliency and risks associated with climate change; and (iv) exposure to and preparations for the expected discontinuation of LIBOR.

Below is an overview of some of the more notable points discussed in the 2021 Exam Priorities.

RETAIL INVESTORS

The Division will continue to focus on retail investors, particularly senior investors and individuals saving for retirement, and will prioritize examinations of registered investment advisers ("RIAs"), broker-dealers, and dually registered or affiliated firms with respect to this class of investor. The Division also plans to assess investment products marketed to or intended for retail investors (e.g., mutual funds, exchange-traded funds ("ETFs"), fixed income (including municipal securities), and microcap securities (i.e., stock of companies that have a market capitalization of under \$250 million)).

Because the compliance date for Reg BI was June 30, 2020, the Division will move away from assessing implementation of Reg BI and instead will assess compliance

with Reg BI, prioritizing examinations of broker-dealers and RIAs to assess compliance with Client Relationship Summary filings (“Form CRS”). The Division will also assess Reg BI requirements related to complex product recommendations, sales-based fees, broker-dealers’ policies, and procedures regarding conflicts of interest, as well as RIA risks associated with fees and expenses, best execution, and undisclosed or inadequately disclosed compensation arrangements, among other things. See Jones Day’s July 2019 Commentary, [“Final Rule on Regulation Best Interest Now Complete,”](#) for additional information about the SEC’s adoption of Reg BI and Form CRS.

INFORMATION SECURITY

The Division will continue to prioritize cybersecurity, and will pay particular attention to whether firms have taken appropriate measures to safeguard customer accounts, oversee vendors and service providers, address malicious email activities, and manage operational risk, given the increase in remote operations in response to COVID-19 (e.g., controls surrounding online and mobile application access to investor account information, electronic storage of books and records, personally identifiable information maintained with third-party cloud service providers, and firms’ related policies and procedures).

OPERATIONAL RESILIENCY AND CLIMATE CHANGE

In light of substantial disruptions to business operations due to COVID-19, the Division will continue examining registrants’ business continuity and disaster recovery plans. Although it was not specifically listed as an examination priority, the Division notes that it will shift its focus to assess whether such business continuity and disaster recovery plans—“particularly those of systemically important registrants”—account for risks associated with climate change. The Division compared the scope of these examinations to the Division’s [post-Hurricane Sandy examinations](#). See Jones Day’s March 2021 Commentary, [“SEC to Review Climate-Related Disclosure: The Start of Things to Come,”](#) for additional information about how the SEC plans to enhance its focus on climate-related disclosure in public company filings.

FINTECH AND INNOVATION

Expanding on last year’s priorities, the Division will continue to focus on developments in the fintech area. In addition to focusing on compliance issues related to digital asset securities, electronic investment advice, and the use of “alternative data” (data gleaned from non-traditional sources) to

provide services to clients, the Division will focus on the use of technology to facilitate compliance with regulatory requirements in firms’ compliance programs, sometimes referred to as “RegTech.” The Division will also continue to examine market participants engaged with digital assets. See Jones Day’s March 2021 Commentary, [“SEC’s Division of Examinations Reiterates Focus on Digital Asset Securities,”](#) for additional information about the Division’s February 26, 2021 Risk Alert on digital asset securities.

AML PROGRAMS

Examinations of broker-dealers and registered investment companies for compliance with their AML obligations under the Bank Secrecy Act continues to be a priority for the Division. The Division will evaluate whether regulated entities are complying with requirements related to filing of suspicious activity reports, performing due diligence on customers, satisfying beneficial ownership obligations, and conducting independent assessments of their AML programs on a timely basis. See Jones Day’s January 2021 Commentary, [“Major U.S. Anti-Money Laundering Reforms Become Law,”](#) about significant reforms to U.S. AML laws that Congress recently enacted.

LIBOR TRANSITION

Following up on its June 2020 Risk Alert announcing its intent to examine registrants on their preparation for the expected discontinuation of LIBOR and the transition to alternative reference rates, the Division specifically listed the discontinuation of LIBOR as an examination priority in the 2021 Exam Priorities. The Division will examine registrants to assess their understanding of any exposure to LIBOR, their preparations for the expected discontinuation of LIBOR, and the transition to an alternative reference rate, in connection with registrants’ own financial matters and those of their clients and customers. See Jones Day’s June 2020 Commentary, [“SEC Staff Announces Examination Initiative on LIBOR Transition Preparedness.”](#) Among the specific topics prudent registrants will be prepared to address are the following: the impact of the LIBOR transition on asset valuations and models, suitability determinations for fixed-income offerings materially impacted by the transition, and the registrant’s understanding of the governing agreements underlying their LIBOR-linked investments.

RIAS AND INVESTMENT COMPANIES

RIAs

The Division will continue to review the compliance programs of RIAs, prioritizing examinations of RIAs that have

not been examined for a number of years or have never been examined. Compliance program elements that the Division will focus on include, among other things, the appropriateness of account selection, portfolio management practices, custody and safekeeping of client assets, best execution, fees and expenses, business continuity plans, and valuation of client assets for consistency and appropriateness of methodology. The Division will also continue to prioritize examinations of RIAs that are dually registered as, or are affiliated with, broker-dealers, or have supervised persons who are registered representatives of unaffiliated broker-dealers.

ESG Factors

The Division will pay particular attention to RIAs' disclosures (e.g., whether disclosures match the RIAs' actual strategies), processes and practices, advertising, and proxy voting policies and procedures and votes related to ESG products, such as mutual funds and ETFs, as well as qualified opportunity funds. Notably, the SEC has had a recent emphasis on ESG (e.g., the creation of the [new role of Senior Policy Advisor for Climate and ESG](#) and a [new Enforcement Task Force focused on climate and ESG issues](#)).

Registered Funds, Including Mutual Funds and ETFs

In reviewing registered investment companies, the Division will focus on funds' compliance programs and governance practices, with a focus on disclosures to investors, valuation, SEC filings, personal trading activities, and contracts and agreements. In focusing on valuation of registered funds, the Division will review funds for their investments in market sectors that experienced, or continue to experience, stress due to COVID-19 (e.g., energy, real estate, or products such as bank loans and high yield corporate and municipal bonds).

The Division will prioritize examinations of mutual funds and ETFs that have not previously been examined or have not been examined in a number of years. The Division will focus on actively managed ETFs, as well as mutual funds' liquidity risk management programs, particularly in light of COVID-19. The Division also emphasizes that it will review money market funds' compliance with stress-testing requirements, website disclosures, and board oversight.

RIAs to Private Funds

Examinations of RIAs to private funds (e.g., private equity, real estate, hedge, and venture capital funds) will focus on liquidity and disclosures of investment risks and conflicts of interest, in addition to other key areas applicable to operations of private funds such as information security, business continuity, and ESG. These examinations will also focus on

RIAs to private funds that have a higher concentration of structured products, such as collateralized loan obligations and mortgage-backed securities, and RIAs to private funds where "recent economic conditions" may have materially impacted the portfolio companies owned by the private fund (e.g., real estate-related investments). Other areas of focus will be preferential treatment of certain investors, cross trades, principal investments, distressed sales, and conflicts around liquidity, such as fund restructurings.

BROKER-DEALERS AND MUNICIPAL ADVISORS

Broker-Dealers

In addition to the Division's emphasis on broker-dealer compliance with Reg BI mentioned above, the Division's broker-dealer examinations will focus on a number of other areas, including compliance with: (i) SEC Rule 15c3-3 under the Securities Exchange Act of 1934 ("Exchange Act"), as amended ("Customer Protection Rule"), which requires broker-dealers to periodically calculate the net amount of cash owed to customers and deposit that amount into a segregated Reserve Account; (ii) Exchange Act Rule 15c3-1 ("Net Capital Rule"), which requires broker-dealers to maintain at all times adequate liquid resources to satisfy customer claims; and (iii) Rule 606 of Regulation NMS, which requires broker-dealers to disclose order routing information. Highlighting today's zero commission environment, the Division will continue to examine broker-dealers' use of payment for order flow, and will also focus on market maker compliance with Regulation SHO (short sales of securities) as well as the operations of alternative trading systems. In light of COVID-19, the Division also may examine broker-dealer funding and liquidity risk management practices.

Municipal Advisors

The Division will focus on the potential impacts of COVID-19 on municipal advisors and their clients, and whether municipal advisors adjusted their practices as a result of the pandemic. The Division will also evaluate municipal advisor compliance with obligations relating to their fiduciary duty to clients, conflicts of interest, documentation of the scope of engagement with clients, among other things. Further, the Division will examine whether municipal advisors have relied on temporary (and now-expired) exemptive relief related to Form MA filing requirements and direct placements of municipal securities, both enacted due to the pandemic. See Jones Day's June 2020 Alert, "[Temporary Exemption From Broker Registration for Municipal Advisors](#)," for more information on the temporary exemption permitting direct placements of municipal securities without broker-dealer registration.

MARKET INFRASTRUCTURE

Clearing Agencies and National Securities Exchanges

The Division will conduct examinations of clearing agencies, other entities exempt from registration as clearing agencies, and national securities exchanges, particularly emphasizing areas impacting the infrastructure of the securities markets (e.g., liquidity risk management, the effect of the LIBOR transition, and cybersecurity). The Division will also assess clearing agency and national securities exchange compliance with SEC Regulation Systems Compliance and Integrity's ("Regulation SCI") requirement to implement and enforce written policies and procedures intended to ensure, among other things, that the regulated entity's technology systems can maintain its operational capabilities.

Transfer Agents

The Division will continue to examine transfer agents' core functions, such as the timely turnaround of items and transfers, recordkeeping requirements, and safeguarding of funds and securities. In light of COVID-19, the Division will also focus on transfer agents' business continuity and disaster recovery plans, as well as their cybersecurity infrastructure. The Division intends to examine transfer agents that service microcap or municipal bond issues, blockchain or online crowdfunding portals, or engage in significant pay-agent activity.

THREE KEY TAKEAWAYS

1. Because topics identified in the 2021 Exam Priorities often become the subject of SEC investigations and enforcement actions, the 2021 Exam Priorities are a good reminder for broker-dealers, investment advisers, and other SEC-regulated entities to review their existing policies, procedures, and practices to determine where enhancements and additional attention may be needed.
2. Broker-dealers should pay particular attention to subject matter areas identified in the 2021 Exam Priorities as they review their sales practices and policies and procedures to ensure compliance with current regulatory requirements, namely those areas relating to retail investors and Reg BI, the LIBOR transition, the Customer Protection Rule, the Net Capital Rule, order routing and payment for order flow disclosures pursuant to Rule 606 of regulation NMS, activities involving digital asset securities, and liquidity risk management practices.
3. Registered investment advisers, including those to private funds, should particularly focus their regulatory and compliance reviews on funds in market sectors that experienced, or continue to experience, stress due to COVID-19, ESG-focused products, and liquidity events.



FINTECH: OCC TAKES SIGNIFICANT STEP IN PERMITTING NATIONAL BANKS TO USE INVN AND STABLECOIN TECHNOLOGY

JANUARY 2021 COMMENTARY

The Situation: On January 4, 2021, the Office of the Comptroller of the Currency (“OCC”) issued an [Interpretive Letter](#) permitting national banks and federal savings associations (“Banks”) to participate in independent node verification networks (“INVN”) and to use stablecoin, a type of cryptocurrency designed to have stable value, to conduct payment and other activities permitted for banks.

The Result: The OCC Interpretive Letter relies upon longstanding regulatory and case law precedent holding that the business of banking should evolve and adapt to technological changes as they occur. The OCC concludes that validating, sorting, and recording payment transactions by serving as a node on an INVN, issuing stablecoin, and exchanging stablecoin for fiat currency such as U.S. dollars are permissible bank-payment activities when conducted consistent with applicable law and sound banking practices.

Looking Ahead: The OCC Interpretive Letter is a significant step allowing for stablecoin and public blockchain integration into the traditional banking sector. By permitting Banks to participate in and use INVNs and stablecoins to carry out the business of banking, the OCC Interpretive Letter advances the potential for transfers of funds between financial institutions without the need for a government intermediary, increasing the speed and efficiency of domestic and cross-border payments.

RECENT CRYPTOCURRENCY REGULATORY DECISIONS

Global market capitalization of digital assets continued to grow in 2020 following robust growth in 2019, though this growth has experienced some volatility. The [2020 Annual Report](#) recently issued by the U.S. Financial Stability Oversight Council suggested that the “benefits and potential risks associated with digital assets underscore the importance of U.S. regulators adopting an approach to digital assets that will provide for responsible innovation in a manner that is safe, fair, and complies with all applicable laws” and further suggested that financial regulators should review existing and planned digital asset arrangements and their risks.

Additionally, in December 2020, the President’s Working Group on Financial Markets issued a [Statement on Key Regulatory and Supervisory Issues Relevant to Certain Stablecoins](#) providing an initial assessment of key regulatory and supervisory considerations for participants in significant stablecoin arrangements with a U.S. nexus that are primarily used for retail payments.

Federal financial regulatory and intelligence agencies continue to take steps to improve clarity around the regulatory framework for digital assets. For example, the Securities and Exchange Commission (“SEC”) and FINRA have issued [Joint Guidance](#) to broker-dealers holding that digital token custody and trading must fit within existing SEC and FINRA laws. The Financial Crimes Enforcement Network, Department of the Treasury (“FinCEN”), [proposed a rule](#) in December 2020 aimed at closing perceived anti-money laundering regulatory gaps for certain convertible virtual currency and digital asset transactions. The FinCEN proposed rule would require financial institutions “to submit reports, keep records, and verify the identity of customers in relation to transactions” related to virtual currency or digital assets held in digital wallets not hosted by a financial institution, known as “unhosted” wallets.

In September 2020, the EU released a [Draft Statement](#) discussing the regulation of markets in crypto-assets (“MiCA”). MiCA aims to set up a dedicated regulatory regime relating to crypto-assets offered to the public, together with a new regime applicable to service providers dealing in crypto-assets, while supporting financial innovation with pilot programs. The regulation on coin issuers and crypto-asset service providers would subject these entities to a single licensing regime across all member states without the need for “passporting.” It creates an open framework allowing cross-European offerings, but also notes that crypto-asset servicers will be subject to licensing rules and ongoing regulatory requirements. These new rules would not prevent existing and regulated financial institutions from offering these services when applying for new licenses. It should

be noted that asset-referenced tokens or electronic money tokens (i.e., stablecoin) would subject issuers to specific regulations, with particular attention paid to its customer base, number of transactions, size of the reserve used to back the tokens, among other criteria.

THE OCC INTERPRETIVE LETTER

The OCC has issued prior interpretive letters on permissible crypto-related activities by Banks, concluding, in an [Interpretive Letter](#) issued in July 2020, that Banks may provide [cryptocurrency custody services](#), and that Banks may hold deposits that serve as reserves for stablecoin, in an [Interpretive Letter](#) issued in September 2020.

The OCC Interpretive Letter issued on January 4, 2021, further advances the OCC’s regulatory analysis of digital assets clarifying that Banks may use INVN and stablecoin as permitted within the business of banking. The OCC has long held that payment activities are a part of the business of banking and consistent with a bank’s primary function.

An INVN is a shared electronic database where copies of the same information are stored on a decentralized network of computers, such as a distributed ledger where cryptocurrency transactions are recorded. Stablecoin is a digital asset designed to maintain a stable value, usually relative to another asset, such as a unit of fiat currency or a commodity, or relative to a basket of assets.

INVNs provide a faster and more efficient process for validating and recording financial transactions. Acting as a node on an INVN to transmit payment instructions and validate payments essentially has the same result as the current methods by which a centralized entity is used to validate payments. The OCC sees the basic functions of INVNs as basic banking functions of transmitting payment instructions and validating payments, and accordingly concludes that a bank may act as a node on an INVN to enable payment activities.

The OCC recognizes that stablecoin is a legitimate method of payment, similar to debit cards, checks and electronically stored value (“ESV”) systems. The OCC equates the use of stablecoins to ESV, each an electronic representation of the dollars on which they are based, and differentiates stablecoins from other popular cryptocurrencies that experience price volatility. According to the OCC, using INVNs and stablecoins may result in “a cheaper, faster, and more efficient means of effecting” payment, with a bank validating transactions on the INVN as a node, assisting in the conversion of stablecoins to dollars or issuing the stablecoin.

The OCC recognizes that there are both benefits and risks to INVNs and stablecoins and that while INVNs might provide stability and increase efficiencies in payment

mechanisms, banks should be sure to use INVNs in a safe and sound manner. Similarly, the OCC notes that any payment activities that involve cryptocurrencies, such as stablecoins, may increase fraud, operational and compliance risks. For example, the OCC warns that cryptocurrencies might present risks associated with anti-money laundering and counter terrorism laws. Growing technologies often require additional expertise and innovative processes to manage these risks, and the OCC cites past developments in electronic custody services and data processing services as examples of proper industry and regulatory adaptations.

FOUR KEY TAKEAWAYS

- The OCC's conclusion that it is legally permissible for banks to use INVNs and stablecoin technology in bank-permissible payment activities is a significant step in recognizing and integrating new technologies into traditional banking.
- Banks that want to participate in or use INVNs and stablecoin must possess the technological and other expertise to manage risks effectively. Banks should ensure they fully understand the associated fraud, money laundering, operational, technology, compliance, vendor, and other risks. Banks should revise their policies and procedures to address these risks.
- State-chartered banks should check their particular state's law regarding parity with national banks to understand how the OCC's Interpretive Letter may affect their legal authority to engage in INVN and stablecoin activities.
- Clients need to understand the legal, regulatory, and strategic risks associated with INVNs and stablecoin, and should develop appropriate policies and procedures that satisfy supervisory requirements.



OCTOBER 2020 ALERT

Federal court grants summary judgment to the SEC on its claim that sales of digital tokens constitute investment contracts under the Securities Act.

On September 30, 2020, U.S. District Judge Alvin Hellerstein granted summary judgment to the Securities and Exchange Commission (“SEC”) in its case against Kik Interactive, Inc., ruling that Kik’s unregistered offering of digital tokens called “Kin” was an offer and sale of securities without a registration statement or applicable exemption in violation of Section 5 of the Securities Act of 1933 (see *U.S. S.E.C. v. Kik Interactive, Inc.*, 19 Civ. 5244 (AKH), slip op. (S.D.N.Y. Sept. 30, 2020)).

In particular, the court ruled that the sale of Kin to the public constituted an “investment contract” and therefore a “security” under the standard articulated in the seminal *SEC v. W.J. Howey Co.* case (328 U.S. 293, 298-99 (1946)); namely, that the sale of Kin involved “an investment of money,” in a “common enterprise,” and with profits that are derived solely from the efforts of others (see *Kik*, slip op. at 8, quoting *Revak v. SEC Realty Corp.*, 18 F.3d 81, 87 (2d Cir. 1994)). In addition, the court concluded that the pre-sale of Kin to accredited investors using a Simple Agreement for Future Tokens (“SAFT”), which Kik argued was exempt from registration, and the subsequent public sale of Kin, were part of the same integrated offering, which therefore meant that the pre-sale did not qualify for the exemption.

This has been a closely watched case, given the number of similar offerings of cryptocurrencies that have been made without registration statements, and the court’s order is expected to guide other U.S. courts that are considering the issue, not to mention potentially emboldening the Commission to bring other, similar enforcement actions.

It follows another victory by the SEC earlier this year in a case against Telegram in regard to its sale of a digital token called Grams to accredited investors using SAFTs (*SEC v. Telegram Group, Inc.*, 448 F. Supp. 3d 352 (S.D.N.Y. 2020)). In that case, the court concluded that the initial sale and distribution of the Grams through SAFTs and potential resale by early purchasers in the secondary market were part of an illegal unregistered offering of securities. Together, the *Kik* and *Telegram* rulings present significant obstacles to companies seeking to offer digital tokens to the public outside the constraints of United States securities laws. Companies seeking to do so should obtain qualified legal counsel about the implications of these rulings.



OCTOBER 2020 ALERT

The prevalence, sophistication, and severity of ransomware attacks have increased anti-money laundering risks faced by financial institutions both as targets of ransomware attacks and as potential intermediaries in facilitating ransomware payments.

Executive: Ransomware is a cyber-attack in which malicious software blocks access to systems or data to extort payment in exchange for restoring access to information systems and data. Due to the proliferation of ransomware attacks, on October 1, 2020, the Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") issued an Advisory providing financial institutions with guidance on ransomware trends, red flags and reporting, and sharing of information to help in identifying and handling ransomware-related transactions. Financial institutions may wish to calibrate their anti-money laundering ("AML") compliance programs to ensure they address the full scope of risks associated with ransomware attacks, including risks arising from third-party intermediaries and virtual currency exchangers. The Department of the Treasury's Office of Foreign Assets Control separately issued parallel guidance concerning [sanctions](#) risks associated with ransomware.

Growth of Ransomware Attacks: Further to the government's continuing efforts to detect and prevent cyber-crime and ransomware attacks, FinCEN's Advisory on "[Ransomware and the Use of the Financial System to Facilitate Ransom Payments](#)" describes several trends: cybercriminals are increasingly targeting larger companies for higher payments, requiring payments using cryptocurrencies, most commonly Bitcoin, and sharing exploit kits and other resources to facilitate attacks. Although "traditional" ransomware attacks have typically demanded payment in exchange for restoring access to or availability of data or systems, attackers are increasingly using "double

extortion" schemes in which they also exfiltrate data and threaten to publish or sell it if the victim does not pay the ransom.

As the financial services sector has become an increasingly attractive target for ransomware attacks, the Group of Seven ("G7") issued a [statement](#) to coordinate efforts to combat ransomware urging all countries to implement the Financial Action Task Force standards to reduce criminals' access to and exploitation of financial services. Additionally, through the auspices of the Conference of State Bank Supervisors, together with the Bankers Electronic Crime Task Force and the U.S. Secret Service, U.S. state financial services regulators issued a [Ransomware Self-Assessment Tool](#) to help financial institutions reduce ransomware risks and identify security gaps.

Financial Intermediaries and Ransomware Payments:

The Advisory highlights risks to financial institutions and intermediaries that facilitate ransomware payments as well as red flags that should trigger suspicious activity reports ("SARs") to prevent ransomware-related activity. Attackers often demand that financial institutions and other intermediaries transmit ransom payments to a virtual currency exchange to purchase virtual currencies. The Advisory indicates that the growth of ransomware attacks has led to the creation of digital forensics and incident response companies and cyber insurance companies that provide services to victims of ransomware attacks, including facilitating payments. The Advisory cautions that facilitating ransomware

payments may implicate money transmission, SARs, and sanctions mandates.

The Advisory reminds financial institutions that AML rules require filing of a SAR based upon the knowledge or suspicion that a transaction involves funds derived from illegal activity or uses a financial institution to facilitate criminal activity, including payments made by financial institutions that are victims of ransomware.

Indicia or “red flags” of ransomware incidents include a digital forensics and incident response firm or cyber insurance company receiving or sending ransom payments; a customer receiving and then quickly sending funds to a virtual currency exchange; and a customer with no virtual currency history unexpectedly initiating a transaction with a convertible virtual currency exchange.

Financial institutions may wish to create a playbook to prepare for ransomware incidents by calibrating their AML compliance programs to address risks associated with ransomware attacks, including risks arising from third-party intermediaries and facilitators and virtual currency exchangers. Financial institutions should review and adjust their transaction and suspicious activity monitoring processes to detect and investigate red flags and decision-making regarding SARs filings.



OCC CONCLUDES THAT NATIONAL BANKS MAY PROVIDE CRYPTOCURRENCY CUSTODY SERVICES

JULY 2020 ALERT

The OCC sees holding the cryptographic access keys to control and transfer cryptocurrency as an “electronic corollary” of banking’s traditional safekeeping methods.

On July 22, 2020, the Office of the Comptroller of the Currency (“OCC”) concluded in [Interpretive Letter #1170](#) that national banks may provide cryptocurrency custody services to customers in both a fiduciary and non-fiduciary role. The OCC Interpretive Letter explains that providing custody services for cryptocurrency falls within the long-standing, traditional authorities of a national bank to engage in safekeeping and custody activities, including through electronic means.

Prior to the OCC Interpretive Letter, as banks entered the internet-era, the OCC permitted them to hold electronic assets, including encryption keys through secure web-based storage. See OCC Conditional Approval 267 (Jan. 12, 1998) and OCC Conditional Approval 479 (July 27, 2001). The OCC has historically viewed these activities as “an electronic expression of traditional safekeeping services by banks” and an extension of a national bank’s electronic banking authority under OCC rules. *Id.*

The OCC sees holding the cryptographic access keys that allow one to control and transfer cryptocurrency as an “electronic corollary of these traditional safekeeping activities.” In short, cryptocurrency custody services are viewed as a natural outgrowth of the safekeeping services, such as safe deposit boxes, that banks have long been authorized to provide. See *Colorado Nat. Bank of Denver v. Bedford*, 310 U.S. 41, 50 (1940).

The OCC indicates that it will support differing cryptocurrency custody methods, including the storage of either cryptographic access keys or cryptocurrencies transferred to the bank by the customer.

Before offering cryptocurrency custody services, a bank should have appropriately tailored policies, procedures, internal controls, and information security systems. A bank must ensure that it provides cryptocurrency custody services in a manner that controls risks and comports with pertinent rules and the terms of the *Comptroller’s Handbook on Custody Services*. Banks should employ specific risk management procedures to address the unique characteristics of particular cryptocurrencies. For example, OCC regulations on record keeping and confirmation requirements may apply to cryptocurrencies that are considered “securities” for purposes of the Federal securities laws. The OCC will review crypto-custody services as part of the normal supervisory process. Accordingly, the OCC recommends any bank that is considering cryptocurrency custody services to consult with the OCC before providing the services.



NO SEARCH WARRANT REQUIRED FOR RECORDS OF BITCOIN TRANSACTIONS, THE FIFTH CIRCUIT HOLDS

JULY 2020 COMMENTARY

IN SHORT

The Situation: While investigating a website for criminal activities, federal agents traced Bitcoin transactions and issued a subpoena to a virtual-currency exchange to identify customers of the site. Using that information, the agents obtained a warrant to search one customer's home where they discovered more incriminating evidence. The customer unsuccessfully moved to suppress the evidence, and he appealed.

The Result: The Fifth Circuit ruled that no search warrant is required to obtain records of Bitcoin transactions under the well-established doctrine that “a person generally has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”

Looking Ahead: Virtual-currency exchanges and other cryptocurrency intermediaries should ensure that they are complying with know-your-customer and anti-money laundering requirements and review their compliance policies and procedures to prepare for government subpoenas.

A Bitcoin user does not have a Fourth Amendment privacy interest in records kept by a virtual-currency exchange, the Fifth Circuit has held. In *United States v. Gratkowski*, No. 19-50492 (5th Cir. 2020), the Court ruled that federal agents could subpoena Bitcoin records from an exchange without first obtaining a warrant based on probable cause. Government investigators can also use sophisticated software to extract information from the Bitcoin blockchain without a warrant, according to the Court, because the blockchain is public.

Although Bitcoin transactions are often described as anonymous, they take place on a blockchain that publicly discloses how much Bitcoin changes hands, as well as the senders' and receivers' “addresses,” similar to bank-account

numbers. The blockchain does not disclose the identities of the users associated with these transactions and addresses. But government investigators can often discover users' identities from other sources: virtual-currency exchanges, hosted-wallet providers, and other cryptocurrency intermediaries that help people send and receive Bitcoin. These companies are required by law to keep records of their customers and transactions, just as banks do, under know-your-customer requirements imposed by anti-money laundering laws. To link an anonymous Bitcoin transaction with a user's real-world identity, the government can subpoena the intermediary.

That is what happened in *Gratkowski*. Federal agents investigating a website for criminal activities used forensic

software to extract a list of suspicious addresses from the Bitcoin blockchain. They then subpoenaed a virtual-currency exchange to trace Bitcoin payments made to those addresses back to customers. The exchange's response identified Gratkowski as one such customer. Using Gratkowski's Bitcoin records to establish probable cause, the agents obtained a warrant to search his home, where they uncovered more incriminating evidence. Charged with federal crimes, Gratkowski moved to suppress the evidence. He challenged both the Bitcoin records obtained from the public blockchain and the Bitcoin records obtained from the exchange. Gratkowski's motion was denied, and he appealed.

Judge Haynes, writing for the Fifth Circuit, decided the case under the well-established doctrine that "a person generally has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Courts have applied this "third-party doctrine" to customer financial records kept by banks. The Fifth Circuit reasoned that Bitcoin records kept by an exchange should be treated the same way. Both banks and exchanges are regulated financial institutions that "keep records of customer identities and currency transactions," although one deals in physical currency and the other in virtual currency. The third-party doctrine also applied to records found on the blockchain, where every Bitcoin user "can see every Bitcoin address and its respective transfers." Since Gratkowski had no privacy interest in his publicly-available Bitcoin records, the government did not need a warrant to run those records through forensic software.

Finally, the Fifth Circuit declined to treat Bitcoin records like cell-phone location records, which enjoy special Fourth Amendment protection under the Supreme Court's recent decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). Unlike cell-phone location records, which provide an "all-encompassing record of the holder's whereabouts," Bitcoin records have a limited financial scope more akin to traditional bank records, the Fifth Circuit held. And also unlike the cell-phone location records in *Carpenter*—which transmitted automatically from the phone to the wireless carrier—the records in *Gratkowski* resulted from the user's own affirmative acts when he conducted Bitcoin transactions.

Gratkowski is the first appellate decision to address Fourth Amendment privacy interests in virtual-currency transactions. While the opinion is not binding outside the Fifth Circuit, we expect the government to urge *Gratkowski's* reasoning in cases nationwide. Bitcoin users, virtual-currency exchanges, and companies that transact business on a public blockchain should therefore consider three practical consequences of the *Gratkowski* decision (in the Key Takeaways below):

THREE KEY TAKEAWAYS

1. **Virtual-currency exchanges should prepare for government subpoenas.** Virtual-currency exchanges, hosted-wallet providers, and other cryptocurrency intermediaries should have personnel and plans in place to respond to subpoenas and ensure compliance with know-your-customer requirements and anti-money laundering laws. It will be better to identify and remedy any gaps in compliance before subpoenas come.
2. **Some Bitcoin users may seek out products and services that enhance user privacy.** The *Gratkowski* decision may spur some Bitcoin users to seek out alternate methods of transacting that enhance user privacy, such as other forms of cryptocurrency that have privacy features Bitcoin lacks, or services that allow Bitcoin users to obscure transaction details.
3. **Blockchain users should be aware that transactions on public blockchains can be viewed by everyone.** The *Gratkowski* case demonstrates that sophisticated forensic software can reveal much about transactions made on a public blockchain. This is undoubtedly positive when it discourages or prevents criminal conduct. However, all blockchain users should keep in mind that transactions on public blockchains can be viewed by everyone and act accordingly. When there is a lawful reason to keep transactions confidential, for instance, legitimate businesses should consider whether a public blockchain is the right platform and should remain alert to potential threats from cybercriminals.



DIGITAL ASSETS DEFINED: FEDERAL AGENCIES WEIGH RESPONSE TO PRESIDENT BIDEN'S EXECUTIVE ORDER ON DIGITAL ASSETS

OCTOBER 2022 WHITE PAPER

On March 9, 2022, President Biden issued Executive Order 14067 (“EO”), “Ensuring Responsible Development of Digital Assets.” The EO, which we discussed in [“White House Issues Executive Order Calling for Inter-Agency Study of Digital Assets,”](#) required a number of federal agencies to issue reports regarding issues raised by digital assets with respect to each agency’s area of jurisdiction. Those agencies have now issued nine reports, covering topics ranging from central bank digital currencies (“CBDC”) to anti-money laundering (“AML”) to the climate and energy implications of creating and using digital assets.

In this *White Paper*, we discuss the high-level takeaways from each report, and what they likely mean for the future development and regulation of digital assets going forward. In two follow-on papers, we will take a closer look at the reports prepared by the White House Office of Science and Technology Policy (“OSTP”), and the U.S. Department of the Treasury.

WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY

The White House OSTP prepared a technical evaluation of developing a U.S. CBDC system ([“Technical Evaluation for a U.S. Central Bank Digital Currency System”](#)). In doing so, the OSTP also set forth the policy objectives of such a system. The report outlines the various choices and limitations that should inform the design and implementation of a “CBDC system” in the United States. Crucially, “CBDC system” includes not only the CBDC itself, but “the public and private sector components built to interact with it, and the laws and regulations that would apply to those components.” The term “components” is to be broadly construed and, by way of example, could encompass things such as smart cards, mobile applications, and intermediaries fulfilling various roles in the system.

The report ([“Policy Objectives for a U.S. Central Bank Digital Currency System”](#)) set forth eight policy objectives, which focus on nuts-and-bolts matters like interoperability with other payment systems as well as higher-level goals such as economic growth, equitable access, national security, and human rights:

1. The CBDC¹ system should include appropriate protections for consumers, investors, and businesses including guardrails against fraud and market failures.
2. The CBDC system should be designed to integrate seamlessly with traditional forms of the U.S. dollar, and be both governable and sufficiently adaptable enough to promote competition and innovation.
3. The CBDC system should provide a good customer experience; make investments and domestic and cross-border fund transfers and payments cheaper, faster, and

- safer; and include appropriate cybersecurity and incident management so as to be protected against cybersecurity attacks and resilient against other potential disasters or failures. The CBDC system itself should be extensible and upgradeable such that it can be iterated upon quickly to improve and harness new innovation, as well as changing technologies, regulations, and needs.
4. The CBDC system should be appropriately interoperable to facilitate transactions with other currencies and systems, such as physical cash, commercial bank deposits, CBDCs issued by other monetary authorities, and the global financial system.
 5. The CBDC system should be available to all and expand equitable access to deposit and payment products and services, as well as credit provided by banks.
 6. The CBDC system should promote compliance with anti-money laundering (“AML”) and combating the financing of terrorism (“CFT”) requirements as well as relevant sanctions obligations.
 7. The CBDC system should be designed and used in accordance with civil and human rights, such as those protected by the U.S. Constitution and outlined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.
 8. The CBDC system should adhere to privacy engineering and risk management best practices, including privacy by design and disassociability.

While some of the objectives may be in tension with each other, the document asserts that its aim is not to prioritize or reconcile any of the concepts, or even take a position on whether a U.S. CBDC should be released at all.

In terms of a technical assessment, the report considers various design options and the ways in which they would further or hinder the realization of the above-stated policy objectives. Those options are broken into six different categories: Participants, Governance, Security, Transactions, Data, and Adjustments. In assessing the options, the report is careful to emphasize that it does not make any assumptions, prioritize any design choices, claim the list of design choices is complete, or take any positions on whether a CBDC system would be in the best interests of the United States.

- **Participants:** This section looks at different options for the transport layer and interoperability. The design of the transport layer within a CBDC system determines the degree to which transactions between two parties are intermediated by a third party, and who that third party is. Interoperability determines the extent to which a CBDC system can execute transactions with other payment systems, domestic or international, digital assets vs. nondigital assets, etc.

- **Governance:** This section looks at permissioning, access tiering, identity privacy, and remediation. “Permissioning” determines whether a system is governed by a set of verified and trusted entities or by a collection of interested participants. Access tiering has to do with the way in which transactions could be parsed and handled differently according to specific attributes. “Identity privacy” relates to who, if anyone, knows the identity of the parties transacting within the CBDC system. And “remediation” has to do with how transaction errors, whether the result of fraud or a simple mistake, are corrected within the system.
- **Security:** This section looks at cryptography and secure hardware. “Cryptography” involves the techniques used to ensure that transactions within the CBDC system are secure. “Secure hardware” considers the extent to which security features within the CBDC system are built into the hardware used to access and operate the system (e.g., smart cards, embedded chips, etc.) vs. managed through software running on general-purpose devices (e.g., computers, tablets, and smartphones).
- **Transactions:** This section looks at signature, transaction privacy, offline transactions, and transaction programmability. “Signatures” concerns how many digital signatures are required to complete a transaction and who must provide them. “Transaction privacy” considers the degree to which transaction details (e.g., account balances, participant location(s), goods sold, etc.) are observable within the system and by whom. “Offline transactions” examines the extent to which parties could effectuate transactions between themselves and then later communicate those transactions to a transaction processor. And “transaction programmability” considers whether third-party developers could develop programs to run within the CBDC system, such as smart contracts.
- **Data:** This section looks at data models and ledger history. “Data models” concerns the way in which ownership records would be stored. “Ledger history” considers whether an ownership and transaction ledger would be stored in a central location or distributed among various locations.
- **Adjustments:** This section looks at fungibility, holding limits, adjustments on transactions, and adjustments on balances. “Fungibility” considers whether a CBDC would have a unique identifier, similar to serial numbers associated with U.S. dollar-denominated bills, or no unique identifier at all. “Holding limits” examines whether to limit entities to holding a set amount of CBDC. And “adjustments on transactions” and “adjustments on balances” looks at whether and how to impose fees on CBDC system users, and whether and how to allow balance adjustments for things like fees and interest, respectively.

A recurring theme in these sections is the sliding scale of privacy vs. AML/CFT compliance, with enhanced privacy making AML/CFT compliance more difficult, and vice versa. The sections also routinely focus on expanding access to

the financial system in an equitable manner, and ensuring interoperability with payments systems that currently exist, and that may come into existence in the future.

The White House OSTP also prepared a report on climate and energy implications associated with digital assets (“[Climate and Energy Implications of Crypto-Assets in the United States](#)”). The report provides answers to several questions specifically set forth in the EO:

How do digital assets affect energy usage, including grid management and reliability, energy efficiency incentives and standards, and sources of energy supply?

The OSTP finds that crypto-asset networks use electricity to power four major functions: (i) data storage; (ii) computing; (iii) cooling; and (iv) data communications—with computing representing the vast majority of electricity use.² It concludes that crypto-assets impact electricity usage and the grid, but that their impact varies depending on the type of crypto-asset. Specifically, the report emphasizes the energy-use differences between proof-of-work (“PoW”) and proof-of-stake (“PoS”) blockchains. The OSTP points to 2021 research showing that each PoS computing device requires 10 to 500 times less power than a typical rig used for PoW Bitcoin mining.³ However, the report finds that total power usage from today’s crypto-asset networks cannot be directly monitored because many computing or mining centers do not disclose their location or report their electricity usage. Another challenge is that energy usage can fluctuate significantly, based on market value fluctuations of the underlying crypto-asset. Despite these challenges, the report estimates the United States’ PoW mining electricity usage to be in the range of 0.9% to 1.7% of total U.S. electricity usage. It also points to such a large range as suggesting a need for miners to report their actual electricity usage to reduce the uncertainties presented to policymakers.⁴

What is the scale of climate, energy, and environmental impacts of digital assets relative to other energy uses, and what innovations and policies are needed in the underlying data to enable robust comparisons?

This section of the OSTP report focuses on the environmental impact of crypto-assets and finds that crypto-asset mining produces GHG emissions and exacerbates climate change primarily by burning coal, natural gas, or other fossil fuels to generate electricity in: (i) an onsite dedicated power plant; (ii) purchasing electricity from the power grid; and/or (iii) producing and disposing of computers and mining infrastructure, and production of power plant fuels and infrastructure.⁵

What are the potential uses of blockchain technology that could support climate monitoring or mitigating technologies?

The OSTP is not optimistic about the value of distributed ledger technology (“DLT”) in certain environmental markets. The report identifies two main types of environmental markets: those created pursuant to a regulatory program and those that are voluntary.⁶ While either market requires the type of robust market infrastructure that DLT is adept at providing—trade execution, payments, clearing and settlement, record-keeping, and security—environmental markets are currently highly centralized.⁷ Given that DLT is designed to solve issues associated with decentralization, the OSTP finds that there may not be a clear advantage to introducing DLT in environmental markets sufficient to justify the switching cost.

Despite its dim view of DLT in environmental markets, the OSTP appears to see potential for DLT in the context of grid reliability and distributed energy resources, or DERs, such as electric vehicles, fuel cells, residential and commercial battery systems, and solar power systems. The OSTP finds that DLT-supported innovation could help to digitize, automate, and decentralize the operation of an electricity grid that estimates say will have more than 100 million new storage devices connected by 2040.⁸ Since such numbers will require greater automation, the OSTP sees smart contracting as a candidate for supporting this aspect of the evolving clean energy marketplace.⁹

What key policy decisions, critical innovations, research and development, and assessment tools are needed to minimize or mitigate the climate, energy, and environmental implications of digital assets?

The OSTP report outlines a number of recommendations to ensure the responsible development of digital assets. These include collaboration among various government entities and the private sector to develop effective performance standards, conduct reliability assessments of crypto-asset mining operations, and analysis of information from crypto-asset miners and electric utilities. They also include promulgating and updating energy conservation standards for crypto-asset mining, encouraging crypto-asset industry associations to publicly report certain information, and promoting and supporting further research and development priorities to improve the environmental sustainability of digital assets.

Overall, the report appears to be aimed at setting the stage for further legislation and regulation that would impact the crypto-asset industry by: (i) informally pressuring the industry to establish certain “best practices” even if such

practices are not initially required; (ii) increasing required reporting; and (iii) setting increasingly stringent performance standards.

DEPARTMENT OF THE TREASURY

The Treasury's report on "[The Future of Money and Payments](#)" includes three main components: (i) a section setting forth Treasury's overview of the current payment system in place today, including recent developments; (ii) a section evaluating options for the U.S. government to pursue in developing a CBDC; and (iii) its four recommendations for improving the U.S. money and payments system.

The overview of the current payments system covers the different retail and wholesale payments systems in use for domestic and cross-border payments; the consumer choices available for consumer-facing payment systems; the roles that banks and non-bank intermediaries play in the current system; and recent developments such as stablecoins, FedNow, and ACH's Real Time Payments network.

The section on a future CBDC is largely reminiscent of the OSTP report on the same topic. It lays out a number of choices to be considered in establishing a CBDC system, such as retail vs. wholesale transactions, whether a CBDC would pay interest, the extent of transaction programmability, the nature of the DLT technology underlying the system, interoperability with foreign CBDCs, and single- vs. two-tier intermediation with the Federal Reserve.

Finally, the report sets forth its recommendations for achieving the policy considerations presented in the EO—namely, building the future of money and payments, supporting U.S. global financial leadership, advancing financial inclusion and equity, and minimizing risks. The recommendations are not detailed, but a few items of note are:

- With respect to a CBDC, Treasury considers potential unintended consequences of a CBDC, including a run to CBDC in times of stress and a reduction in credit availability to the extent that CBDC uptake reduces bank deposits and, indirectly, bank lending.
- On the subject of federal payments regulation, Treasury notes that a federal framework would provide a common floor for existing state standards (such as minimum financial resource requirements) and also that it should address run risk, payments risks, and other operational risks consistently and comprehensively.

The Treasury's report on crypto-assets ("[Crypto-Assets: Implications for Consumers, Investors, and Businesses](#)") includes four main components: (i) a section setting forth Treasury's overview of the current crypto-assets market; (ii) a section providing a description of current uses of

crypto-assets; (iii) a set of risks and exposures for consumers, investors, and businesses in the crypto-asset market, categorized into conduct risks, operational risks, and intermediation risks; and (iv) Treasury's four recommendations to address risks associated with the crypto-asset sector.

The section on the current crypto-assets market describes three categories of relevant entities: crypto-asset platforms, miners and validators, and data aggregators. It also provides four central use cases for crypto-assets: (i) financial markets, products, and services that use native crypto-assets for trading, lending, and collateral activities of other crypto-assets, that are mostly speculative in nature; (ii) use as a medium of exchange for goods and services, in limited cases; (iii) market infrastructure for traditional assets using permissioned blockchains for payments, clearing, and settlement; and (iv) other commercial activities, largely non-fungible tokens ("NFTs").

Treasury views three categories of risks and exposures as the most significant in this space: conduct risks, operational risks, and intermediation risks. Conduct risks include the use of crypto-assets for fraud and scams, information asymmetries between users and platforms, and platforms providing access to bad actors, providing products and services to retail investors without disclosing conflicts or ensuring suitability, and engaging in frontrunning and market manipulation. Operational risks include hacks, difficulty patching bugs in immutable smart contracts, tradeoffs between security and scalability, deanonymization, and misaligned incentives for miners and validators. Intermediation risks include inadequate resources or capabilities for risk mitigation, inability to absorb financial shocks, and bankruptcy/insolvency.

The report asserts that some risk arises from deliberate noncompliance with existing regulation but also from gaps and lack of clarity in the current framework for financial regulation, supervision, and enforcement as it applies to crypto-assets. In that vein, the report makes the following recommendations:

- U.S. regulatory and law enforcement authorities should pursue "vigilant monitoring" of the crypto-asset sector, aggressively pursue investigations, and expand and increase investigations and enforcement, particularly into misrepresentations made to consumers and investors;
- Agencies should review existing regulations and clarify regulatory requirements applicable to crypto-asset products and services, and should act in collaboration with each other while providing guidance in plain language; and
- Agencies should provide education to consumers and investors.

Treasury also issued a report, titled “[Action Plan to Address Illicit Financing Risks of Digital Assets](#)” (“Illicit Financing Strategy”), which outlines priorities and action items to ensure that the U.S. government modernizes the U.S. Department of Treasury’s anti-money-laundering/countering-the-financing-of-terrorism (“AML/CFT”) regime to keep abreast of structural and technological changes to the financial services and markets that result from the increasing issuance and use of digital assets.

Treasury’s Illicit Financing Strategy identifies illicit finance and national security risks and proposes a number of action items to address those risks. However, most of the action items are presented in the Illicit Financing Strategy at a high level of generality, and will have to be fleshed out by Treasury, FinCEN, and others going forward before the industry can or should take concrete action in response.

The identified risks are as follows: money laundering, proliferation financing, terrorist financing, cross-border nature and gaps in AML/CFT regimes across countries, anonymity-enhancing technologies, disintermediation, and virtual asset service provider (“VASP”) registration and compliance obligations. Treasury identifies a number of go-forward action items for combating and mitigating these identified risks, including: monitoring emerging risks; improving global AML/CFT regulation and enforcement; updating Bank Secrecy Act regulations; strengthening U.S. AML/CFT supervision of virtual asset activities; holding cybercriminals and other illicit actors accountable; engaging with the private sector; supporting U.S. leadership in financial and payments technology; and advancing work on a CBDC, in case one is determined to be in the national interest.

DEPARTMENT OF JUSTICE

As with the other reports discussed in this *White Paper*, the report of the Attorney General on “[The Role of Law Enforcement In Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets](#)” was produced in response to the EO. The report gives a brief taxonomy of criminal activity related to digital assets, but—at the direction of the EO—focuses mainly on the role of law enforcement in identifying and investigating crime related to digital assets. The report also adds several potential legislative and regulatory recommendations that could “enhance” DOJ’s efforts to disrupt and prosecute digital asset-related criminal activity. Each section is summarized below.

The report begins by noting that the majority of relevant activity resides in three categories: (i) digital assets as a means of payment for or to facilitate criminal activity; (ii) digital assets as a means of concealing criminal activity; and (iii) crimes involving the digital asset ecosystem. The report also flags an emerging area of concern—the rise

of decentralized finance (“DeFi”). While there is no agreed-upon definition of “DeFi,” in the context of DOJ enforcement, it broadly refers to digital asset protocols and platforms that allow for some form of automated peer-to-peer transactions—usually through the use of smart contracts based on blockchain technology. DOJ is particularly concerned regarding these platforms’ application to fraud, investor and consumer protection, and market integrity. Under the DeFi umbrella, the report also notes that the rise of NFTs presents an opportunity for similar exploitation.

With respect to the role of law enforcement, the report notes recent multi-agency efforts to crack down on the illicit use of digital assets, including classic cases like the Silk Road and DOJ’s Digital Currency Initiative. The report continues by outlining numerous divisions at DHS, Treasury, and the Secret Service charged with varying duties in monitoring and investigating fraud and other criminal activity related to digital assets. After briefly discussing a particular example involving \$10 million in bitcoin, the report concludes with a brief overview of other enforcement mechanisms arising from the SEC, CFTC, CFPB, OCC, FDIC, FTC, and other private-sector partnerships.

Lastly, the report outlines a laundry list of possible regulatory moves that would enhance law enforcement’s ability to crack down on illicit digital asset activity. The report designates each with varying levels of priority. DOJ’s top priority is an extension of the existing prohibition against disclosing subpoenas to VASPs that operate as money-services businesses. In addition, DOJ also recommends strengthening federal law prohibiting the operation of an unlicensed money-transmitting business and extending the statute of limitations for crimes involving digital assets from five to 10 years. Lower priorities include supporting legislation designed to address the challenges in gathering evidence of such crimes and stronger penalties to further deter criminal digital asset activity.

DEPARTMENT OF COMMERCE

In the Department of Commerce’s report on “[Responsible Advancement of U.S. Competitiveness in Digital Assets](#),” Commerce sets forth broader conceptual frameworks, with fewer specific recommendations. And Commerce regularly defers to other departmental reports that are discussed above. Commerce’s framework sets forth four categories of actions: (i) regulatory approaches; (ii) international engagement; (iii) public–private engagement; and (iv) research and development.

Regulatory Approaches

Commerce takes the position that the SEC is already attempting to apply existing financial regulations to digital

assets, and Commerce believes this is critical to future success: “Continued and regular enforcement of applicable financial laws and regulations is a foundational principle of U.S. competitiveness in financial services, including digital assets.” Moreover, “Commerce endorses regulators’ existing approach that both ensures regulation of the financial sector, including through application of existing law, and responsible innovation that identifies and mitigates risks prior to launch.”

International Engagement

Commerce recommends that federal departments and agencies should “continue to engage internationally to promote development of digital asset policies and CBDC technologies consistent with U.S. values and standards.” Commerce also recommends engagement with the Organization for Economic Cooperation and Development, multilateral development banks, and Asia-Pacific Economic Cooperation.

Public–Private Engagement

Commerce recommends a number of key issues that warrant public–private engagement: (i) an advisory committee; (ii) consumer and investor protection and education; (iii) diversity, equity, and inclusion; (iv) workforce development; (v) payment system modernization; (vi) sustainability; and (vii) accurate and complete economic statistics on economic activity.

Research and Development

Commerce notes the role of federal agencies in foundational research, and recommends continued promotion of research and development in financial technologies and digital assets to continue U.S. technological leadership.

FINANCIAL STABILITY OVERSIGHT COUNCIL

The Financial Stability Oversight Council’s (“FSOC”) “[Report on Digital Assets Financial Stability Risks and Regulation](#)” assesses the extent to which digital assets might pose systemic risks to the financial system.

The report begins by defining the scope of digital assets—which it defines as CBDCs and crypto-assets. The report focuses primarily on the latter, which it defines as private-sector digital assets that depend primarily on cryptography and distributed ledger or similar technology. Two primary examples, therefore, would be Bitcoin and Ethereum. The report also discusses key technological developments and financial innovations and market developments in this

space, including the market capitalization peak of \$3 trillion in November 2021 to its current level of around \$900 billion.

The report next discusses potential financial stability risks. Those risks are, for the moment, tempered by the lack of significant interconnections between the crypto-asset ecosystem and the traditional financial system. Those interconnections could, however, rapidly grow as the crypto-asset ecosystem continues to evolve. Thus, the report assesses the vulnerabilities within that ecosystem, such as drops in asset prices, financial exposures via interconnections within the ecosystem, operational vulnerabilities, funding mismatches, the risk of runs on assets, and the use of leverage. The report also notes that, interconnections aside, crypto-assets could pose financial stability risks if they were to attain a large enough scale.

The report also discusses regulation of crypto-assets in the context of the above-identified risks. The report observes that the “current regulatory framework, along with the limited overall scale of crypto-asset activities, has helped largely insulate traditional financial institutions from financial stability risks associated with crypto-assets,” before going on to discuss various regulators and regulations, and their (potential) applicability to crypto-assets.

The report’s more interesting aspects reside in the FSOC’s recommendations. There, the report begins by noting that “large parts of the crypto-asset ecosystem are covered by the existing regulatory structure.” That may come as a bit of a surprise, given the ongoing legal battles concerning whether certain crypto-assets are securities, commodities, or something else altogether. It is, however, consistent with recent regulatory enforcement actions in this space, where both the SEC and the CFTC have been increasingly aggressive in asserting their authority over crypto-asset ecosystem participants. The report then notes the “gaps” in the regulation of crypto-asset activities that would benefit from additional attention:

- Limited direct federal oversight of the spot market for crypto-assets that are not securities;
- Opportunities for regulatory arbitrage; and
- Whether vertically integrated market structures can or should be accommodated under existing law and regulations.

The first gap primarily concerns, in the report’s eyes, spot markets for bitcoin “and possibly other crypto-assets that are not securities.” By the report’s own assessment, this market is rather limited. But the report urges additional regulation to “ensure orderly and transparent trading, to prevent conflicts of interest and market manipulation, and to protect investors and the economy more broadly.”

The second gap, relating to regulatory arbitrage, characterizes optionality in the existing U.S. regulatory framework as a design defect rather than an intentional feature to permit innovation. FSOC states that opportunities for regulatory arbitrage can occur “when the same activity can be carried out lawfully under more than one regulatory framework.” This fact is, of course, a hitherto noncontroversial hallmark of the U.S. banking system, in which banks may choose to be chartered under state or federal law and from a variety of different banking charters, for example. But the FSOC views this flexibility as creating opportunities for crypto-asset providers to “provide financial services that resemble services provided by banks, traditional securities intermediaries, or other financial institutions, but without being subject to, or in compliance with, the same standards and obligations.”

The report therefore urges regulators to coordinate with one another in their supervision of crypto-asset entities, especially when “different entities with similar activities may be subject to different regulatory regimes or when no one regulator has visibility across all affiliates, subsidiaries, and service providers of an entity.” In a similar vein, the report recommends that the FDIC, FRB, OCC, and state bank regulators use their existing authority to review services provided to banks by crypto-asset service providers. The report also recommends that Congress pass legislation that would create: (i) a comprehensive prudential framework for stablecoin issuers; and (ii) a supervisory framework where regulators have visibility into the activities of all the affiliates and subsidiaries of crypto-asset entities.

The third gap, relating to vertically integrated market structures, largely concerns recent requests by some market participants to disintermediate certain aspects of the market for crypto-assets. Specifically, these participants seek to provide direct retail access to investors. The report’s primary concerns stem from consumer protection and managing the risk associated with the leverage or credit offered to retail investors. The report draws particular attention to the practice of managing risk by marking positions to market on a very frequent basis and conducting automatic liquidations where margin calls go unmet. While this may be an effective risk management tool, exposing retail investors to rapid liquidations raises its own set of concerns around disclosures, education, and potential conflicts of interest.

The report is, in some ways, more notable for what it does not say or do. It does not, for instance, provide any additional clarity on whether crypto-assets are securities, commodities, or something else. It also does not call for dramatic regulatory changes. Rather, it essentially calls on the member agencies to keep doing what they are doing. That posture would seem to benefit entities already within the regulatory perimeter, which can explore crypto-asset services and products within a risk management and

control framework with which regulators are more comfortable and, in so doing, shape regulatory views on these activities to their advantage. In contrast, firms outside of or unable to gain access to the regulatory perimeter, including would-be “disruptors” to incumbent providers, are more likely to find themselves in an adversarial relationship with regulators.

ENDNOTES

- 1 News reports indicate that the Department of Justice issued a legal opinion on the Federal Reserve’s authority regarding a CBDC, but those legal views have not yet been shared with Congress (or the public).
- 2 White House Office of Science and Technology Policy, *Climate and Energy Implications of Crypto-Assets in the United States* 13 (Sept. 8, 2022).
- 3 *Id.*
- 4 *Id.* at 15.
- 5 *Id.* at 21.
- 6 *Id.* at 27.
- 7 *Id.* at 28.
- 8 *Id.* at 29.
- 9 *Id.*



DIGITAL ASSETS DEFINED: WRITING DIGITAL ASSETS INTO THE BANKRUPTCY CODE

NOVEMBER 2022 COMMENTARY

As discussed in previous installments of this White Paper series, the Lummis-Gillibrand Responsible Financial Innovation Act (the “Bill”)¹ proposes a comprehensive statutory and regulatory framework in an effort to bring stability to the digital asset market. One area of proposed change relates to how digital assets and digital asset exchanges would be treated in bankruptcy. If enacted, the Bill would significantly alter the status quo from a bankruptcy perspective.

OVERVIEW OF DIGITAL ASSETS IN BANKRUPTCY

There is little reported jurisprudence in the United States specifically relating to insolvency proceedings involving digital assets (e.g., cryptocurrencies). In fact, how these assets are treated in bankruptcy in certain aspects is currently developing, as several significant players in the cryptocurrency arena have commenced bankruptcy and insolvency proceedings in the United States and abroad (e.g., Voyager Digital Holdings, Celsius Network, Three Arrows Capital). The only other analogue was in 2014, when the high-profile cryptocurrency exchange, Mt. Gox, commenced a bankruptcy proceeding in Japan after halting bitcoin trading due to major security breaches and bitcoin theft. After years of legal proceedings, the Japanese trustee announced in October 2021 that a civil rehabilitation plan was accepted by a majority of creditors, yet it remains uncertain when distributions to creditors will occur and the effect market volatility will have on such distributions.²

In light of the lack of U.S. precedent and overall volatility in the cryptocurrency market, if passed, the Bill could provide much-needed certainty relating to the treatment of digital assets in a U.S. bankruptcy proceeding. To do so, the Bill largely proposes to integrate digital assets into existing statutory and regulatory frameworks relating to the treatment of commodities and the relief available to commodity brokers in bankruptcy.

The primary objective of the existing provisions of the Bankruptcy Code³ relating to commodities is to minimize the ripple effect and disruption that the bankruptcy of a major commodities player could have on the markets. The statutory framework relating to the liquidation of a commodity broker has been tested very little.⁴ Moreover, the U.S. Commodity Futures Trading Commission (“CFTC”) has enacted a complicated web of rules—the Part 190 Rules⁵—which apply in conjunction with, and sometimes supersede, the Bankruptcy Code in a commodity broker liquidation.

The Bill proposes to amend, among other things, the definition of “commodity broker” to include “digital asset exchange,” which the Bill in turn defines as “a centralized or decentralized platform which facilitates the transfer of digital assets”⁶ and “a trading facility that lists for trading at least one digital asset.”⁷ This, among other proposed changes, would enact significant changes to both the relief available to a digital asset exchange should it file for bankruptcy and the treatment and protections offered to customers and non-debtor parties to digital asset contracts in a bankruptcy proceeding. For example, should a digital asset exchange seek bankruptcy relief, the Bill proposes to require such exchange to liquidate under the chapter 7 bankruptcy scheme relating to commodity brokers (the “Commodity Broker Liquidation Subchapter”).⁸ Conversely, in instances where a digital asset exchange is not the

bankrupt entity but is party to a digital asset contract with a debtor, section 556 of the Bankruptcy Code would generally protect the digital asset exchange from certain key provisions of the Bankruptcy Code, which, if permitted to apply, could potentially cause a domino effect in the markets.⁹

BANKRUPTCY RELIEF AVAILABLE TO DIGITAL ASSET EXCHANGES

As proposed by the Bill, the only bankruptcy relief available to a digital asset exchange would be chapter 7 liquidation under the Commodity Broker Liquidation Subchapter. A digital asset exchange would not qualify for chapter 11 relief.¹⁰ By limiting bankruptcy relief to the Commodity Broker Liquidation Subchapter, the Bill would, among other things, put digital asset exchanges into an established framework that specifically governs the treatment of customer property vs. non-customer property, customer rights, and the portability of customer positions in digital assets.

As noted previously, the overall purpose of the Commodity Broker Liquidation Subchapter is to minimize the ripple effect and disruption that the insolvency of a commodity broker could have on the markets. This is accomplished by a host of mechanisms, many of which equip customers with strong protections and powers that non-debtor parties ordinarily do not have in traditional chapter 7 or chapter 11 bankruptcies. The Commodity Broker Liquidation Subchapter provides a skeletal framework by which commodity brokers (as defined by the Bankruptcy Code)¹¹ are liquidated, which would include the appointment of a bankruptcy trustee. The Bankruptcy Code provisions are supplemented by and, at times, superseded by the Commodity Exchange Act¹² and the Part 190 Rules, which contain the bulk of regulations defining the trustee's powers and responsibilities in a commodity broker liquidation.

One hallmark function of the Commodity Broker Liquidation Subchapter and the Part 190 Rules is to protect “customer property” (typically funds held by the debtor on account of a commodities customer¹³). The Bill proposes, among other things, to include “digital asset” in the definition of “customer property.”¹⁴ In a commodity broker liquidation, customer funds must be segregated and treated as property of the customer, not property of the bankrupt commodity broker. The Commodity Broker Liquidation Subchapter and the Part 190 Rules also give customers the highest priority claims over customer property, subject to payment of certain expenses for administering the bankruptcy case. Another significant customer protection is that a bankrupt commodity broker must undergo best efforts to promptly transfer all customer accounts to another non-bankrupt commodity broker.¹⁵ In contrast, the restructuring regime under chapter 11 of the Bankruptcy Code does not specifically enumerate these customer protections, which would

likely result in the parties constantly litigating to determine or seek to enforce such rights.¹⁶ Accordingly, the conglomerate of statutes and rules governing a commodity broker liquidation seeks to provide more certainty, reduce litigation, and minimize the “domino” effect on the markets that could ensue by a commodity broker bankruptcy.¹⁷

Another aspect of the Bankruptcy Code designed to preserve the market is that sections 546(e) and 764(b) of the Bankruptcy Code effectively insulate from avoidance all payments made pre-bankruptcy or within seven days after the bankruptcy filing from a commodity broker to its customers.¹⁸ These provisions also facilitate the trustee's directive to make best efforts to transfer all customer accounts to another commodity broker as soon as possible after the bankruptcy filing.

The Commodity Broker Liquidation Subchapter and the Part 190 Rules also require the trustee to provide notice to customers of the bankruptcy filing requesting that the customer instruct the trustee as to the disposition of such customer's specifically identifiable property and file a proof of claim.¹⁹ The trustee must comply with, to the extent practicable, the customer's instructions relating to the disposition of customer property. The primary objective of these provisions is to facilitate a prompt transfer of all customer accounts to another commodity broker, ensure that customers receive their pro rata share of customer property, and mitigate the ripple effect a commodity broker bankruptcy could have on the market.

SECTION 556 COMMODITY BROKER AND COMMODITY CONTRACT PROTECTIONS

The Bill also proposes to provide a digital asset exchange with certain protections in instances where such exchange is not the bankrupt entity but is party to a digital asset contract with a debtor. Specifically, the Bill seeks to expand section 556 of the Bankruptcy Code to enable a digital asset exchange to exercise its contract rights notwithstanding certain provisions of the Bankruptcy Code.²⁰

First, upon a bankruptcy filing, the “automatic stay” immediately halts all litigation and actions against the debtor or its property, including a non-debtor's efforts to enforce its contract rights against the debtor.²¹ Section 556 permits non-defaulting “protected parties”—e.g., commodity brokers—to commodity contracts with a debtor to exercise their contractual rights notwithstanding the automatic stay. These rights can include, for example, the right to liquidate, terminate, cancel, or set off mutual debts and claims relating to commodity contracts. Were this not so, a commodity contract could be in a state of limbo for the entire pendency of the bankruptcy—possibly years—which could wreak havoc on the markets.

Second, in ordinary bankruptcy circumstances, section 365 of the Bankruptcy Code empowers a debtor to assume or reject executory contracts (i.e., contracts where both counterparties have material unperformed obligations).²² In a chapter 11 reorganization case, the debtor may assume or reject an executory contract at any time before confirmation of a plan, possibly years after commencement of the case.²³ In the context of commodities and derivatives contracts, the debtor would be, at minimum, incentivized to delay assuming or rejecting the contract until after the date on which the debtor was required to perform to see if the market price of the commodity fluctuated to the debtor's benefit. To mitigate this problem, section 556 allows a protected party at any time to exercise its contractual rights.

Third, a debtor is equipped with certain powers to claw back fraudulent or preferential pre-bankruptcy transfers or transactions.²⁴ Section 556 operates in conjunction with section 546(e) of the Bankruptcy Code to exempt from clawback a transfer “made by or to (or for the benefit of) a [protected party]” that is “in connection with a ... commodity contract.”²⁵ These protections limit the trustee's ability to avoid a host of transfers that are germane to the commodity and derivatives markets—in particular, for example, maintenance margin and mark-to-market payments.²⁶ Section 546(e) does not, however, disarm the debtor's powers to avoid transfers made with the actual intent to hinder, delay, or defraud creditors.

CONCLUSION AND OUTLOOK

While it is unlikely the Bill will pass in its current form, it proposes a framework that could establish much-needed certainty regarding how digital assets are treated in bankruptcy. The pending bankruptcy and insolvency cases involving digital assets may highlight additional issues unique to the treatment of digital assets in bankruptcy and prompt Congress to propose further changes to the Bankruptcy Code. At present, while subject to some debate, a digital asset exchange could seek to reorganize or liquidate under chapter 11 of the Bankruptcy Code, which means far less certainty for customers than if the digital asset exchange were subject to the Commodity Broker Liquidation Subchapter and Part 190 Rules.

ENDNOTES

- 1 Lummis-Gillibrand Responsible Financial Innovation Act, S. 4356, 117th Cong., § 101(a) (2022) (proposed 31 U.S.C. § 9801(2)).
- 2 “Mt. Gox Creditors to Get Billions in Bitcoin After Plan Approved,” Bloomberg.com, October 20, 2021.
- 3 11 U.S.C. §§ 101 *et seq.*
- 4 See, e.g., *In re Peregrine Financial Group, Inc.*, Case No. 12-27488 (Bankr. N.D. Ill. July 10, 2012).
- 5 17 C.F.R. § 190.00 *et seq.*
- 6 S. 4356, § 203(a) (proposed 26 U.S.C. § 864(b)(C)).
- 7 *Id.* § 401 (amending 7 U.S.C. § 1a).
- 8 11 U.S.C. §§ 761-767.
- 9 *Id.* § 556.
- 10 See *id.* § 109(d) (providing that “[o]nly ... a person that may be a debtor under chapter 7 of this title (except a stockbroker or a commodity broker) ... may be a debtor under chapter 11 of this title.”); §§ 761-767 (liquidation regime for commodity brokers).
- 11 *Id.* § 101(6).
- 12 7 U.S.C. § 1 *et seq.*
- 13 11 U.S.C. § 761(10) (defining “customer property” as “cash, a security, or other property, or proceeds of such cash, security, or property, received, acquired, or held by or for the account of the debtor, from or for the account of a customer...”). Not all cash, securities, or property subject to a commodity contract fall within the “customer property” protections.
- 14 S. 4356, § 407(e)(2) (amending 11 U.S.C. § 761(10)).
- 15 See 11 U.S.C. § 766(c).
- 16 While the Commodity Broker Liquidation Subchapter definitively establishes customer protections, whether a party or property is entitled to such protections could be subject to litigation.
- 17 Commodity Fut. Trad. Comm'n, Bankruptcy—Proposed Rules, 46 Fed. Reg. 57,535 *et seq.* (Nov. 24, 1981).
- 18 11 U.S.C. §§ 546(e); 764(b). Specifically, section 764(b) and the Part 190 Rules protect, in most instances, any transfer or liquidation of a commodity contract from avoidance if such transfer or liquidation is approved by the CFTC by rule or order.
- 19 *Id.* § 765.
- 20 S. 4356, § 407(c) (amending 11 U.S.C. § 556).
- 21 11 U.S.C. § 362(a).
- 22 *Id.* § 365.
- 23 See *id.* § 365(d)(2).
- 24 See *id.* §§ 544, 547, and 548.
- 25 *Id.* § 546(e).
- 26 Courts hold that the safe harbor provisions of section 546(e) do not automatically bar avoidance claims, but are an affirmative defense that is waived if not timely raised. See, e.g., *Tronox Inc. v. Kerr McGee Corp. (In re Tronox Inc.)*, 503 B.R. 239, 338–40 (Bankr. S.D.N.Y. 2013).



JANUARY 2023 COMMENTARY

IN SHORT

The Situation: Since clarifying the legal permissibility of certain crypto activities in 2020 and early 2021, the Federal banking agencies have begun to tighten regulatory scrutiny of such activities, warning banks regarding applicable risks, imposing procedural checks on their commencement, and emphasizing the importance of engaging in those activities in a safe and sound manner.

The Result: On January 3, 2023, the Federal Reserve, Federal Deposit Insurance Corporation (“FDIC”), and Office of the Comptroller of the Currency (“OCC”) issued a joint statement expressing their skepticism that certain crypto-asset-related activities can be conducted in a safe and sound manner at the current time. They further noted the importance of preventing risks related to the crypto-asset sector from migrating to the banking system.

Looking Ahead: Although the crypto-asset-related activities addressed by earlier OCC interpretive letters may still be legally permissible for banks, the agencies’ view that certain of these activities are “highly likely to be inconsistent with safe and sound banking practices” nonetheless narrows the path forward for banks seeking to engage in them. It is unclear whether the agencies will issue further guidance or direction to banks engaged or considering engaging in such activities.

In recent years, certain banks have expressed interest in or have engaged in crypto-asset-related activities or have provided banking services to crypto-asset firms. Some crypto-asset firms have sought or received banking charters. The OCC issued a number of interpretive letters in 2020 and early 2021, acknowledging that it is legally permissible for national banks to provide cryptocurrency custody services, hold stablecoin reserves, participate as nodes in distributed ledgers, and use stablecoins. The OCC also approved

the conversion or conditional chartering of several banks engaged in crypto-asset-related activities.

Since then, however, the OCC and other banking agencies have adopted a more conservative approach. In a subsequent interpretive letter, for instance, the OCC emphasized the fact that any banking activities, including crypto-asset-related activities, must be conducted in a safe and sound

manner, and directed banks to seek supervisory “non-objection” before engaging in any crypto-asset-related activities. Over the course of 2022, the Federal Reserve and FDIC followed suit, issuing guidance documents that likewise directed banks to seek prior notice before engaging in these activities and noting that regulators would provide “relevant supervisory feedback.”

The [Joint Statement on Crypto-Asset Risks to Banking Organizations](#) (“Statement”) is the agencies’ most explicit and clear articulation of their policy approach to crypto-asset-related activities. Consistent with past guidance and in response to market developments in 2022, the agencies identify a number of risks associated with these activities in the Statement, including fraud, run risk, and immature risk management and governance practices. Accordingly, the agencies note the importance of preventing risks related to the crypto-asset sector that cannot be mitigated or controlled from migrating to the banking system.

The Statement goes beyond past guidance in expressing the agencies’ current views on safety and soundness:

Based on the agencies’ current understanding and experience to date, the agencies believe that issuing or holding as principal crypto-assets that are issued, stored, or transferred on an open, public, and/or decentralized network, or similar system is highly likely to be inconsistent with safe and sound banking practices.

This conclusion could be read to apply to some activities previously identified as legally permissible by the OCC as well as other crypto activities upon which the OCC (or other banking agencies) have yet to opine publicly. The agencies also state that they have “significant safety and soundness concerns with business models that are concentrated in crypto-asset-related activities or have concentrated exposures to the crypto-asset sector.” Notwithstanding the disclaimer about banks being neither prohibited nor discouraged from providing banking services to customers of any specific class or type, the Statement raises doubt as to whether there is a viable path forward for banks to engage in crypto-asset-related activities or serve crypto-related firms in anything other than a limited fashion.

These blanket safety and soundness pronouncements create a high bar for banks seeking to engage in these activities. They raise, rather than answer, a number of questions: (1) What does “safety and soundness” mean in the context of crypto activities, including traditional banking activities like custody, payments, and deposits? (2) Who is responsible for defining it—the bank, its regulators, or both? (3) Are banks currently engaged in crypto activities acting in an unsafe or unsound fashion? (4) What about banks providing traditional banking services to crypto firms? Given the confidential nature of the supervisory process, and the lack of detail and clarity in the joint statement, the public can only guess, and banks are likely to be discouraged from pursuing crypto activities.

Two Key Takeaways

1. The Federal Reserve, FDIC, and OCC have stated that issuing or holding crypto-assets is “highly likely to be inconsistent with safe and sound banking practices,” and they have “significant safety and soundness concerns with business models that are concentrated in crypto-asset-related activities or have concentrated exposures to the crypto-asset sector.”
2. Banks should be cautious in whether and how they proceed with crypto activities or serve crypto firms, and be prepared for supervisory criticism.



CFTC PARTNERS WITH SEC AND DOJ TO BRING COORDINATED DEFI ENFORCEMENT ACTION TARGETING ORACLE MANIPULATION

JANUARY 2023 COMMENTARY

IN SHORT

The Situation: Decentralized finance (“DeFi”) is a rapidly growing sector that, by definition, eschews centralized financial institutions altogether. Misconduct that has accompanied that growth has drawn the attention of the Commodity Futures Trading Commission (“CFTC”), which has brought three DeFi cases in the last 12 months.

The Result: The latest subject of this scrutiny allegedly artificially affected prices through “oracle manipulation” on three digital asset exchanges to benefit his “perpetual futures” contract positions on a DeFi market. In response, the CFTC recently brought a civil enforcement action, its first for a fraudulent or manipulative DeFi scheme, charging an individual with wash trading and with unlawfully obtaining more than \$110 million in digital assets through this manipulative scheme.

Looking Ahead: The CFTC, U.S. Securities and Exchange Commission (“SEC”), U.S. Department of Justice (“DOJ”), and other federal agencies will continue to bring cases involving issues of first impression to apply their jurisdiction in new markets, including DeFi markets, in response to new methods of perceived violations of the statutes they administer.

On January 9, 2023, the CFTC initiated a civil enforcement action against the defendant, who came under scrutiny in October 2022 when he allegedly employed a manipulative strategy across three digital asset exchanges, and Mango Markets, a DeFi protocol, that yielded over \$110 million in digital assets. The DOJ and SEC also brought parallel charges. In its complaint, the CFTC alleges that on October 11, 2022, the defendant misappropriated more than \$110 million in digital assets from Mango Markets through oracle manipulation. An oracle is a data feed that moves data on and off a blockchain. Oracle manipulation

can consist of artificially influencing the data feed to the oracle and/or into the blockchain—in this case, the Mango Markets blockchain. This is the type of oracle manipulation the CFTC alleged in its complaint.

The defendant allegedly executed his improper scheme by creating two anonymous accounts on Mango Markets, which he used to establish long and short perpetual futures contracts in the different accounts based upon the relative prices of MNGO, the native Mango Markets token; and USDC, a stablecoin. According to the complaint, the defendant then began purchasing substantial quantities of MNGO

on three digital asset exchanges that were the inputs for the Mango Markets oracle. The complaint alleges that these high quantity, large-scale transactions severely inflated the price of MNGO on those exchanges, in turn significantly increasing the value of the defendant's long perpetual futures position on Mango Markets. He then purportedly cashed out his position by taking a loan he did not intend to repay, which was collateralized by the value of the long position, effectively completely draining Mango Markets's liquidity, and requiring it to suspend operations. Although the value of the defendant's short position decreased dramatically, the defendant needed to establish the short position so that he would have a counterparty for his long position in his other account, according to the complaint. The CFTC charged the defendant with wash trading for executing this offsetting trade.

The complaint states that the defendant then contacted the Mango Decentralized Autonomous Organization ("DAO")—the Mango Markets blockchain operator—to negotiate his return of some of the digital assets that he had "borrowed," conditioned on Mango Markets agreeing, among other things, to not pursue any criminal investigations or freeze the defendant's funds. The defendant agreed to return approximately \$67 million in digital assets but retained about \$47 million, according to the complaint.

This case represents the first CFTC enforcement action involving DeFi manipulation and fraud and the third CFTC DeFi action overall in a relatively short span of time, since January 2022. The first two were [actions against Polymarket](#) in January 2022 and [Ooki DAO](#) in September 2022. This trend suggests that the CFTC is attuned to DeFi developments and focused on this space. Two CFTC commissioners released statements concurrent with the announcement of the complaint suggesting that the CFTC is just getting started. For instance, Commissioner Kristen Johnson noted that she supports the CFTC using its "existing authority to vigorously pursue misconduct ... in novel venues like a decentralized digital asset exchange." Commissioner Caroline Pham noted that this enforcement action makes clear that perpetual futures can constitute a swap, which brings such a scheme within the CFTC's jurisdiction.

As to perpetual futures, it is interesting that, although the product is called a perpetual "futures," a product over which the CFTC also has jurisdiction, the CFTC characterized it as a swap. This may be because the CFTC has lost several cases (e.g., *CFTC v. Zelener*, 373 F.3d 861 (7th Cir. 2004); *CFTC v. Erskine*, 512 F.3d 309 (6th Cir. 2008)) in which it sought to characterize products as futures; and the definition of "swap" in the Commodity Exchange Act ("CEA"), the statute the CFTC administers, is quite broad and possibly easier to apply to particular new products. The CFTC has also stated in the past that the name given to a product does not dictate its legal treatment.

The case is also a notable example of cooperation and coordination among the CFTC, DOJ, and SEC in the DeFi enforcement space. In that regard, the CFTC's Division of Enforcement has an [Office of Cooperative Enforcement](#), which "provides expert help and technical assistance with case development and trials to U.S. Attorneys' Offices, other federal and state ... agencies, and international authorities." [The CFTC's Mango Markets enforcement press release](#) makes clear that it is working closely with the DOJ and the SEC ([which charged the defendant](#) with manipulating MNGO, "a so-called governance token that was offered and sold as a security"), to crack down on various fraudulent schemes involving digital assets. Relatedly, [DOJ's criminal complaint against the defendant](#) was unsealed on December 27, 2022.

Two Key Takeaways

1. The CFTC and other federal agencies are focused on DeFi misconduct.
2. Though DeFi is new, the statutes cited in enforcement actions administered by the CFTC, DOJ, and SEC (including the CEA, securities laws, or wire fraud) are not new. Therefore, DeFi innovators wishing to avoid a federal enforcement action would be well advised to become familiar with the applicable federal regulatory scheme.



FED POLICY STATEMENT ADDS HURDLES TO DIGITAL ASSET ACTIVITIES AND INNOVATION BY STATE BANKS

FEBRUARY 2023 COMMENTARY

The Situation: The Federal Reserve Board (“Board”) has issued a new [policy statement](#) (“Policy Statement”) imposing limits, including Board approval requirements, on digital asset activities and other novel activities of state-chartered member banks.

The Result: The Policy Statement generally defers to the Office of the Comptroller of the Currency (“OCC”), applying substantive requirements and, in some cases, processes, such as “supervisory nonobjection,” of the OCC to applications by state banks that are members of the Federal Reserve System (“Fed”). The Policy Statement applies broadly, but its preamble suggests that the Board’s initial focus is on digital asset activities.

Looking Ahead: Although the immediate impact of the Policy Statement will likely be on digital asset activities, the terms of the Policy Statement apply to “novel and unprecedented activities” generally. And while the Policy Statement appears at first blush to reflect Board deference to the OCC (and FDIC as appropriate), its effects are more likely to constitute a check on the ability of state banking authorities to permit state banks to develop innovative methods and new technologies to conduct the business of banking.

At its best, the dual banking system in the United States allows the states to act as Justice Brandeis’s “laboratories of democracy.” Frequently during the banking industry’s history, innovation has taken place at the state level. And what is innovative today may well become standard or even banal tomorrow: For example, it was state banks that first introduced the checking account to U.S. consumers.

The publication of the Policy Statement appears to have been driven by the Board’s concerns regarding the risks of cryptocurrency to the stability of the banking system (or perhaps even to the stability of individual banks with

significant exposure to cryptocurrencies), and it may well succeed in reducing those risks. But its effects will also include limiting the flexibility of state banking authorities and the banks they charter (at least those that are Fed member banks) to innovate over time, using methods and technologies that have nothing to do with cryptocurrency.

On its face, the Policy Statement announces that, under Section 9(13) of the Federal Reserve Act, the Board is adopting a rebuttable presumption that state member banks may engage as principal only in activities permissible for national banks unless explicitly authorized to do

so by federal statute or FDIC regulation—and may only do so subject to any attendant conditions imposed by the applicable federal regulator. Otherwise, the Board will treat requests to engage in such a “novel and unprecedented” activity as a change in the general character of the business of the bank such that the state member bank must obtain Board permission under Regulation H, under a rebuttable presumption that the activity is impermissible.

In the preamble, the Board provided two examples of how the rebuttable presumption process would impact digital assets: (i) under the Policy Statement’s framework, there is no legal basis for holding digital assets as principal; and (ii) state member banks may not issue “dollar tokens” (a new term roughly analogous but not identical to stablecoins) except as permitted by existing OCC interpretive letters. Therefore, a state member bank would have to obtain “supervisory nonobjection” from Fed staff before issuing a stablecoin: a hurdle unlikely to be surmounted under the Policy Statement and other recent guidance.

The Board published the Policy Statement on the same day that the Fed denied Custodia Bank’s application for membership and a master account. Custodia, a Wyoming special purpose depository institution (“SPDI”), had applied for Fed membership nearly two years ago. Custodia sued the Board and the Federal Reserve Bank of Kansas City, its regional Federal Reserve Bank, in an attempt to force the Fed to act on its application. In denying the application, and consistent with the Policy Statement, the Fed cited safety and soundness risks associated with Custodia’s proposed digital asset activities. It also reasoned that Custodia did not have a sufficient risk management framework to mitigate such “safety and soundness risks” that generally accompany digital asset activities.

Although some stakeholders may welcome the Policy Statement’s transparency, it is a notably broad assertion of federal authority over creations of state law and a potentially high cost to pay for the privilege of Fed membership. In taking significant steps to reduce risks that appear largely to be limited to a handful of financial institutions, the Policy Statement raises a host of questions ranging from the merely technical to the overarching dynamics of the dual banking system:

- Will the Board expect state member banks to comply with nonpublic terms, conditions, and limitations imposed on national banks?
- Will the Board distinguish between: (i) nonbinding terms, conditions, and limitations set forth in guidance documents such as interpretive letters; and (ii) enforceable conditions “imposed in writing” within the meaning of 12 USC 1818?
- What role will regional Federal Reserve Banks and state banking authorities play in the Board’s process under

the Policy Statement, including in rebutting the Board’s presumption?

- Will the FDIC respond in kind, to harmonize powers between state member banks and state non-member banks?

Two Key Takeaways

1. The Policy Statement gives the Board greater leverage over state member banks seeking to engage in any “novel and unprecedented activities.”
2. State member banks should expect significant scrutiny when attempting to proceed with “novel and unprecedented activities,” including digital asset activities, and should expect to face heightened skepticism from the Fed generally, and more involvement from the Board specifically.



“METABIRKINS” BAGGED: NFT CREATOR FOUND LIABLE FOR TRADEMARK INFRINGEMENT

FEBRUARY 2023 COMMENTARY

In a closely watched trademark infringement case involving non-fungible tokens (“NFTs”), a jury found that the sale of digital images of Hermès’s Birkin bags as NFTs infringed and diluted Hermès’s trademarks.

Rejecting arguments that NFTs depicting Birkin handbags with colorful fur are entitled to First Amendment protection, on February 8, 2023, a jury in the Southern District of New York found artist Mason Rothschild liable for infringing and diluting the trademarks of Hermès International (“Hermès”). The jury also found that Rothschild’s registration of the MetaBirkins.com domain name constituted cybersquatting.

This case was the first to try the issue of whether copying a real-world brand as an NFT could qualify as protected artistic expression. Hermès claimed that Rothschild’s “MetaBirkin” NFTs caused consumer confusion and disrupted its efforts to enter the NFT space. In contrast, Rothschild argued that sales of his fur-covered blurry images of “Metabirkin” NFTs were a form of protected expression as a reference to the fashion industry’s antifur movement and as a comment on the Birkin bag’s influence on modern society. As such, Rothschild argued that he was immune from liability under the First Amendment, teeing up the issue of whether NFTs were the type of artistic expression that could be covered by the *Rogers v. Grimaldi* test.

At summary judgment, Judge Rakoff determined that “MetaBirkin” NFTs could constitute a form of artistic expression and held that the *Rogers v. Grimaldi* test applied to Hermès’s claims. Under *Rogers*, trademark use as part of an expressive work is protected by the First Amendment

if the use is both (i) artistically relevant and (ii) otherwise not explicitly misleading. In addition to the *Rogers* defense, Rothschild asserted that confusion was not likely because the “MetaBirkin” images are not merely reproductions of Birkin bags (but rather are fanciful depictions), are not actual handbags, and given the market prices of the parties’ products, consumers would carefully check the entire description of the “MetaBirkin” NFTs before purchase.

The holding in *Rogers* notwithstanding, following a five-day trial, the jury found that the NFTs were not art protected by the First Amendment, finding in favor of Hermès on all of its claims and awarding Hermès \$110,000 for Rothschild’s net profits and \$23,000 in statutory damages for cybersquatting.

The decision is the first to analyze infringement of a real-world brand in a virtual context and should be considered by both trademark owners and NFT creators in considering the limits of First Amendment protection in connection with the creation and sale of NFTs. The case is *Hermes International et al. v. Rothschild*, Case No. 1:22-cv-00384 (S.D.N.Y.).



HARD FORKS AND AIRDROPS: THE IRS ISSUES CRYPTOCURRENCY TAX GUIDANCE

JANUARY 2020

The IRS's first guidance on the taxation of cryptocurrency in five years provides some new insights, but also leaves several issues unresolved. Jones Day partner Lori Hellkamp discusses Revenue Ruling 2019-24, with particular attention to the tax treatment of "hard forks" and "airdrops," tips for remaining compliant, and the remaining questions relating to the taxation of virtual currencies.



[TO LISTEN TO THE PODCAST](#)

CHAPTER V

**REGULATORY
ISSUES
(U.S.-STATE LEVEL)**



CALIFORNIA MOVES TO REGULATE DIGITAL ASSET EXCHANGES AND CRYPTOCURRENCY COMPANIES

SEPTEMBER 2022 ALERT

On August 30, 2022, the California State Legislature passed (and Governor Newsom is expected to sign into law) a “Digital Financial Assets Law,” which will impose licensing requirements on digital asset companies and cryptocurrency exchanges beginning January 1, 2025.

California’s new Digital Financial Asset Law (“DFAL”) will impose a variety of regulatory requirements on digital asset companies and cryptocurrency exchanges. Governor Newsom is expected to sign the DFAL into law, and new licensing requirements will spring into effect on January 1, 2025. The DFAL will prohibit a person from engaging in digital financial asset business activity without a license from the California Department of Financial Protection and Innovation (“Department”). Under the proposed law, “digital financial asset activity” will include exchanging, transferring or storing a digital financial asset, or engaging in digital financial asset administration both directly or through a vendor. It will also include holding electronic precious metals and related activities as well as online gaming assets tied to legal tender or the original value. “Digital financial assets” will be defined as a digital representation of value that is used as a medium of exchange, unit of account, or store of value and that is not already legal tender. The DFAL will apply to any person (including an individual, business, or any other legal entity) conducting digital financial asset business activity “with or on behalf of” a resident of California, as defined in the DFAL. The license application will require extensive background information.

A primary goal of the DFAL is to reduce consumer risk. The sponsor stated that DFAL indicates the legislature understands “that a healthy cryptocurrency market can only exist if simple guardrails are established.” The bill fashions these guardrails in the form of licensing and other compliance requirements for businesses and extensive oversight opportunities for the Department. To date, the Department

has taken a relatively light-touch approach with respect to some digital asset companies, including cryptocurrency exchanges, issuing a number of no-action letters in which it held that these companies were not subject to existing California money transmission licensing and compliance requirements. However, pursuant to the new DFAL, licensing requirements and several other strictures will be imposed on digital asset businesses.

Among other requirements, licensees will be required to maintain records of all California client activity for at least five years (a requirement that may sit uneasily with technologies focused on the preservation of anonymity). Licensees must also maintain a monthly ledger that outlines all assets, liabilities, capital income, and expenses of the licensee. Prior to engaging a California resident as a customer or client, each business will be required to make disclosures about fee totals, fee timing, and fee calculation. Licensees will be required to create and staff a 24-hour, toll-free helpline with live customer assistance. Licensees will also be required to create and maintain a set of security and other policies and procedures, including information security, business continuity, disaster recovery, antifraud, and AML and OFAC compliance programs.

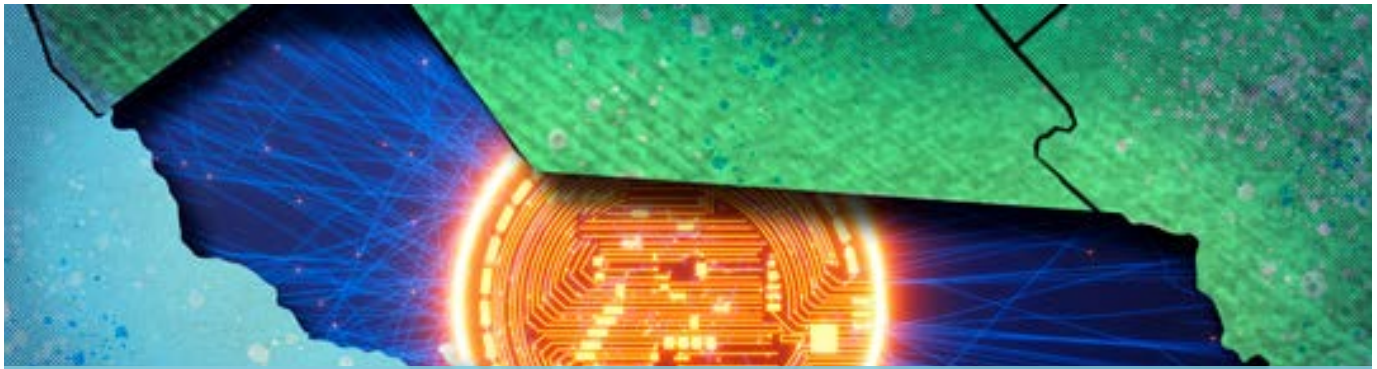
The DFAL will also grant the Department broad oversight and enforcement authority. The DFAL will allow the Department to conduct examinations of licensees and take enforcement measures against both licensed and unlicensed operators. Examinations can be undertaken at any time without notice to the business and at the business’

expense. Enforcement measures include judicial actions and fines of up to \$20,000 per day for licensees—and \$100,000 per day for unlicensed businesses.

In practice, the proposed California law is similar to New York’s “BitLicense” regulation. But unlike the BitLicense, the California law includes a “stablecoin” prohibition which bars a licensee from engaging in certain digital financial asset activity where the asset is a stablecoin unless (i) the issuer is a bank or licensee and (ii) the issuer owns eligible securities with the aggregate market value of not less than all outstanding stablecoins issued or sold in the United States. This provision will become inoperative on January 1, 2028.

The DFAL was presented to the governor on September 12, 2022.

The intersection of state regulatory regimes like California’s with federal law will bear close attention for digital currency businesses and those considering investments in them. This includes paying particular attention to federal treatment of digital assets that are or may be securities, and contemplating SEC and CFTC treatment of cryptocurrencies and other digital assets under a new and more comprehensive regulatory regime. Both of the major pieces of proposed legislation currently being considered by Congress to regulate digital assets (the Lummis-Gillibrand and Stabenow-Boozman bills) provide for federal preemption of at least some aspects of state regulation of digital assets. But if the DFAL is adopted in California and is not preempted by a comprehensive federal regime, the requirements of the DFAL described above may emerge as de facto national standards.



CALIFORNIA GOVERNOR ORDERS AGENCIES TO CREATE TRANSPARENT REGULATORY FRAMEWORK FOR BLOCKCHAIN AND DIGITAL ASSETS

MAY 2022 ALERT

California's governor issued an executive order requiring state agencies, led by the Department of Financial Protection and Innovation, to create a "transparent" regulatory framework for blockchain technologies and digital assets.

On May 4, 2022, California's governor issued [Executive Order N-9-22 \("California EO"\)](#), requiring California's Department of Financial Protection and Innovation ("DFPI") "to develop a comprehensive regulatory approach to crypto assets harmonized with the direction of federal regulations and guidance." The order frames California's goal for this regulatory framework as "creat[ing] a transparent and consistent business environment for companies operating in blockchain ... that harmonizes federal and California laws, balances the benefits and risks of consumers, and incorporates California's values, such as equity, inclusivity, and environmental protection." The order also acknowledges California's goal of "remaining the premiere global location for responsible crypto asset companies to start and grow" as a priority. At the same time, the order's emphasis on consumer protection demonstrates California's concern that digital assets pose unique risks to consumers and require careful examination.

The California EO contemplates collaboration and consultation with federal regulators, consistent with the federal strategy articulated in the [White House's executive order on ensuring responsible development of digital assets](#). To that end, the California EO requires various state agencies to collaborate on a report that makes recommendations for "[c]reating a regulatory approach to crypto assets harmonized between federal and state authorities, led by DFPI," and includes input from a broad range of stakeholders, as well as "relevant state agencies regarding ... the relationship of crypto assets to priorities in energy, climate, and preventing criminal activity."

The California EO specifically directs the DFPI to, among other things

- Engage with federal agencies and other state financial regulators to promote a common approach that increases the reach of DFPI's consumer protection efforts and reduces unnecessary burdens, if any, on companies seeking to operate nationwide;
- Exercise its authority under the California [Consumer Financial Protection Law](#) ("CCFPL") to develop guidance and, as appropriate, regulatory clarity and supervision of private entities offering crypto asset-related financial products and services in conjunction with California stakeholders; and
- Initiate enforcement actions for violations of the CCFPL, enhance its collection and review of consumer complaints regarding crypto asset-related financial products and services, work with companies offering such products and services to remedy complaints, and consult with appropriate law enforcement agencies regarding criminal activity.

Also relevant, in 2018, California passed legislation directed at consumer privacy and cybersecurity, creating a new regulatory framework, which may have unique state-level implications.

We will continue to monitor developments and counsel with clients as more concrete steps are taken in this process.



NEW YORK JOINS OTHER STATES IN ENFORCEMENT ACTIONS AGAINST UNREGISTERED VIRTUAL CURRENCY LENDING PLATFORMS

OCTOBER 2021 ALERT

The actions highlight a continuing trend by state regulators seeking to regulate cryptocurrency.

On October 18, 2021, New York Attorney General Letitia James directed two virtual currency lending platforms to immediately cease their unregistered and allegedly unlawful activities in New York and sent letters to three other platforms seeking information about their lending products and operations. These actions highlight a continuing trend by state regulators seeking to bring cryptocurrency-related products and services within their regulatory purview despite regulatory uncertainty at the federal level.

The [cease-and-desist letter sent to the two virtual currency lending platforms](#) alleged that they were unlawfully selling or offering for sale securities within the ambit of New York’s Martin Act within New York or to New Yorkers without having registered as brokers, dealers, or salespersons pursuant to Office of the Attorney General (“OAG”) regulations. The platforms were demanded to cease such activity, and confirm that the activity had ceased, or explain why the OAG should not take further action. The Martin Act sets forth a broad list of instruments that are declared to be securities, including “any stocks, bonds, notes, evidences of interest or indebtedness or other securities. . . .” It is a formidable anti-fraud statute that the OAG frequently invokes because it has a six-year statute of limitations and, according to the OAG and some court interpretations, does not require proof of intent or justifiable reliance. According to the OAG, because the virtual currency lending products at issue promise a fixed or variable rate of return to investors and claim to deliver those returns by, among other things, trading, or

further lending or hypothecating those virtual assets, they “fall squarely within any of several categories of ‘security’” under the Martin Act. A spokesperson for one of the platforms that received a cease-and-desist letter reportedly stated that, contrary to the OAG’s allegations, the platform did not offer the products at issue in New York, and used IP-based geoblocking to prevent New Yorkers from accessing the products.

From the other three platforms, the OAG has requested [information](#) concerning, among other things, each lending product they offer, how they use the virtual currency deposited with their platforms, the jurisdictions they operate in, information regarding any New Yorkers that accessed the platform, and how a stablecoin is used in their lending products.

Through these actions, New York has now joined five other states—New Jersey, Texas, Alabama, Kentucky, and Vermont—that have recently taken regulatory action against cryptocurrency market participants, despite regulatory uncertainty concerning decentralized finance (“DeFi”) and cryptocurrency at the federal level. This trend is likely to continue. Market participants should monitor state-level developments and be prepared for increased regulatory scrutiny from states, in addition to federal regulators like DOJ, the SEC and the CFTC, which continue to be [aggressive](#).



CRYPTO AND THE REACH OF UNCLAIMED PROPERTY LAWS: IS NEW ILLINOIS LEGISLATION THE FUTURE?

SEPTEMBER 2021 WHITE PAPER

Cryptocurrencies are quickly becoming part of the financial mainstream, with institutional and retail investors alike adding them to their portfolios in record numbers. State legislatures are trying to keep up with this growth by modifying abandoned and unclaimed property laws. Illinois Senate Bill 338, signed into law by Governor J.B. Pritzker (D) as P.A. 102-288 on August 6, 2021, exemplifies this trend. As amended by P.A. 102-288, the Illinois Revised Uniform Unclaimed Property Act will require holders to escheat dormant crypto and liquidate crypto into U.S. dollars in order to escheat. This both represents an administrative burden for crypto custodians and may be unwelcome by long-term crypto investors.

DEFINING AND UNDERSTANDING VIRTUAL CURRENCY

In 2017, Illinois adopted the definition of virtual currency that was developed for the Illinois Revised Uniform Unclaimed Property Act (“RUUPA” or “Act,” 765 ILCS 1026/15-101 et seq.):

a digital representation of value used as a medium of exchange, unit of account, or store of value, that does not have legal tender status recognized by the United States. The term does not include (A) the software or protocols governing the transfer of the digital representation of value; (B) game-related digital content; or (C) a loyalty card [or gift card]. 765 ILCS 1026/15-102(32).

The amended Act expands that definition to include “any type of digital unit, including cryptocurrency, used as a medium of exchange, unit of account, or a form of digitally stored value, which does not have legal tender status recognized by the United States.”

Unlike many other financial assets, cryptocurrencies and other blockchain-based digital assets were designed so they could be held directly by the owner, without a central

repository. Many people hold custody of their cryptocurrencies in this way, using wallet software that they alone control. This can be technologically challenging for some because it requires them to manage unwieldy hexadecimal codes known as private keys, and it places a burden on them to not lose those private keys. Because of these difficulties, many people prefer to have a third party hold custody of their cryptocurrency. Numerous hosted wallet service providers offer custodial services.

DORMANCY HOLDERS AND THE ABILITY TO ESCHEAT

One core component of abandoned and unclaimed property (“AUP”) laws is the tracking period for determining when a property has become “dormant.” Most common property types become dormant within one to five years. Once property becomes dormant, the holder of the property must contact owners to remind them that a debt is owed to them. The amended Illinois Act establishes a five-year dormancy period for virtual currency based on the last contact with the holder. Such contact, when it is sufficient

to defer dormancy, is referred to in the Illinois statute as an owner's "indication of interest" in the property.

The amended Act, however, does not specify types of owner-to-holder contacts for crypto that would constitute an indication of interest that defers dormancy. Using existing AUP frameworks as a guide, one might compare crypto to securities, where an indication of interest can be in the form of a vote, phone call, or email to the transfer agent to update the owner's personal information, and in some states, direct deposit of dividends. The analogy has limitations, though, because securities have a welter of requirements and reporting obligations placed upon those issuing, owning, and dealing in them.

A comparable regulatory framework unique to crypto transactions has not yet developed for escheat purposes. All or most crypto custodians likely have the electronic monitoring capacity to track when users log into the account, buy or sell crypto, or transfer crypto from one wallet to another. It is reasonable to anticipate that logging into one's account is a sufficient indication of interest to stave off dormancy, but are passive actions that affect an owner's wallet similar? As an example, if another party deposits crypto into the owner's wallet, will that toll dormancy? In many states, direct deposit of a securities dividend is no longer sufficient as an indication of interest. Will it be similar for crypto?

What such a framework may require becomes even more complicated as different types of crypto platforms are evaluated from an escheat-compliance perspective. Cryptocurrency exchanges in the United States are required under various applicable know-your-customer ("KYC") laws and regulations to implement policies that allow them to know the identity and addresses of their customers. The states, and their unclaimed property audit agents, are likely to deem such businesses the holder of property, and therefore hold them responsible for monitoring its dormancy and escheat.

Decentralized finance—DeFi—transactions are, however, different from transactions on an exchange. In DeFi transactions, there is no intermediary business or individual, such as a bank or an exchange that holds funds and reconciles accounts. DeFi protocols are built with open source code and rely on smart contracts, meaning there is no central organization or individual that directs or controls them. Smart contracts have written contract or loan provisions associated with them. If certain instructions are sent to a smart contract, and the conditions are met, then the code will execute automatically.

For example, DeFi liquidity pools allow lenders to deposit funds in a lending pool contract, for which a borrower can call on that contract and request to borrow funds. If all coded conditions are met, the loan will go through. Likewise, decentralized apps ("Dapps") beyond the DeFi

space contain a series of smart contracts that interact with one another and execute functions based on instructions they receive.

Any assets held at noncustodial smart contract addresses have the potential to become dormant. Monitoring contacts with such addresses and demanding escheat from ostensible holders may prove difficult, if not impossible, to enforce given their noncustodial nature.

Further, because there is no central administrator and no legal requirement or mechanism to collect owner names and addresses, in many cases, the only known information about the transacting parties will be their public keys. To which jurisdiction would a holder escheat dormant crypto when there is no owner name or physical address, or when there may be no state of incorporation or legal domicile for the holder to use? Further, the purported holder may not be located in the United States, raising the question of whether these transactions are subject to U.S. jurisdiction.

Gary Gensler, chair of the Securities and Exchange Commission ("SEC"), [recently vowed to "take our authorities as far as they go" and also asked for additional tools to regulate the crypto and DeFi industries](#). As the SEC continues to develop its regulatory structure, anticipate escheat laws to follow.

ESCHEATING CRYPTO

Once a crypto asset becomes dormant, the amended Act mandates the holder liquidate the crypto within 30 days prior to the compliance filing and remit the proceeds to the appropriate government authority. The term "escheat" refers to taking ownership of property. That term is inexact but commonly used to describe the process of remitting abandoned property to a state that will hold the property in custody for the owner. Illinois holds remitted abandoned property solely as a custodian, as stated in Section 15-804 of its Act, and is responsible for the safekeeping of the property.

The price of crypto fluctuates in dollar terms. It is not fixed like a paycheck or a receivable credit on account denominated in U.S. dollars. While there are a few crypto products with stable values, for instance stablecoins linked to a national currency like the U.S. dollar, the majority of cryptos see their values fluctuate as determined by the economic trends and vagaries that influence supply and demand. Crypto is often purchased with the expectation that the value will increase exponentially. Crypto values have fluctuated wildly, with prompts ranging from a reaction to a tweet to the economy to rumors. When liquidating dormant crypto, the holder would be locking in the value of the asset on the day of liquidation. The states have expressed their limitations with their ability to take custodial possession of the

multitude of crypto products. However, the Commissioner's Prefatory Note in the 1972 Uniform Unclaimed Property Act described the following policy behind the uniform act:

The Uniform Act is custodial in nature—that is to say, it does not result in the loss of the owner's property rights. The state takes custody and remains the custodian in perpetuity. Although the actual possibility of his presenting a claim in the distant future is not great, the owner retains his right of presenting his claim at any time, no matter how remote. State records will have to be kept on a permanent basis. In this respect the measure differs from the escheat type of statute, pursuant to which the right of the owner is foreclosed and the title to the property passes to the state. Not only does the custodial type of statute more adequately preserve the owner's interests, but, in addition, it makes possible a substantial simplification of procedure. 8 Uniform Laws Annotated 74 (1972).

The solution of requiring liquidation undermines that custodial nature. While owners can still collect their value, that value is now fixed and finite, unable to ride the ebbs and flows of the market.

Further, contracts with crypto custodians may contain provisions that limit the ability of a “holder” to liquidate and escheat crypto. Crypto holders may not have the legal right to use the owner's private key to direct a transaction on the blockchain to liquidate their value. While there is case law, such as *People v. Marshall Field & Co.*, 404 N.E. 2d 368 (Ill. App. 1980) that set forth anti-limitation provisions on “private escheat,” there are notable differences from the crypto holder scenario. In the *Marshall Field* case, the holder created contract provisions for its gift cards that would terminate the card value just shy of the period for which it would become escheatable (a five-year termination to undermine a seven-year dormancy period). *Marshall Field*, 404 N.E. 2d at 373. The court found that the anti-limitation provisions addressed contract terms that would be in “fundamental conflict with public policy.” *Id.* In comparison, the crypto exchanges hold private keys that control crypto. Is requiring an exchange or an online wallet provider to take an action beyond its contractual terms in fundamental alignment with public policy?

The true intent of the Illinois RUUPA is to safely hold crypto until the owner claims it. In this regard, the state has implemented protections for securities that could be emulated for crypto. Section 15-703 of the Act provides that the state must hold escheated shares for three years after delivery; if the shares are sold prior to that time, the owner is entitled to claim the value of the shares at the time of the claim, plus dividends and interest. The amended Act lacks a comparable safeguard for crypto. The state is limited in

infrastructure that would allow crypto to be transferred to the state in a custodial manner. However, there are viable alternatives, such as implementing a longer mandatory holding period (e.g., 10 years), developing strategic alliances with viable third-party providers to act as a holding mechanism for crypto, or directing the holder to segregate and hold the crypto until the state may give direction for the sale.

OWNER RECOURSE

The amended RUUPA states that “the owner shall not have recourse against the holder or the administrator to recover any gain in value that occurs after the liquidation of the virtual currency under this subsection.” It is unlikely that this limitation will dissuade legal action by the angry owner of crypto that increased tenfold since the date of liquidation for escheat compliance.

If the historical litigation trend by owners of escheated securities provides any guidance, owners will not stand by as docile observers when a holder liquidates his or her crypto for escheatment. When finding the value of crypto increased significantly after his wallet was liquidated, a crypto owner will likely go after everyone involved in what he views as an unlawful seizure and taking. States notoriously have not stepped up to shield duly compliant holders in the past, even in the face of a statutory obligation to do so. Query why they would behave differently with crypto.

Crypto is the new unclaimed property frontier. In fact, Delaware passed identical language to that of Illinois and mandates the liquidation and escheat of crypto, whereas New York and D.C. introduced bills that do not require liquidation of cryptocurrencies prior to escheat. Do P.A. 102-299 and similar proposals embody an appropriate balance for the states to safeguard the rights of owners of crypto, or do such state laws evoke the pickaxes and pans wielded by gold prospectors of old? We will likely find the answers in court.



NEW YORK DEPARTMENT OF FINANCIAL SERVICES IMPOSES PENALTY AND CONSENT ORDER FOR CYBERSECURITY VIOLATIONS

MARCH 2021 ALERT

The New York Department of Financial Services (“NYDFS”) fined a mortgage bank \$1.5 million for violations of New York’s Cybersecurity Regulation, including failure to report a past cyber incident.

On March 3, 2021, the NYDFS [announced](#) it had entered into a [consent order](#) with a mortgage bank for violating New York’s first-in-the-nation [Cybersecurity Regulation](#), which became effective in March 2019. The settlement results from the agency’s findings during a routine compliance examination that the mortgage bank had failed to investigate adequately a cyber incident that exposed private data, failed to report the incident under state data breach notification laws and the NYDFS Cybersecurity Regulation, and failed to conduct a comprehensive cybersecurity risk assessment—despite a certification of compliance with the Cybersecurity Regulation provided by the Chief Information Security Officer.

The examination revealed that the bank was aware of a successful phishing attack on an employee’s email account that contained sensitive personal data of loan applicants. The NYDFS considered the bank’s investigation into the incident to be inadequate because the bank did not review the contents of the email account to identify affected personal information and did not notify affected consumers and state agencies of the incident, as required under state data breach notification laws. The NYDFS also concluded that the bank had failed to comply with the NYDFS Cybersecurity Regulation, which required the bank to notify NYDFS within 72 hours of determining that the incident required notice to another government agency. As part of the settlement, the bank agreed to pay a \$1.5 million penalty and to comply with all provisions of the Cybersecurity Regulation.

The settlement demonstrates that the NYDFS is devoting resources to examining financial institutions for compliance with the Cybersecurity Regulation. To diminish the risk of an enforcement action, financial institutions should review their policies and test their implementing practices governing cyber, information and data security, privacy, business continuity, operations and risk management, and technology. In particular, to facilitate timely reporting of cybersecurity incidents, financial institutions should assess the sufficiency of their cyber incident response plans and reporting protocols and remediate issues before NYDFS conducts an examination.



CALIFORNIA PASSES LEGISLATION TO CREATE MINI-CFPB

OCTOBER 2020 COMMENTARY

IN SHORT

The Situation: On January 1, 2021, the California Consumer Financial Protection Law (“CCFPL”) will go into effect, and the Department of Financial Protection and Innovation (“DFPI”) will become the financial sector’s new state regulator.

The Result: The DFPI will replace California’s current Department of Business Oversight (“DBO”), and DFPI will regulate financial products and services in the state in accordance with the CCFPL.

Looking Ahead: Nonbank small business lenders and fintech companies, and the institutions that work with them, should prepare for the rollout of the new law, and all financial institutions should expect to be subject to more comprehensive oversight and regulation in California.

On August 31, 2020, the California State Legislature passed a bill that would enact the CCFPL and launch the DFPI as a new state regulator in the financial sector. As discussed in a previous Jones Day [Alert](#), this proposal was initially introduced through Governor Gavin Newsom’s 2020–21 budget and was [tabled](#) due in part to COVID-19 considerations. This led to the proposal moving over to the California State Legislature. Governor Newsom signed the bill on September 25, 2020, and it will go into effect on January 1, 2021.

Under the CCFPL, California’s current Department of Business Oversight (“DBO”) will be replaced by the DFPI, and, while retaining the DBO’s prior powers, the DFPI will be charged with regulating financial products and services in the state in accordance with the CCFPL. The CCFPL will “make it unlawful for covered persons or service providers, as defined, to, among other acts, engage in unlawful, unfair, deceptive, or abusive acts or practices with respect to consumer products or services, or offer or provide a consumer

a financial product or service that is not in conformity with any consumer law.” The DFPI will have wide-ranging regulatory and enforcement power, including the ability to conduct investigations, issue subpoenas, levy fines, bring civil and administrative actions, and declare acts as “abusive.” After the CCFPL becomes law, the DFPI will be required to promulgate implementing regulations, which will undoubtedly bring into further focus the regulated activities that will be within the scope of the CCFPL and DFPI.

Much of this structure is borrowed from the Consumer Financial Protection Act of 2010, which created the federal Consumer Financial Protection Bureau (“CFPB”). As a result, the DFPI is widely considered a “mini-CFPB,” and various commentators have highlighted the importance of the new law. For example, former DBO Commissioner Jan Lynn Owen explained that the CCFPL will enable California to become “a gold standard as a financial services regulator.” And, Richard Cordray, the first Director of the CFPB who had substantial involvement in the creation of the DFPI and

CCFPL, noted that “it could be the most powerful year ever for consumer financial protections in California.”

In enacting its mini-CFPB, California follows in the footsteps of states like New York, New Jersey, and Pennsylvania. But, California’s version of the mini-CFPB differs in a few key ways; namely, unlike in New Jersey and Pennsylvania, this unit will not be housed within the state Attorney General’s office. Instead, like the Department of Financial Services in New York, the DFPI will operate as an independent agency, with a dedicated staff and budget. As a result, the DFPI will be empowered to bring civil suits, with the possibility of big fines, independent of the Attorney General.

The CCFPL, however, is limited in a very important way. A “Covered Person” under the law is a person, or the affiliate of a person, that: (i) engages in offering or providing a consumer financial product or service to a resident of California; or (ii) any service provider to the extent that the person engages in the offering or provision of its own consumer financial product or service. But, this is carved back by a long list of exempted entities in the law including: (i) banks, savings associations and credit unions, as well as bank or savings and loan holding companies; (ii) persons otherwise licensed by the DFPI (i.e., finance lenders, brokers, residential mortgage lenders, money transmitters, escrow agents, and check sellers); and (iii) persons licensed under other California state laws not administered by the DFPI.

This exemption is key insofar as it seems to suggest that many major financial institutions will not be directly subject to the CCFPL. The California Bankers Association—which successfully lobbied for the exemption—said it is “neutral” on the bill due to the exemption being included. The end result is that mostly nonbank small business lenders and fintech companies are subject to the CCFPL. These entities should be actively preparing for the rollout of the new law and should expect to be subject to more comprehensive oversight and regulation in California, and the banks and financial institutions that partner with these entities should get ready to feel some effects as well.

TWO KEY TAKEAWAYS

1. The DFPI will have broad regulatory and enforcement power, including the ability to conduct investigations, issue subpoenas, levy fines, bring civil and administrative actions, and declare acts as “abusive.”
2. While California’s mini-CFPB will be a powerful force in consumer financial protections, the CCFPL is limited due to the exemptions carved out under the law.



FIRST DEPARTMENT UPHOLDS NY AG'S AUTHORITY TO INVESTIGATE VIRTUAL CURRENCY UNDER THE MARTIN ACT

AUGUST 2020 COMMENTARY

In Short

The Development: The First Department held that the New York Attorney General (“NYAG”) has broad authority to investigate virtual currency companies, while narrowing the scope of jurisdictional challenges that can be made to an ex parte request for documents and testimony, and to enjoin respondents from taking certain further action, pursuant to NY GBL 354.

The Result: In the first appellate decision to apply the NYAG’s investigative authority under the Martin Act to the cryptocurrency industry, the Appellate Division of the Supreme Court of New York, First Department issued a decision on July 9, 2020 in *James v. iFinex* that confirmed the NYAG’s wide latitude to investigate companies pursuant to the Martin Act.

Looking Ahead: The Appellate Division’s decision underscores the recent focus by the NYAG to police both the traditional banking industry as well as the fintech space. Companies hoping to challenge the NYAG’s authority to investigate securities and commodities fraud pursuant to the Martin Act face significant obstacles, as reflected in the First Department’s procedural and substantive findings.

BACKGROUND

In November 2018, the NYAG initiated an investigation into respondents BFXNA Inc., BFXWW Inc., and iFinex Inc. (collectively, iFinex) regarding tether, a virtual currency. The investigation was prompted by liquidity concerns regarding the ability to redeem tether at the represented value. During the course of the investigation, the NYAG requested and obtained an ex parte order pursuant to General Business Law (“GBL”) § 354, compelling respondents to produce documents and staying certain further actions pending the ongoing investigation into tether.

Respondents initially moved to quash or modify the ex parte order, and the modification request was granted in part. Respondents then moved to dismiss the ex parte order for, among other things, lack of specific personal jurisdiction and lack of subject matter jurisdiction, arguing that tether is not a security or commodity, and that iFinex wasn’t engaged in any business activity purposefully directed at New York. That motion was denied, leading to the instant appeal.

DECISION

On appeal the First Department affirmed the lower court's denial of respondents' motion to dismiss for lack of subject matter jurisdiction and lack of personal jurisdiction, finding that the trial court properly rejected respondents' attempts to limit the NYAG's investigative authority under the Martin Act.

The First Department began its decision with a discussion of the broad powers of the NYAG under the Martin Act to seek an ex parte order compelling the production of documents and testimony and enjoining respondents. The decision notes at the outset that the case raises important issues regarding the scope of the NYAG to investigate fraud under the Martin Act, and held that the trial court "properly rejected the attempts by respondents to limit [the NYAG's] lawful authority to protect New York residents."

The First Department held that, under the Martin Act's statutory scheme, once a court has issued an ex parte order pursuant to a GBL 354 application, it has no further role in the NYAG's investigation. Thus, the issuing court's authority is limited to considering a responding party's motion to modify or vacate the order. On that basis, the First Department held that there was no action or proceeding for the court to "dismiss" when respondents filed their motion to dismiss.

Nevertheless, the Court considered respondents' personal and subject matter jurisdiction arguments on the merits, and held that:

- i. Tether is a "commodity" under the Martin Act. The First Department held that that the Martin Act's definition of commodities was broad enough to encompass virtual currencies like tether, because commodities include "any foreign currency, any other good, article, or material." On that basis, the First Department held that the NYAG's documentary and other requests related to tether fell squarely within the subject matter jurisdiction of the NYAG's investigative authority.
- ii. iFinex had sufficient minimum contacts in New York to exercise specific personal jurisdiction. The First Department held that there were multiple bases for exercising personal jurisdiction over iFinex, including previous trading by New Yorkbased customers and the New York residence and conduct of business of one of respondents' executives within the state. The Court noted that the NYAG can establish personal jurisdiction to exercise its investigative authority by a "far lighter showing" than would be required to bring a lawsuit. As the Court also noted, this means that a Martin Act Investigation can be used to develop the information required to establish personal jurisdiction for a lawsuit.
- iii. The alleged deficiencies in service of respondents was a mere technical infirmity that could not support a finding of lack of personal jurisdiction.

The NYAG's investigation of iFinex is still underway; no charges have been brought to date.

TWO KEY TAKEAWAYS

1. The First Department has once again confirmed the broad reach of the NYAG's investigative powers of the Martin Act, reading an expansive definition of the word "commodities" to include virtual currencies. This decision serves to further emphasize the significant reach of the NYAG in policing both traditional and nontraditional areas of the financial sector and suggests that other virtual currencies and assets with similar features will likely be considered commodities in the future. The investigation underpinning this decision also provides a window into how the NYAG's office views cryptocurrencies and may signal future scrutiny by the office of the cryptocurrency industry.
2. The First Department's holding that the issuing court's authority is limited to considering a party's motion to vacate or modify an ex parte order pursuant to GBL 354 means that respondents will need to include within a motion to vacate or modify all contemplated challenges, including jurisdictional challenges, to the order. Targets of investigation should also be evaluating the timing of raising any issues concerning personal jurisdiction and subject matter jurisdiction when considering whether to file a motion to modify or vacate. Any jurisdictional challenges may be unlikely to succeed in light of the court's finding that a "lesser" showing is needed to establish jurisdiction under the Martin Act than is required in a lawsuit. It remains to be seen whether subject matter jurisdiction will ultimately be found to also require a "lighter" showing for an investigation under the Martin Act than traditional litigation.



FEBRUARY 2023 COMMENTARY

IN SHORT

The Situation: Following a string of bankruptcies among virtual currency firms, the New York Department of Financial Services has issued guidance on the practices and procedures it expects from certain state-regulated entities providing virtual currency custodial services.

The Result: These entities should review their current arrangements regarding customer safeguards in the context of the guidance, including how their customers' assets are segregated and whether they are treated solely as the property of their customers, as well review their due diligence and disclosure procedures with respect to customer assets under custody.

Looking Ahead: The guidance is designed to clarify the relationship between a virtual currency custodian and its customers to ensure the latter are better protected in the event of bankruptcy, particularly in situations where ownership of the virtual currency is at issue. New York has long been a first mover in virtual currency, and this guidance may influence future actions at the federal level.

NEW YORK DEPARTMENT OF FINANCIAL SERVICES ISSUES GUIDANCE FOR VIRTUAL CURRENCY CUSTODIANS

On January 23, 2023, the New York Department of Financial Services (“NYDFS”) issued guidance to certain New York-regulated virtual currency entities on proper disclosure and custody practices. The *Guidance on Custodial Structures for Customer Protection in the Event of Insolvency* (the “Guidance”) applies to entities that provide virtual currency custodial services as either holders of New York’s BitLicense or its Limited Purpose Trust Charter. The Guidance sets forth NYDFS’s expectations for virtual currency entities (“VCEs”) that provide custodial services

(“VCE Custodians”) on standards and procedures “to better protect customers in the event of an insolvency or similar proceeding ... [by] providing a high level of customer protection with respect to asset custody under the BitLicense.” Notably, the Guidance is not a statute or a regulation with the force of law.

The Guidance sets forth NYDFS’s expectations in four areas:

- **Segregation of and Separate Accounting for Customer Virtual Currency:** NYDFS expects that VCE Custodians will hold the virtual currency of customers in either “separate on-chain wallets and internal ledger accounts for each customer” or omnibus wallets containing only customer virtual currency held by the VCE Custodians as agents or

trustees. That is, VCE Custodians should not commingle proprietary digital assets with customer assets. If a VCE Custodian holds customer virtual currency in an omnibus wallet—comingling customer assets with other customer assets only—it must uphold appropriate recordkeeping and internal audit trail procedures such that it is able to promptly and accurately identify each customer’s beneficial interest.

- **VCE Custodian’s Limited Interest in and Use of Customer Virtual Currency:** The Guidance restricts a VCE Custodian’s interest in the assets under its control, directing VCE Custodians to “structure their custodial arrangements in a manner that preserves the customer’s equitable and beneficial interest in the customer’s virtual currency.” Further, the Guidance advises VCE Custodians to treat all customer assets under their control as solely the property of the customers, and to avoid handling customer assets as if they were the property of the VCE Custodians. NYDFS expects that customer assets will not be used to secure or guarantee an obligation of, or extend credit to, the VCE Custodian or others.
- **Sub-Custody Arrangements:** VCE Custodians may enter into sub-custody arrangements with third parties, provided that they conduct appropriate due diligence and obtain prior approval from NYDFS.
- **Customer Disclosure:** VCE Custodians must disclose their terms of service to customers, including their procedures for segregating customer assets, what property interest customers will retain, and how the VCE Custodians can use the virtual currencies they hold. VCE Custodians must also obtain customers’ acknowledgment of such terms. For VCE Custodians that offer digital asset staking and lending programs, more clarity may be needed on how these disclosure provisions interact, if at all, with NYDFS’s expectation that VCE Custodians will not make extensions of credit using customer assets.

Significance of the Guidance

NYDFS issued the Guidance subsequent to a string of bankruptcies in the virtual currency space. Customer rights have been a central issue in these recent bankruptcies, particularly in regards to whether ownership of customer virtual currency held by a custodian lies with the customer or with the custodian (and therefore the bankruptcy estate). In such situations, one way that some VCE Custodians have attempted to protect customer rights to their assets is to include language in customer agreements permitting the parties to “opt-in” to Article 8 of the Uniform Commercial Code (the “UCC”), which, by electing to treat the VCE Custodian as a “securities intermediary” and the virtual currency as “financial assets” under the UCC, can provide a customer with greater protections in the event of

bankruptcy. The Guidance, however, does not mention this option. See UCC, Article 8, Sections 8-103, 8-303.

The question of how customer digital assets held by failed VCE Custodians should be treated is still playing out in bankruptcy courts, although a recent ruling in the *Celsius Network* bankruptcy proceedings indicates that the answer hinges on the nature of the custodial relationship. On January 4, 2023, the Bankruptcy Court for the Southern District of New York ruled that customer assets in certain Celsius accounts belonged to the bankruptcy estate, not to Celsius customers, as the customers had “entered a contract which contained unambiguous and clear language regarding transfer of title and ownership of assets” to Celsius. *Celsius Network LLC, et al.*, Case No: 22-10964, Docket No. 1822, at 39 (Bankr. S.D.N.Y. 2023). The Guidance could help to prevent similar future situations by ensuring customers retain equitable and beneficial interest in the virtual currencies stored with VCE Custodians, and by setting an expectation of clear disclosures to customers regarding the property interest maintained by customers in digital assets stored with custodians.

Three Key Takeaways

1. NYDFS has taken notice of issues customers face when VCE Custodians file for bankruptcy and, as a result, has provided clarifying guidance to BitLicensees and New York limited purpose trust companies that provide custodial services for customer digital assets.
2. The Guidance lays out customer protections that NYDFS expects VCE Custodians to provide, including procedures for segregation of funds, a clear custodial relationship (as opposed to a debtor-creditor relationship), properly vetted and approved sub-custody arrangements, and appropriate disclosure practices.
3. If a VCE Custodian maintains procedures as outlined in the Guidance, customers may enjoy greater protections in the event of the custodian’s insolvency.

CHAPTER VI

**REGULATORY
ISSUES
(INTERNATIONAL, EU)**



DUBAI'S DIGITAL ASSETS ASPIRATIONS

OCTOBER 2022 COMMENTARY

IN SHORT

The Situation: On 11 March 2022, Dubai Law No. 4 of 2022 Regulating Virtual Assets in the Emirate of Dubai (the “Law”) came into effect. The Law establishes the foundation of a regulatory regime for virtual assets in Dubai with the goals of protecting investors and promoting responsible business growth. To achieve those goals, the Law: (i) creates a virtual assets regulator; (ii) empowers the regulator to create appropriate laws and regulations; (iii) defines “Virtual Asset”; and (iv) identifies services that will require a license.

The Result: The first six months of this Law have seen Dubai’s dedicated virtual assets regulator, the Dubai Virtual Assets Regulatory Authority (“VARA”), take two important steps. First, it has issued administrative orders governing the marketing, advertising, and promotion of Virtual Assets. Second, it has issued provisional approval to operate in Dubai—referred to as a Virtual Asset Minimum Viable Product License (“MVP License”)—to several global crypto, blockchain, and digital asset market participants.

Looking Ahead: We expect the regulations and orders to be established by VARA to cover a broad range of matters, including: (i) detail around the classification of different virtual assets and tokens; (ii) the issuance of a code of professional ethics binding on virtual asset service providers; (iii) a regime establishing embargos on specific virtual assets and/or virtual asset-related activities; and (iv) the development of rules and regulations related to KYC, anti-money laundering, and financial crime. In the medium-term, we hope to see regulations defining the extent and scope of cooperation as between the United Arab Emirates’ (“UAE”) federal pan-emirate, individual emirate, and financial free zone regulators. This should enable market participants to offer digital asset-related products and services across the UAE without seeking approvals from multiple authorities.

INTRODUCTION

The UAE and its individual emirates are positioning themselves as hubs for the digital asset economy by introducing laws and regulations designed to promote market confidence. Lawmakers and regulators, both onshore and within the UAE's financial free zones (the DIFC in Dubai and the ADGM in Abu Dhabi), have created separate legislative frameworks for market participants looking to operate in the sector. Dubai recently adopted a virtual asset regulatory scheme for the purpose of protecting investors and promoting responsible business growth.

A potential challenge for market participants will be navigating the different frameworks across the UAE's jurisdictions due to the varying and sometimes overlapping laws, such as: (i) decisions by the UAE Securities and Commodities Authority; (ii) circulars by the UAE Central Bank; (iii) regulations of the ADGM and DIFC; and (iv) overarching criminal laws that can apply. Nonetheless, it is clear that businesses conducting virtual assets activities in "onshore" Dubai must comply with the Law, its administrative orders, and its upcoming implementing regulations.

VARA'S AUTHORITY

VARA has been established as an independent entity with financial and administrative autonomy to achieve the goals of the Law. VARA's jurisdiction spans across the Emirate of Dubai, including in all its free zones other than in the DIFC. Once the Law's implementing regulations are adopted, industry participants must establish a presence in Dubai, register with VARA, and obtain a license prior to engaging in any of the virtual assets activities identified in the Law.

VARA is mandated to protect investors and dealers in Dubai by monitoring transactions and preventing price manipulation of virtual assets. It has a broad range of powers to classify, define, regulate, expand, and prohibit these activities. Its responsibilities include:

- Issuing and enforcing the applicable rules in Dubai (excluding the DIFC) and developing a code of ethics;
- Establishing additional controls for conducting virtual assets-related activities, such as the provision of management, clearing, and settlement services for virtual assets;
- Assessing, classifying, and specifying the different types of virtual assets;
- Preparing the general policy and strategic plans related to the regulation of virtual assets services;
- Supervising, licensing, and regulating the sector across Dubai's mainland and the free zone territories (again, excluding the DIFC); and

- Providing anti-money laundering support and raising public awareness on dealing in virtual assets and their associated risks.

VARA undertakes its regulatory responsibilities in coordination with the Dubai Digital Authority, as well as with UAE federal regulators such as the Central Bank of UAE and the Securities and Commodities Authority. These regulators' oversight somewhat overlaps, and therefore, market participants in Dubai need to carefully consider all relevant regulations and engage with all three regulators at an early stage of any enterprise.

DEFINITION OF THE TERM "VIRTUAL ASSETS" UNDER THE LAW

The Law broadly defines "Virtual Assets" as:

"digital representation[s] of value that can be digitally traded, transferred or used as an exchange or payment tool or for investment purposes, including virtual tokens, and any digital representation of any other value as determined by VARA."

Not only is this a broad definition, but its final limb empowers VARA to determine what may constitute a virtual asset, giving the regulator an element of control over the asset class. This reinforces the importance of market participants proactively engaging with regulators and advisors at an early stage.

The definition contains elements that are common to the legislative approach in other jurisdictions. For example, under the Law, "Virtual Assets": (i) are "created electronically/digitally"; (ii) "confer digital representation of value"; and (iii) are "digitally traded or transferred". Legislation in the United States, England, Singapore, and the European Union use similar elements when setting the parameters for what constitutes virtual or digital assets. Of course, this should not be taken to mean that "Virtual Assets" under the Law would by default constitute virtual or digital assets in these other jurisdictions. This is a fast-developing area of law, and these salient elements can change as the asset class evolves.

PRESENCE AND LICENSING REQUIREMENTS FOR CERTAIN SERVICE PROVIDERS

The Law requires service providers to establish a presence in Dubai, register with VARA, and obtain a license prior to conducting any of the following virtual assets activities in Dubai or any of its free zones:

- Operating and managing virtual assets platform services;
- Exchange services between virtual assets and currencies, whether national or foreign;

- Exchange services between one or more forms of virtual assets;
- Virtual assets transfer services;
- Virtual assets custody, management, or control services;
- Services related to the virtual assets' portfolio; and
- Services related to the offering and trading of virtual tokens.

VARA has been empowered to expand, classify, and/or further define the above activities and to set prohibitions on such practices.

Although the Law does not apply in the DIFC, as a practical matter, industry participants who wish to operate in the DIFC can at present do so from their onshore Dubai presence, given that neither the DIFC nor its regulator, the DFSA, have established a presence requirement.

It remains to be seen what VARA's presence requirement will mean for truly decentralized technologies, as the Law does not provide an exception for such technologies. However, with both the gift of giving and the power to revoke licenses, VARA is now the ultimate gatekeeper into Dubai's digital asset economy—with this in mind, prudent operators wishing to target consumers in Dubai would be well-advised to comply with the Law.

IMPLEMENTING REGULATIONS AND ADMINISTRATIVE ORDERS

The Law grants the Director General of the Dubai World Trade Centre Authority, of which VARA is a part, the power to adopt implementing regulations proposed by VARA and for VARA to issue administrative orders.

The timeframe for the issuance of any implementing regulations is not prescribed in the Law, and VARA has not disclosed its intended timeframe for proposing regulations. But under the Law, the Director General is empowered to issue regulations by publishing them on VARA's website, without the need to publish in the *Official Legal Gazette*. We expect the initial package of implementing regulations will set out, among other things, the administrative procedures related to the procurement of licenses, as well as the information and documents required of applicants for VARA to grant its approval. Ultimately, VARA's role in proposing these regulations gives it a high degree of influence over the future direction of Dubai's virtual assets regulatory regime.

On 25 August 2022, VARA issued its first two administrative orders. These orders establish: (i)

the rules on marketing, advertising, and promotions related to virtual assets (the "Marketing Regulations"); and (ii) the fines applicable for breaches of the Marketing Regulations (the "Penal Regulations"). They are designed to ensure consumers, and in particular less sophisticated retail consumers, are safeguarded from unscrupulous actors in the industry.

The Marketing Regulations provide a nonexhaustive list of activities that constitute advertising and promotion. They also set out prescriptive guidelines on the nature of any advertising materials and how the promotion of virtual assets must be made in Dubai. Specifically, all marketing relating to virtual assets and/or virtual assets activities must:

- Be fair, clear, not misleading and clearly identifiable as marketing or promotional in nature;
- Not mislead in relation to the real or perceived advantages of virtual assets;
- Include a prominent disclaimer with respect to the volatility and unpredictability of the value of virtual assets;
- Not advocate that investments are safe, low risk, or that returns are guaranteed;
- Not imply that investment decisions are trivial, simple, easy, or suitable for all (without due diligence);
- Not imply that past performance of investments is an effective guide for, or guarantee of, a future return;
- Not imply an urgency to buy virtual assets in anticipation of future gains, or create a fear of missing out on future gains, by not buying now;
- Not advocate the purchase of virtual assets using credit or other interest accruing facilities;
- Ensure that any targeted marketing is undertaken responsibly by licensed entities, to present only appropriate products or services to the audience, including but not limited to defined criteria on investor qualification, and event attendance; and
- Otherwise comply with all applicable laws, regulations, guidelines, or other rules applicable across the UAE.

We expect these rules will apply to marketing and promotional materials or activities in a broad set of circumstances, ranging from coin/product launches to crypto-related events and conferences. Stakeholders across the digital asset industry should be aware of their application. Interestingly, the Marketing Regulations are intended to apply to any entity that seeks to target or cater for UAE residents and customers, even if the promoter is a foreign entity that is not licensed by VARA. How VARA will interpret

the extent to which foreign entities “cater for residents” and therefore fall within the scope of the regulations is not yet clear. Even if a foreign entity falls within scope and is found to breach the regulations, it remains to be seen whether or how VARA will enforce its rules on an extraterritorial basis.

ENFORCEMENT AND PENALTIES

Violations of the Law or of its future regulations can result in penalties and fines, including the suspension or revocation of a license to engage in virtual assets activities or the revocation of the violating party’s commercial license.

In enforcing the Law and its related regulations, VARA has the capacity and powers of a judicial officer and can collaborate with the relevant local and federal authorities to access and seize records, documents, devices, and properties as needed. All persons, including virtual assets service providers, must cooperate with VARA and meet its requests in accordance with the provisions of the Law and its implementing regulations.

Penalties for noncompliance with the Marketing Regulations are set out in the Penal Regulations. Fines start from AED 20,000 and go up to AED 500,000 per offence for repeat offenders. VARA reserves the right to revoke any VARA-issued license, rescind any approvals, and/or suspend any commercial trade license in coordination with the relevant regulatory authorities.

VARA IN ACTION

The first six months of this Law have seen VARA issue MVP Licenses to a number of global crypto, blockchain, and digital asset exchange applicants. The initial interest from global institutions is a positive step for Dubai’s digital asset ecosystem and reinforces the value of regulating the industry. Applicants will be required to apply for full VARA licenses in due course.

Given the breadth of powers granted to VARA, we expect its future implementing regulations and administrative orders could cover a broad range of matters, including: (i) detail around the classification of the different types of virtual assets and tokens; (ii) the issuance of a code of professional ethics binding on virtual asset service providers; (iii) a regime establishing embargos on specific virtual assets and/or virtual asset-related activities; and (iv) the development of rules and regulations related to KYC, anti-money laundering, and financial crime. However, the extent to which virtual asset industry players with MVP Licenses actually establish long-term, meaningful operations in Dubai as a result of this new framework will depend very much on the details of the regime.

OUR EXPERIENCE

Given the ever-evolving nature of digital assets and the underlying technologies which underpin the asset class, we expect more laws and regulations regulating the industry to be adopted in the UAE in the short to medium-term. For example, we would not be surprised to see regulations defining the extent and scope of cooperation as between the UAE’s federal pan-emirate, individual emirate, and financial free zone regulators. This should enable market participants to offer digital asset-related products and services across the UAE without potentially requiring multiple approvals. As the regulatory framework develops, investors and technology developers will benefit from the certainty afforded by an established regime, creating further opportunities for innovation and growth.

Contact us if you have any questions about the Law or would like more information about our capabilities on digital asset-related matters. Our international fintech team regularly advises businesses operating in the digital asset industry on complex matters, often requiring cross-border collaboration across disciplines ranging from regulatory compliance; banking, finance, and securities; corporate M&A and joint ventures; and fraud, anti-money laundering, and investigations.

THREE KEY TAKEAWAYS

1. The virtual asset sector and efforts to regulate it are in the nascent stages, but Dubai is among the jurisdictions moving virtual asset regulation into the mainstream. Under its new Law, service providers engaging in virtual assets activities in Dubai or any of its free zones (except DIFC) must now: (i) obtain a valid license from VARA; (ii) establish a presence in the Emirate; and (iii) comply with provisions of the Law and its implementing regulations. For the time being, entities with a presence in onshore Dubai can operate in the DIFC without duplicating their presence there.
2. The Law empowers VARA to propose regulations and gives the Director General of the Dubai World Trade Centre Authority the authority to issue such regulations by publishing them on VARA’s website. While implementing regulations have not been published yet, VARA has issued two administrative orders that ultimately seek to protect consumers in relation to the marketing and promotion of virtual assets.
3. VARA’s powers are broad and include enforcement authority. Because of the penalties associated with violation of the Law or its implementing regulations, industry participants subject to the Law should engage early with VARA, other regulators in the UAE, and their advisors.



AUGUST 2022 WHITE PAPER

The European Parliament (“EP”) and Council have formally adopted the Digital Markets Act (“DMA”) in July 2022, imposing new behavioral obligations on large digital platforms qualifying as “gatekeepers.” The final agreement introduces several changes compared to the initial proposal detailed in our [January 2021 Commentary](#), the most significant of which are: increase in the thresholds that qualify a business as a gatekeeper; the addition of web browsers and virtual assistants to the list of core platform services; additional behavioral obligations, including an interoperability requirement for messaging services; and new sanctions for systematic violations such as a temporary ban on a gatekeepers mergers and acquisitions.

The European Commission (“EC”) [initially proposed](#) the DMA in December 2020 with the stated goal of promoting fair and contestable markets in the digital sector. The DMA is an unprecedented shift in the European Union’s oversight of large digital platforms. Historically, the EC observed a “law enforcement” approach when addressing the conduct of digital platforms, investigating and sanctioning conduct only when it believed a practice violated EC competition law. The DMA, however, is a more regulatory approach that eliminates the EC’s burden to analyze and prove market definition, market power, and efficiencies.

WHAT IS THE DMA?

As described in our June 2020 *Alert*, “European Commission Considers Expanding Investigative and Regulatory Authority in Digital Sector,” the EC launched a public consultation to propose regulations of “very large online platforms” with the goal of “ensur[ing] contestability, fairness and innovation and the possibility of market entry” in online platform markets.¹ The DMA proposal in December 2020 followed years antitrust enforcement at EU- and Member State-levels focused on large digital platforms. Those cases have met with mixed results. Advocates for increased enforcement argued that the existing antitrust laws are inadequate to address the unique antitrust problems they allege large digital platforms present, and that, even if successful, the European Union’s efforts have taken too long to achieve.

Attempting to solve for those “problems,” the DMA would establish far-reaching, behavioral rules automatically

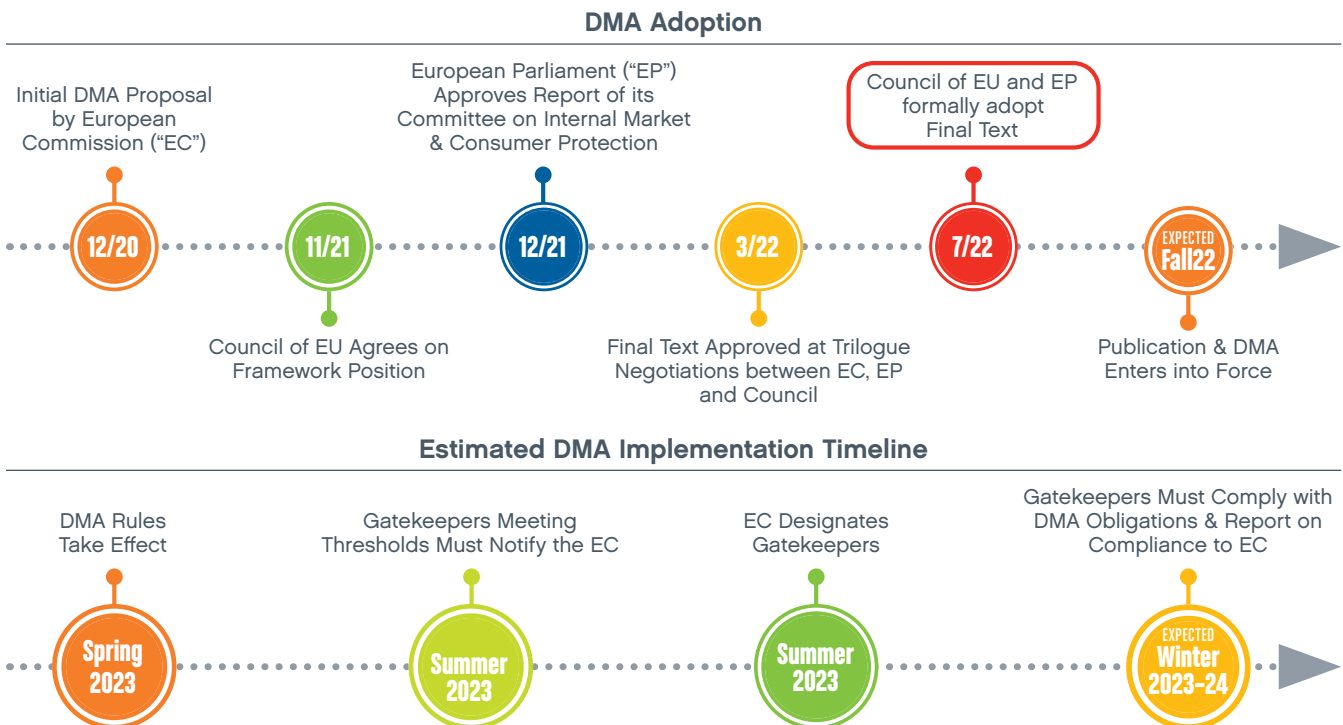
applicable to all businesses predesignated as a “gatekeeper.” At a conceptual level, gatekeepers are online platforms such as marketplaces, social media, or app stores that “control” access to users, goods, or services. More specifically, the DMA defines “gatekeepers” to include businesses of a certain size, based on various user, revenue, or valuation thresholds, and that provide certain “core platform services,” such as online search engines or cloud computing services. The DMA subjects companies designated as gatekeepers to a long list of behavioral dos and don’ts, many of which were the subject of EC and Member State antitrust investigations and litigation against online platforms. The DMA therefore eliminates the EC’s obligation to conduct an extensive antitrust investigation required to prove dominance, anticompetitive effects, or adequate remedies.

WHEN WILL THE DMA TAKE EFFECT?

Approximately 20 months passed between the launch of the DMA proposal and its formal adoption, which is short by EU standards. Now that the European Parliament and Council have adopted the DMA, it will be published in the official journal during fall 2022 and enter into force in spring 2023.

The EC will then undertake a process in which it designates gatekeepers, i.e., the businesses subject to regulation under the DMA. Designated gatekeepers will then have to comply with the new set of rules by early 2024. The implementation of this regulation will undoubtedly be massive and complex. The EC is expected to recruit about 80 to 150 staff to form the unit in charge of DMA oversight.

Figure 1: Anticipated Timelines



WHAT IS A GATEKEEPER?

As noted above, at a high level, a gatekeeper is an online provider of “core platform services” such as an online marketplace, search engine, social media outlet, or app store that “controls” access to users, goods, or services. A gatekeeper needs to be designated as such by the EC.

The DMA also sets forth certain revenue, valuation, and user thresholds above which a company will be presumed to be a gatekeeper. The aim of the DMA is to prevent a gatekeeper from imposing allegedly unfair conditions for business users and end users of core platform services.

Figure 2: The Two Prongs of a Gatekeeper

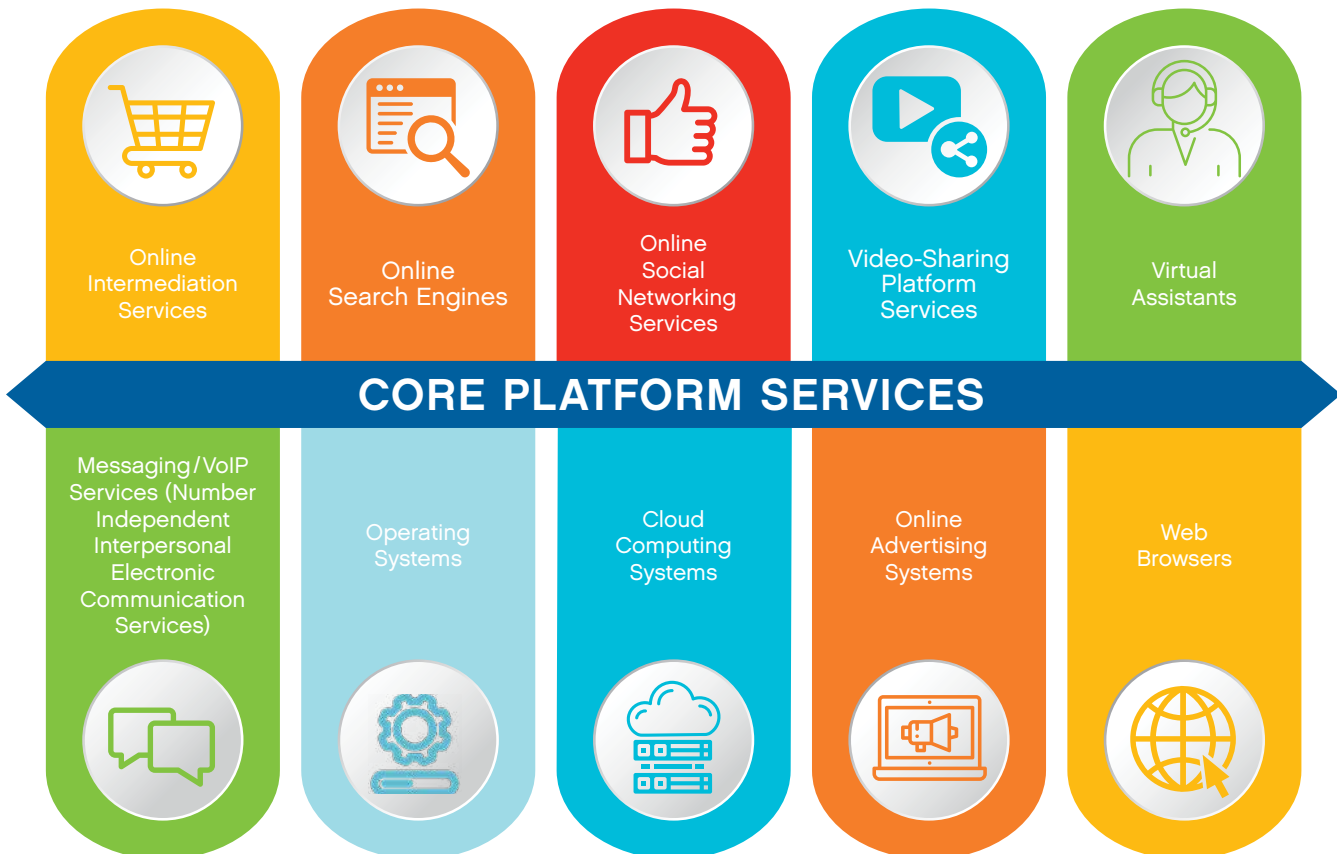


What Are Core Platform Services?

The DMA applies only to companies that offer the type of digital services categorized as a core platform service, identified below in Figure 3. The EC developed the list of core platform services based on its view that those services

are “most widely used by business users and end users” and because “based on current conditions, concerns about weak contestability and unfair practices by gatekeepers are more apparent and pressing.”²

Figure 3: List of Core Platform Services

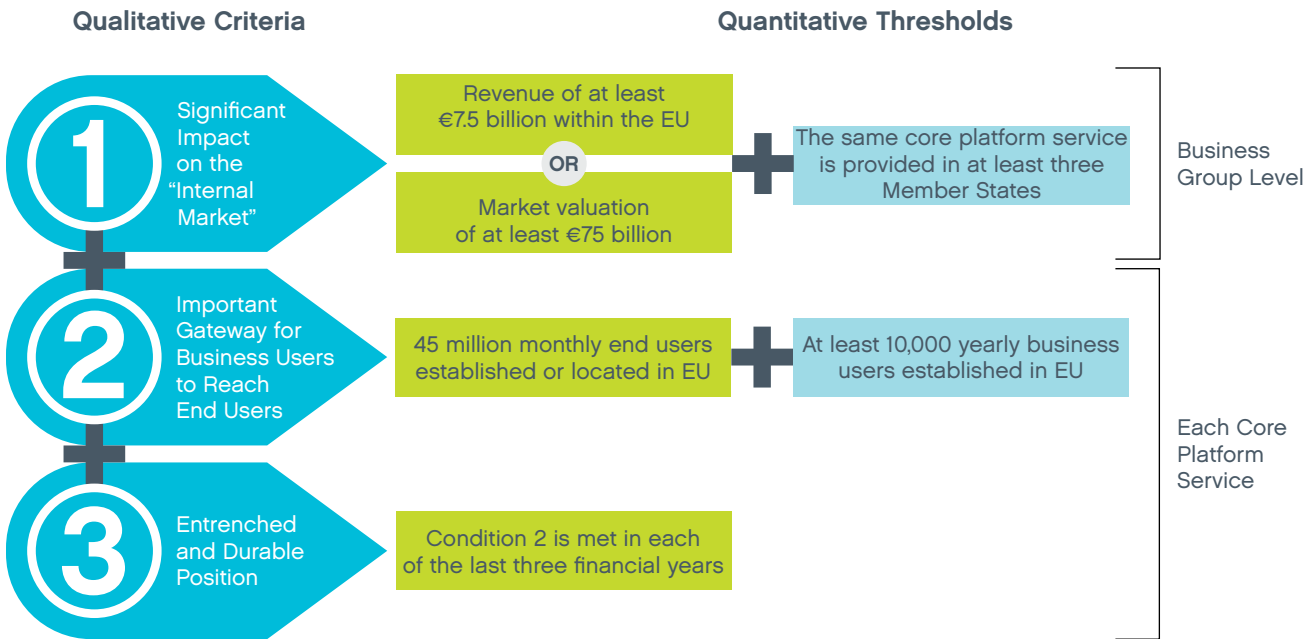


What Are the Gatekeeper Thresholds?

Under the DMA, the EC will designate a core platform service provider as gatekeeper if it fulfills three cumulative, qualitative criteria, presumed when the quantitative thresholds in Figure 4 are met. Preliminary expectations are that

the DMA could capture the businesses of approximately 10 to 15 companies, most of which are likely to be based in the United States.

Figure 4: Gatekeeper Qualitative and Quantitative Criteria



The EC’s gatekeeper presumption is rebuttable. Therefore, providers of core platform services that otherwise meet the EC’s thresholds will have an opportunity to argue that their business does not meet the qualitative thresholds due to specific circumstances. Conversely, the EC has authority under the DMA to investigate whether a core platform service provider meets the qualitative criteria, even if that provider does not meet the quantitative thresholds, and designate that company as a gatekeeper. The EC may consider factors such as network effects and data-driven advantages, scale and scope effects, business user or end user lock-in, a conglomerate corporate structure, vertical integration prone to cross-subsidization, data combinations, or leveraging, among other criteria.

There are a handful of other rules for potential gatekeepers to consider that will affect the scope and timing of EC regulation.

- As noted above, to qualify as a gatekeeper, a company must provide or offer the core platform service to business users established in the European Union and end

users established or located in the European Union. Gatekeeper status therefore is not based upon a company’s principal place of business or corporate residence. Thus, the DMA is likely to have an extraterritorial effect as the EC intends for it to apply regardless of a company’s location or the law otherwise applicable to the provision of a company’s services.

- In some cases, a company may provide several core platform services but have gatekeeper status for only a subset of its services. In those circumstances, the DMA will apply only to those core platform services for which the EC has designated the company as a gatekeeper.
- A company that provides several core platform services will be regulated under the DMA only for the services for which the EC has designated it a gatekeeper, and after such designation has taken place.
- The DMA empowers the EC to modify, over time and under certain circumstances, the list of core platform services, thresholds, and list of obligations to reflect innovation in digital markets.

WHAT WILL THE EC'S GATEKEEPER DESIGNATION PROCESS BE LIKE?

Once the DMA goes into effect, likely in spring 2023, a company will have two months to notify the EC that it meets the gatekeeper thresholds and, if appropriate, present arguments about why the EC should not designate the company as a gatekeeper. The EC in turn will have 45 working days (instead of 60 in the initial proposal) to make a designation, which is subject to judicial review. A designated gatekeeper

then will have six months to bring its core platform services in compliance with the obligations in the DMA and to explain in a report to the EC how it will comply with the DMA, with the EC expecting compliance by early 2024. The EC subsequently will review each gatekeeper designation every three years, to ascertain whether the gatekeeper conditions remain fulfilled.

Figure 5: EC Designation Process



WHAT IS THE IMPACT OF A GATEKEEPER DESIGNATION ON A BUSINESS?

The DMA introduces 22 behavioral obligations to which all designated gatekeepers must comply, in addition to new merger control (Article 14) and audit requirements (Article 15). The behavioral obligations will prevent gatekeepers from pursuing practices that in the EC's views are unfair or that limit the ability of small or new competitors to challenge larger incumbents, even if the conduct does not otherwise violate an existing antitrust law. Critics of the DMA argue that existing competition law is capable of policing any anticompetitive behavior and that the DMA's regulatory approach could stifle innovation or increase privacy and security risks.³

Figures 6 and 7 identify the DMA obligations. Obligations under the DMA are either "self-executing" (Art. 5) or "susceptible of being further specified" (Art. 6 and 7). Although gatekeepers must comply with both sets of rules, the list in Article 5 prohibits discrete conduct related to the gatekeeper's dealings with customers or end users that, in the EC's view, a gatekeeper can implement without further guidance. Examples include prohibitions on tying distinct core platform services, most-favored nations clauses, or anti-steering provisions.

In contrast, compliance with Article 6-7 obligations may require further consultation with the EC to interpret the obligation or to develop metrics by which the gatekeeper can measure its compliance. The balance of the Article 6-7 rules cover interoperability with core platform services and access to platform data. While the EC could refuse a

request to consult regarding Article 6-7 obligations, the EC expressed a willingness to dialogue with gatekeepers about how to best implement all obligations.

Although the 22 behavioral obligations are a patchwork of stand-alone dos and don'ts, the balance of the obligations can be bucketed to achieve a handful of objectives:

- Reducing purported advantages of big data and lowering alleged entry barriers
- Facilitating switching and multihoming
- Ensuring platform or device neutrality
- Preventing lock-in effects
- Prohibiting "leveraging" conduct such as tying, sideloading (not allowing third-party application stores or software to run on an operating system), or limits on gatekeeper ID or payment services
- Promoting transparency

While the EC in theory could apply all of the obligations to all gatekeepers, some are formulated in a way that they will apply only to specific core platform services (e.g., access to search data, messaging interoperability). The impact of the obligations thus may be different depending on the core platform services at stake and the business models pursued by each gatekeeper (e.g., whether they already follow closed or open economic models). The obligations could be summarized as follows:

Figure 6: DMA Article 5 “Self-Executing” Rules

DMA Article	Prohibition	⊗	
	Obligation	✔	
5(2)	⊗		Combination of personal data across platform services or from third-party services without user consent.
5(3)	⊗		Price parity or most-favored nations (“MFN”) clauses.
5(4)	⊗		Contract terms that prevent business users from doing business with customers outside of the platform (“anti-steering”).
5(5)	⊗		Restrictions on access and use, on a business user app, to content, subscriptions, features, and other items, even when acquired outside of the platform (“usage restrictions”).
5(6)	⊗		Restrictions on user complaints about the gatekeeper’s services to public authorities or courts.
5(7)	⊗		Mandatory interoperation with an identification service, web browser engine, or technical service that supports payment services related to services provided by the business user using that gatekeeper’s core platform services.
5(8)	⊗		Tying core platform services.
5(9)–(10)	✔		Transparency of prices and fees for online advertising services.

Figure 7: DMA Article 6-7 Rules “Susceptible of Being Further Specified”

DMA Article	Prohibition	⊗	
	Obligation	✔	
6(2)	⊗		Use of a business user’s nonpublic data to compete with that business.
6(3)	✔		Easy uninstallation of software applications on an operating system.
6(4)	✔		Sideloaded: Installation, use, and/or interoperability of third-party software applications or app stores, subject to limited security measures.
6(5)	⊗		Preferencing products the gatekeeper offers over similar products or services of a third party.
6(6)	⊗		Restricting end users’ ability to switch between different software applications accessed using the gatekeeper’s core platform services.
6(7)	✔		Nondiscriminatory access to or interoperation with the gatekeeper’s hardware or software features.
6(8)	✔		For advertisers and publishers, access to the gatekeeper’s performance tools and data necessary to verify advertisements of inventory.
6(9)	✔		Portability of an end user’s data or data generated through the core platform service.
6(10)	✔		Access to a business user’s data or data generated through the core platform service.
6(11)	✔		Fair, reasonable, and nondiscriminatory (“FRAND”) access to ranking, query, click, and view data related to free and paid search generated by end users on a gatekeeper’s online search engine.
6(12)	✔		FRAND general conditions for business users to access software app stores, online search engines, and online social network services.
6(13)	⊗		Disproportionate conditions when users want to terminate the provision of a core platform service (e.g., in terms of notice period, reasons for termination, or fees).
7	✔		Interoperation of instant messaging, including text messages and sharing of images, voice messages, videos, and other attached files.

This final version of the DMA contains a number of revisions to the obligations as compared to the [initial proposal](#). The final DMA:

- Prohibits all parity (MFN) clauses, whether wide or narrow. “Wide” clauses prevent a supplier from offering better terms on other intermediation services, while “narrow” clauses prohibit only better offers on the supplier’s own online sales channel.
- Grants users the right to unsubscribe from core platform services.
- Extends FRAND access obligations that initially covered only app stores to also cover social media networks and search engines.
- Requires a gatekeepers that sell devices to offer users a choice screen before installing web browsers, virtual assistants, or search engines.

- Obligates a gatekeeper that operates messaging services to provide third-party messaging services the option of interoperating with the gatekeeper’s services. The DMA also applies this obligation to group chat and voice and video call services over four years.
- Requires that a gatekeeper establish an internal and independent “compliance function” comprising one or more compliance officers to monitor DMA compliance.

A number of the obligations, such as interoperability obligations, will be complex and costly to implement. Moreover, they raise many technical and practical questions, perhaps most significantly around data privacy and cybersecurity. Likewise, gatekeeper plans for DMA compliance must be considered in light of other EC rules such as the General Data Protection Regulation (“GDPR”), the proposed Data Act (See our February 2022 *Alert*, “[European Commission Proposes Legislation Facilitating Data Access and Sharing](#)”), and telecom regulations, among others, that will affect DMA obligations related to data portability, for example.

HOW IS THE DMA DIFFERENT FROM THE COMPETITION LAWS?

Most of the obligations included in the DMA stem from antitrust case law at both EU and national levels. Therefore, both the DMA and the antitrust laws potentially could apply in parallel, and the DMA states that it does not prevent the application of EU and national antitrust law. The EC also has made clear that it does not see the parallel application of the DMA and antitrust law as a violation of the *non bis in idem* principle set forth in the Court of Justice’s decision in *C-117/20 BPost*, which held that it was permissible for the EC to apply telecom and antitrust regulations in parallel to the same conduct. However, the EC’s views nevertheless may be challenged in the European courts, depending on the specific circumstances of the case. In the near term, to the extent it has a choice, we expect that the EC will favor application of the DMA over antitrust both because the DMA places fewer legal burdens on the EC and because it will want to develop its authority in this area.

In the area of merger control, the DMA introduces an obligation for designated gatekeepers to pre-report to the EC transactions in which the merging entities or the target provides core platform services or any other digital service or enables the collection of data, even if the transaction does not satisfy the EU merger filing thresholds. That requirement is consistent with the [EC’s new approach to Article 22 of the EU Merger Regulation](#), in which national competition authorities can refer, for EC antitrust review, acquisitions involving companies that do not meet the EU or national filing thresholds if the acquisition target might be competitively significant in the future. Under the DMA, the EC will obtain information on gatekeepers’ intended transactions and share that information with Member States, so that they, in turn, can request that the EC conduct an antitrust review of gatekeepers’ mergers and acquisitions.

WHO WILL ENFORCE THE DMA, AND WHAT ARE THE PENALTIES FOR VIOLATIONS?

The DMA designates the EC as the sole enforcer of the new law. National authorities may initiate investigations against gatekeepers, in coordination with the EC, which makes enforcement decisions. However, the DMA is not likely to displace the role of national competition authorities in antitrust challenges to gatekeeper conduct as national authorities may still apply national competition law to the conduct of gatekeepers. For example, certain Member States have rules related to “abuse of economic dependence” that some national authorities have attempted to apply to so-called “lock-in effects” in B2B transactions.⁴ Likewise, although it is potentially redundant with the DMA, in

January 2021, [Germany adopted special competition rules](#) for certain digital platforms across multiple markets. The DMA established an advisory group composed of national regulators (including telecommunications, data protection, competition, consumer protection, and audiovisual) to assist and facilitate the work of the EC.

The EC may assess fines for DMA violations up to 10% of the infringer’s worldwide revenue, or up to 20% for a repeated infringement, which is twice the fine for EU antitrust law violations. In the case of repeated violations—i.e., at least three violations in eight years—the EC can impose behavioral or

structural remedies, including a temporary ban on certain types of acquisitions or even the breaking up of a gatekeeper. All EC decisions can be appealed before the Court of Justice.

The DMA is a regulation directly applicable in EU Member States and thus entails a risk of private enforcement, in which business and individual plaintiffs may seek remedies under the DMA before national courts in damages or injunction proceedings. Class action suits based on DMA violations also can be expected, as the DMA is included in the scope of the [EU Collective Action Directive](#).

CONCLUSION

In the wake of the DMA publication in October 2022, businesses with core platform service operations should assess whether they qualify as gatekeepers under the thresholds, and consider the need to notify their gatekeeper status to the EC. The list of gatekeeper obligations is long, and it may not be clear whether the DMA captures certain business practices. Companies at risk of a gatekeeper designation should evaluate their compliance with the obligations and may consider anticipating the regulatory dialogue with the EC to further ascertain practical implementation of the obligations.

To monitor the DMA implementation, gatekeepers should establish independent internal compliance teams, whose expertise ideally should span across competition, privacy, and potentially telecom or media rules. Besides gatekeepers, all companies supplying or using core platform services should consider the risks and opportunities that the DMA generates, for example in terms of interoperability and access to data.

ENDNOTES

1. The DMA builds on the 2019 Regulation on platform-to-business relations (“P2B Regulation”), which established transparency obligations for online intermediation services and online search engines provided to business users. Some have argued that those regulations were insufficient to ensure fair and contestable digital markets and control the allegedly anticompetitive conduct of large online platforms, hence the need for the DMA.
2. See [Proposal for a DMA](#).
3. See, e.g., Makan Delrahim, Assistant Attorney General, U.S. Dep’t of Justice, Antitrust Div., [Keynote Address at Silicon Flatirons Annual Technology Policy Conference at The University of Colorado Law School](#) (Feb. 11, 2019).
4. Rules against “abuse of economic dependence” prohibit one party with superior economic strength from engaging in anticompetitive conduct against a counterparty with a relatively inferior bargaining position. The “lock-in” effect is a disputed argument that a purchaser of a primary product or service has no alternative but to continue purchase products or services (e.g., in an aftermarket) from the same supplier or its designee.



EU EXTENDS TRAVEL RULE TO CRYPTO-ASSETS

JULY 2022 ALERT

On June 29, 2022, the European Parliament, the Commission, and the Council reached a provisional agreement on the European Union proposal to update Regulation 2015/847 on information accompanying the transfer of funds (“TFR”) by extending its scope to transfers of crypto-assets. The final text is to be published.

Presented as part of the future European AML/CFT legislative package, the revised TFR aims to regulate the transfer of crypto-assets to avoid illicit flows and consists of an adaptation of the existing TFR rules currently applying to cash transfers only.

This regulation should be read in light of the forthcoming Markets in Crypto-Assets Regulation with respect to certain definitions which also will apply to these new rules.

Under the future TFR regime, the crypto-asset service provider (“CASP”) of the party initiating the transfer will have to ensure that the transfer includes information on both the initiator and the beneficiary. The thresholds (from the first euro or from 1,000 euros) will apply depending on whether the transfers occur between CASPs, between CASPs and unhosted wallets, or between unhosted wallets.

The beneficiary’s CASP then will have to check whether the required information is included in the transferring message prior to executing the transfer.

One of the main challenges with the application of this “travel rule” relates to unhosted wallets, which are crypto-asset wallet addresses held directly by their owners without using a CASP. Although affected parties may have difficulty complying with the technical requirements of the rule, no exemption has been provided for exclusions to its application, raising concerns in the crypto-asset space. One may expect some refinement in the final text to take into account the specificities of crypto-assets without detracting from the objective of increased transparency.

Another issue relates to the protection of personal data as it is not envisaged to provide for specific rules of the EU General Data Protection Regulation to apply to information “travelling” under the TFR. This will therefore also need to be addressed by specific legislation.



AUSTRALIAN FINANCIAL SERVICES REGULATORY UPDATE

JUNE 2022 NEWSLETTER

August 2022

This August 2022 edition of the *Update* covers:

- Recent legal and regulatory developments, including the commencement of cyber security incident notification obligations for critical financial market infrastructure assets, AUSTRAC's guidance on ransomware and criminal use of digital currencies, ASIC's guidance on the risk of greenwashing by superannuation and managed funds, and APRA's risk management expectations and policy roadmap for crypto-assets;
- Recent financial services litigation, including ASIC's successful appeal against short-term lenders BHF Solutions Pty Ltd and Cigno Pty Ltd, and the commencement of proceedings by ASIC against Macquarie Bank Ltd for allegedly failing to adequately monitor and control transactions by third parties; and
- Other regulatory enforcement action, including a court enforceable undertaking offered by NAB and accepted by AUSTRAC to address concerns with NAB's compliance with the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).
- Recent financial services litigation, including the imposition of a \$30 million penalty on the Mayfair 101 Group for misleading investors through its advertising, a \$20 million penalty on Colonial First State Investments Limited for misleading superannuation members through a communications campaign, the agreement reached between ASIC and Westpac on six regulatory matters and the commencement of proceedings by AUSTRAC against Crown Melbourne and Crown Perth; and
- Other regulatory enforcement actions, including a \$110,250 infringement notice issued by the ASIC Markets Disciplinary Panel to BGC Partners (Australia) Pty Ltd, an investment broker, for noncompliance with the ASIC Market Integrity Rules (Futures Markets) 2017.

READ THE ISSUE

June 2022

This June 2022 edition of the *Update* covers:

- Recent legal and regulatory developments, including the release of regulatory guidance on crypto asset-related investment products, the imposition of additional licence conditions on the ASX following the market outage, ASIC's report on the cyber resilience of financial markets firms, the adoption of Magnitsky-style targeted sanctions in Australia and ASIC's surveillance of investment switching by super fund executives;
- Recent financial services litigation; and
- Other regulatory enforcement action, including a total of \$1.86 billion in remediation paid or offered by six of Australia's financial services institutions in relation to financial advice misconduct since 2016 and the closure of a criminal investigation into AMP Financial Planning Pty Limited for fees for no service.

READ THE ISSUE

July 2021

This July 2021 edition of the *Update* covers:

- Recent legal and regulatory developments, including Australian regulatory expectations regarding the LIBOR transition, AUSTRAC's issuance of new rules to reflect the recent AML/CTF reforms and the passing of the 'Your Future, Your Super' package of reforms;
- The continuing fallout of the Financial Services Royal Commission and the recent cases demonstrating ASIC and APRA's continuing commitment to enforcement action in relation to matters referred by the Commissioner; and
- Other regulatory enforcement action, including investigations recently commenced by AUSTRAC's Enforcement Team and criminal charges laid against a retail bank for false and misleading conduct.

READ THE ISSUE**May 2021**

This May 2021 edition of the *Update* covers:

- Recent legal and regulatory developments, including the release of ASIC's immunity policy for market misconduct offences, a FATF consultation on proliferation of financial risk and digital currency, and ASIC and APRA's focus on the management of cyber risk and climate risk;
- A recent decision of the Full Court of the Federal Court of Australia upholding an order compelling compliance with a s 33 notice by an authorised representative of an AFS licensee;
- The continuing fallout of the Financial Services Royal Commission and the recent cases demonstrating ASIC and APRA's continuing commitment to enforcement action in relation to matters referred by the Commissioner; and
- Other regulatory enforcement action, including the Federal Court finding that the Mayfair 101 Group made misleading or deceptive statements in its advertisements and the imposition of AFS licence conditions on a retail OTC derivatives issuer.

READ THE ISSUE**February 2021**

This February 2021 edition of the *Update* covers:

- Recent legal and regulatory developments, including the release of APRA's policy and supervision priorities for 2021, the launch of APRA's Cyber Security Strategy 2020 – 2024, Australian regulatory support for the ISDA IBOR Fallbacks Protocol and Supplement, and Australia's renewed focus on sanctions;
- Two recent Federal Court decisions which support ASIC's position on obligations to comply with ASIC notices and to substantiate any claims for legal professional privilege;
- The continuing fallout of the Financial Services Royal Commission and the recent cases which demonstrate that ASIC and APRA appear to remain committed to taking enforcement action in relation to matters referred by the Commissioner;
- The recent AUSTRAC enforcement action, including Beach J's consent order imposing a \$1.3 billion on Westpac last year and, in contrast, an infringement notice issued by AUSTRAC to State Street for a penalty of \$1.25 million; and
- Other regulatory enforcement action, including the imposition of a \$75 million penalty on OTC derivative issuers.

READ THE ISSUE**September 2020**

This September 2020 edition of the *Update* covers:

- Recent legal and regulatory developments which relate to licencing and regulatory relief, consumer protection, financial markets, anti-money laundering and capital and prudential requirements for authorised deposit-taking institutions ("ADIs");
- The recent decision of Federal Court in *Australian Securities and Investments Commission v Hutchison* [2020] FCA 978, which affirmed that the phrase "in relation to" a financial service is to be construed widely;
- The continuing fallout of the Financial Services Royal Commission and the recent cases which demonstrate that ASIC and APRA remain committed to taking enforcement action in relation to matters referred by the Commissioner; and
- The latest regulatory enforcement action, including the first criminal conviction for failing to comply with client money obligations.

READ THE ISSUE



BREAKTHROUGH IN ITALIAN CRYPTOCURRENCY REGULATION: STATUTORY REGISTRATION FOR PROVIDERS AND EXCHANGERS

MARCH 2022 ALERT

The Italian Ministry of Economy and Finance (“MEF”) issued a new decree (“Decree”) requiring that virtual asset/currency service providers promptly enroll in a soon-to-be established special section of the register held by Organismo Agenti e Mediatori (“OAM”), with the aim of monitoring cryptocurrency exchanges and implementing anti-money laundering controls.

For quite some time, both national and international authorities have kept an increasingly close eye on cryptocurrency markets, although with limited intervention powers. On April 28, 2021, the Bank of Italy and the Italian Securities and Exchange Commission (“Consob”) issued a joint statement calling upon the public and small savers to beware of the risks embedded in “crypto-activities.” Consob also issued tailor-made sanctions when it found that certain services qualified as Markets in Financial Instruments Directive (“MiFID”) services were provided without the required authorizations and licences by using its general surveillance powers.

The Decree sets clear(er) requirements for the provision of any virtual currency/digital assets services in Italy by introducing administrative sanctions in case of violation of the applicable regulation.

Pursuant to the Decree, the special section shall become operational by May 18, 2022 with a 60-day grandfathering period for operators already active in Italy. From that date onwards, any provider of cryptocurrency exchange, crypto trading, digital wallet and, widely, any virtual currency related services (“Providers”) must enroll in the special section to carry out business in Italy and, as a result, implement ad hoc policies and procedures to ensure compliance with the new Italian legal framework. Any failure to enroll will result in administrative sanctions and the exercise of any such services will be unlawful.

The Decree also establishes: (i) periodical disclosure obligations upon (a) the Providers towards the OAM (with respect to clients and transactions carried out in Italy) and (b) the OAM towards MEF; and (ii) cooperation undertakings between OAM and the other authorities, e.g., AML, Bank of Italy, and Consob.

A number of jurisdictions have implemented the Financial Action Task Force (“FATF”) recommendations on virtual asset service providers, including the United Kingdom, Spain, France, Ireland, and the Netherlands, to name a few. It is likely that the impact of these new proposals in Italy will follow the pattern seen elsewhere, with a number of current providers leaving the market but others taking advantage of the opportunities created by this new regime.



CAPITAL RELIEF FOR SOFTWARE ASSETS: EUROPEAN COMMISSION AMENDS OWN FUND REQUIREMENTS

JANUARY 2021 COMMENTARY

IN SHORT

The Development: New Regulation (EU) 2020/2176 (the “Regulation”) provides regulatory capital relief, allowing certain software assets to be considered when calculating Common Equity Tier 1 (“CET1”) capital. It entered into force on December 23, 2020, and the new deduction method is applicable since December 31, 2020.

The Significance: In view of the increasing digitalization in the banking sector and to encourage IT investments, prudently valued software assets that will not be materially affected in resolution, insolvency or liquidation, will no longer be deducted from CET1.

Looking Ahead: The Regulation aims to provide relief for institutions hit by the COVID-19 pandemic and to accelerate investments in technology. Financial institutions may benefit from capital relief and should determine their qualifying software assets to update their capital planning.

DIGITALIZATION AND LEGISLATIVE INTENT

Regulation (EU) 575/2013 on prudential requirements for credit institutions and investment firms (“CRR”) was amended by Regulation (EU) 876/2019 (“CRR2”), including the capital treatment of software assets, which to date had to be deducted from regulatory capital when they were accounted for as intangible assets (article 36.1 (b)). The rationale had been that “software assets are usually tailor-made and cannot be easily sold on the market as stand-alone assets if needed (i.e. to absorb losses on an ongoing concern if losses arise).”

In connection with the revision of CRR, the EU legislator focused on supporting digitalization and encouraging IT investments in the banking sector. Now, certain prudently valued software assets should no longer be deducted from

CET1. Accordingly, CRR2 amended article 36.1(b) of CRR to exclude from the deduction mechanism “prudently valued software assets the value of which is not negatively affected by resolution, insolvency or liquidation of the institution.” A delegated regulation had to be adopted detailing the conditions of this new regime.

COHERENT SUPERVISORY STANDARDS

As observed in the EBA’s Final Report (EBA/RTS/2020/07), assessing the recoverable value of intangible assets is complex due to the multitude of different software applications in use by institutions. The economic value of these assets needs to be weighed against supervisory considerations and balanced accordingly. This called for a simplified approach to the prudential treatment of software assets,

preventing operational obstacles for institutions and to facilitate coherent supervision by the authorities. Consequently, the Regulation amends Delegated Regulation (EU) No. 241/2014, which lays down technical standards regarding own funds, and establishes a new regime for the deductibility of software assets from CET 1 items.

REGULATORY TECHNICAL STANDARDS

The key provision in the Regulation setting out the new deduction method for software assets is Art. 13(a), which is added to Delegated Regulation (EU) 241/2014. According to this provision, prudently valued software assets may be exempt from CET1 deduction if their valuation is not negatively affected by resolution, insolvency or liquidation of the institution. Interestingly, no particular definition is provided for “prudently valued software assets,” either in CRR2 or in this provision.

The new provision introduces a day-by-day regulatory amortization of software assets over a three year period. The amount to be deducted for each software asset is the difference between the accumulated amortization under prudential versus applicable accounting standards. The prudential amortization is calculated starting from the date on which the software asset is available for use and accordingly is then amortized under accounting standards. The remaining balance of the software asset carrying amount is risk-weighted at 100% (i.e. fully deducted). Investments in maintenance and upgrades of existing software assets are to be considered as other assets, provided that they are recognized as intangible assets under applicable accounting standards.

EARLY ENTRY INTO FORCE DUE TO CRR QUICK FIX

The CRR Quick Fix (Regulation (EU) 2020/873) accelerated the entry into force of this capital relief measure in light of the COVID-19 pandemic. Hence, the Regulation entered into force on December 23, 2020, and the new deduction method is applicable since December 31, 2020.

THREE KEY TAKEAWAYS

1. The Regulation introduces a day-by-day regulatory amortization of software assets over three years. Especially for the Fintech sector subject to capital requirements under CRR, like payment service institutions or electronic money issuers notably with significant software assets, this can materially increase their regulatory capital base.
2. The Regulation does not prevent institutions from fully deducting their software assets from CET1 items, nor does it hinder authorities to scrutinize software assets and exercise supervisory powers where there is a concern of undesired prudential benefits resulting from significant investments in software.
3. The Regulation entered into force on December 23, 2020, and the new deduction method is applicable since December 31, 2020.



DECEMBER 2020 COMMENTARY

IN SHORT

The Situation: The European Union and United Kingdom have both warned companies to prepare for a no-deal Brexit.

The Result: There is a real possibility that the Brexit Implementation Period will end on 31 December 2020 without a trade deal between the United Kingdom and European Union.

Looking Ahead: Companies sending personal data from the European Economic Area (“EEA”) to the United Kingdom must put in place arrangements to comply with the EU data transfer rules as a matter of urgency.

THE EU DATA TRANSFER RULES

From 1 January 2021, the United Kingdom will be a “third country” for the purposes of the EU General Data Protection Regulation (“GDPR”), and companies in the EEA may transfer personal data to the United Kingdom only by using an approved data transfer mechanism (such as the EU Standard Contractual Clauses (“SCC”) or Binding Corporate Rules (“BCR”)) or where one of the GDPR exceptions applies. The exceptions are unlikely to apply to regular data transfers.

In time, it is possible that the EU Commission will grant the United Kingdom an “adequacy decision” (establishing that the United Kingdom’s data protection regime is “essentially equivalent” to that of the European Union). This would allow transfers without additional measures being taken. The UK Government’s position is to maintain a close alignment with EU data protection laws and to seek such a decision. However, this will take time and is by no means certain.

For the moment, there is no equivalent issue for data transfers from the United Kingdom to the EEA. The United Kingdom has issued guidance stating that, given the alignment of the United Kingdom and the EU data protection rules, UK companies will continue to be able to send personal data to the European Union after 31 December 2020. This position will be kept under review.

In addition, data transfers from non-EEA countries to the United Kingdom will need to comply with the data protection rules of those countries. Where a country has an existing EU adequacy decision (such as, for example, Canada, Japan, or Switzerland), it is likely to have rules restricting data transfers to third countries (which will, after 31 December 2020, include the United Kingdom). The position for specific country transfers should be checked.

REQUIRED STEPS

Anyone making regular transfers of personal data from the EEA to the United Kingdom should implement a legal transfer mechanism by 31 December 2020. Those using SCCs should also bear in mind the impact of the recent *Schrems II* decision and the upcoming SCCs which are currently expected to be adopted in early 2021 (see our *Commentary*, “[Ensuring International Data Flows After Schrems II](#)”).

In addition, the GDPR applies to non-EU based companies that sell to or monitor individuals in the European Union. From 1 January 2021, UK companies carrying out such selling or monitoring must appoint an EU representative unless their processing is occasional, does not include, on a large scale, special categories of personal data (such as health data) and is low risk.

The United Kingdom has equivalent provisions for non-UK companies, which from 1 January 2021 will apply to EU companies that sell to or monitor individuals in the United Kingdom.

Companies should assess if either requirement applies to them and appoint any necessary representatives. They should also update their GDPR notices to data subjects to reflect the post-Brexit situation. This means transfers to the United Kingdom need to be referred to as third-country transfers, including a reference to the safeguards used (such as SCC or BCR) and where those can be obtained. The records of processing activities should also be updated to reflect the data transfer mechanisms in place for transfers to the United Kingdom.

Finally, companies should address these issues with their key suppliers in the European Union and in other countries with transfer restrictions applicable to the United Kingdom as a third country in order to avoid critical interruptions in the supply of goods and services.

FOUR KEY TAKEAWAYS

1. If there is no deal in place between the European Union and the United Kingdom before 31 December 2020, companies need to put in place a transfer mechanism to deal with any transfers of personal data from the EEA to the United Kingdom after 31 December 2020.
2. Companies should consider if they need to appoint a representative in the European Union or United Kingdom under the applicable data protection rules.
3. Companies need to update their notices to data subjects to reflect the post-Brexit situation, and update their records of processing activities.
4. Companies will need to ensure that their key suppliers have taken similar steps in order to avoid critical interruptions in the supply of goods and services.



BOOSTING BLOCKCHAIN: GERMANY TO INTRODUCE ELECTRONIC SECURITIES

AUGUST 2020 COMMENTARY

IN SHORT

The Situation: The requirement for a paper-based note for issuing securities under the German law has been an obstacle for the use of security tokens in Germany. With the release of a draft bill (the “Bill”) permitting the issuance of electronic bearer bonds under German law, Germany is paving the way for digitalizing its financial markets.

The Result: The Bill now proposes to remove the global note requirement. It sets out a legal framework for the issuance of electronic bearer bonds including those issued as security tokens on a blockchain. The Bill is another milestone in the provision of legal certainty for blockchain-based securities in Germany after the introduction of the crypto custody license as of January 1, 2020.

Looking Ahead: The Bill will provide legal certainty to issuers and institutional investors and boost the use of distributed ledger technology (“DLT”) for the issuance of blockchain-based security tokens under German law. Permitting the exchange of existing traditional securities into electronic securities (“e-Securities”) (and *vice versa*) and the consolidation of both types of securities will open up the market for institutional investors. This legislation comes ahead of an expected EU-wide legislative initiative on crypto assets toward the end of 2020.

BACKGROUND

Under German civil law, the issuance of a bearer bond requires a paper-based document with a wet ink signature (with the exception of certain government bonds). Even though a security issued as a paper-based (global) note can be transferred electronically through the securities settlement system, the requirement of a paper-based (global) note presents a major practical restriction on issuing German law securities in token form on a blockchain. Accordingly, security tokens under German law have, to

date, taken the form of a subordinated participation right which is not subject to a paper note requirement.

SCOPE

The Bill permits the issuance of securities in electronic form. For the time being, these e-Securities are limited to bearer bonds, but the Bill is designed to permit other forms of securities, such as shares or fund units, to be issued in electronic form going forward.

THE REGISTERS

The Bill provides that for e-Securities the requirement of a paper-based note is replaced by the entry of the e-Securities into a register operated by a supervised entity. The register may be a central register that must be operated by a central securities depository (“CSD”) under a CSD license. Alternatively, the register may also be a decentralized register, a so-called crypto security register (*Kryptowertpapierregister*), in order to permit the issuance of blockchain-based e-Securities as security tokens, which the Bill refers to as crypto securities and treats as a sub-category of e-Securities. The crypto security register may be operated by the issuer or a third-party registrar appointed by the issuer. The crypto registrar will be subject to regulatory supervision by the Federal Financial Supervisory Authority, or BaFin, and will require a license for the provision of crypto security registration services (*Kryptowertpapierregisterführung*) with an initial capital requirement of EUR 730,000. That license is to be distinguished from the license for the provision of custody services for crypto assets (*Kryptowerte*) for others (including the custody of private keys for crypto assets and crypto securities). That is a separate license that only requires a capital of EUR 125,000.

TERMS AND CONDITIONS AND TRANSFERS

The terms and conditions of e-Securities (and any amendment thereto) must be submitted to the registrar in electronic form. The issuance of e-Securities must also be published in the official gazette in Germany, the *Bundesanzeiger*. Transfers will be effected by an agreement between the buyer and the seller and an instruction by the buyer to the registrar to register the buyer as the new holder of the e-Securities.

CONSOLIDATION WITH TRADITIONAL SECURITIES

The Bill also provides for an exchange and consolidation mechanism that will help kick-start the market for e-Securities. Issuers may exchange their existing securities into e-Securities and vice versa, and both can be consolidated into a single series. e-Securities can also be registered in the name of a CSD and can then be cleared and settled under the existing systems. For regulatory purposes, including the Markets in Financial Instruments Directive (“MiFID”) and prospectus requirements, they are treated the same way as traditional securities. The exchange and consolidation mechanism and the regulatory treatment in line with traditional securities will facilitate the generation of a meaningful volume and liquidity of securities needed for a functioning market and make it attractive for both, issuers and (institutional) investors.

THREE KEY TAKEAWAYS

1. While to date, security tokens have been issued in the form of participation rights, the Bill proposes a new framework to provide legal certainty for issuing bearer bonds in electronic format, removing the requirement for a (global) note in paper form. These e-Securities may also be issued as security tokens on a blockchain as crypto securities. For regulatory purposes (including MiFID and prospectus requirements), e-Securities (including crypto securities) are treated the same way as traditional securities.
2. Issuance will be by way of registration of the e-Securities in a register that can (i) either be a central register operated by a regulated CSD or (ii) in order to permit blockchain-based crypto securities, a decentralized register operated by the issuer or a third-party registrar appointed by the issuer. The operation of a decentralized register will require a license from the German regulator.
3. Under the proposed framework, traditional securities can be exchanged for e-Securities and vice versa. e-Securities can also be consolidated with traditional securities of the same series. This will help to generate significant volume and liquidity of e-Securities which is required to kick-start the market for e-Securities (including crypto securities) and attract institutional investors.



FACILITATING TRANSATLANTIC FINTECH INNOVATION AND COOPERATION: THE NEW MOU BETWEEN THE NYDFS AND THE FRENCH ACPR

JUNE 2020 COMMENTARY

The Situation: From both sides of the Atlantic, United States and French financial authorities are keen to facilitate technology innovations in the financial sector. Beyond having set up dedicated teams to focus on the development of new financial technology (“fintech”), the New York State Department of Financial Services (“NYDFS”), and the Autorité de contrôle prudentiel et de résolution (“ACPR”) are improving international cooperation in support of financial innovation.

The Result: On June 3, 2020, the NYDFS and the ACPR executed a non-binding memorandum of understanding (“MOU”) aimed at encouraging and enabling the development of innovative financial services in the New York and French markets. The NYDFS is the first U.S. financial services regulator to sign an MOU with the ACPR.

Looking Ahead: Any person from France or from New York State who wishes to create or expand fintech activities in the other jurisdiction will benefit from a referral mechanism and the same level of support and information when contacting the authority based in the other jurisdiction, thereby promoting France and New York as innovation hubs for financial services technology.

BACKGROUND

Both the ACPR and NYDFS have established programs or departments that specialize in the implementation of technology in the financial services sector. These departments are the preferred points of contact for innovators that face legal or regulatory challenges in ensuring compliance with licensing or other rules applicable to their businesses in developing financial products and services. Through the new MOU, the French and New York authorities have established an environment and contacts that facilitate the use of innovative financial technology between France and New York.

SCOPE OF COOPERATION

Cooperation under the new MOU will consist of establishing a referral mechanism, sharing information and supporting financial technology innovators:

- **Referrals and Interaction:** Any fintech innovator will be able to contact the authority in its own jurisdiction, which will contact the other authority. Based on the information passed on by the referring authority, the other authority will interact with the innovator as if it were a person residing or incorporated within its jurisdiction.
- **Information sharing:** The authorities will share general information, market trends, and information on policy and

supervision issues. Dialogue between the two authorities will be conducted regularly through conference calls, meetings, or conferences.

- **Equivalent support:** Each authority will offer equivalent support to French or U.S. innovators, in providing information and assistance to applicants to facilitate their registration or licensing, if required, with relevant people knowledgeable in the fintech area.

To help financial technology innovators bring products and services to market, the MOU does not preclude the option for innovators to contact the foreign authority directly, or through its national authority.

CONFIDENTIALITY

The two authorities have agreed to share information relating to an innovator only with the prior written consent of the other authority and have confirmed their respective duties of confidentiality.

Each authority agreed to use the information disclosed pursuant to the MOU exclusively for regulatory and supervisory responsibilities, and in accordance with the purpose of the MOU. Any other use of the information shall be subject to the prior written consent from the authority that shared the information.

THREE KEY TAKEAWAYS

1. The new MOU should promote new and expanded transatlantic financial services technology innovations by supporting cooperation between the French and New York State authorities.
2. The new MOU should ensure that financial services innovators will be treated fairly and with the same level of support as national innovators.
3. Financial services technology innovators may expect a better convergence of supervision and regulation applied to fintech-based activities between France and New York State due to the new MOU.



CHINA ACCELERATES BLOCKCHAIN ADOPTION IN THE NEW DECADE

JANUARY 2020 COMMENTARY

IN SHORT

The Situation: Authorities in China have cracked down on privately developed cryptocurrency, yet have heavily invested in and encouraged the development of other blockchain applications and services.

The Result: The rapidly rising number of blockchain projects in China is accompanied by increased regulation, including a requirement that blockchain-related projects be registered with the Cyberspace Administration of China.

Looking Ahead: As China's central bank continues to develop a government-backed digital currency, there will likely be no lifting of the crackdown on other types of cryptocurrency in China. However, blockchain technology will continue to expand, and foreign companies doing business in China should closely monitor related legal developments.

CRACKING DOWN ON CRYPTOCURRENCY

It was said that China is controlling around 70% of the cryptocurrency mining operations around the world. Since 2014, the People's Bank of China has been working on developing a fully backed digital fiat currency, and is expected to become the first national central bank in the world to launch an official currency in digital form. In the lead-up to its introduction, Chinese financial regulators have cracked down on other cryptocurrency-related firms and activities. As early as 2013, China's central bank and other authorities jointly issued the *Notice on Prevention of Risks imposed by Bitcoins* to prohibit financial institutions from transacting bitcoins, denominating products and services in bitcoins, or providing bitcoin-related services. These restrictions were expanded in September 2017 when Chinese authorities published the *Announcement Preventing the Financing*

Risks of Initial Coin Offerings ("Announcement"), essentially banning initial coin offerings ("ICOs") and ICO-related financing activities (an ICO is the introduction of a new cryptocurrency in order to raise capital, similar to an initial public offering of stock).

The Announcement declared ICO financing to be an unauthorized illegal public financing, akin to the illegal issuance of securities or even financial fraud. It further required authorities to close down trading platforms that provide an exchange service between legal tender and cryptocurrency and other services related to cryptocurrency, such as pricing and intermediary services, and prohibited financial institutions and payment institutions from providing these services. The Announcement has led to a nationwide crackdown of cryptocurrency, including bitcoin.

In late 2019, Chinese President Xi Jinping declared his support and encouragement of the development of blockchain technology in China. With blockchain being the key technology behind cryptocurrency and cryptoassets, many investors and entrepreneurs mistakenly interpreted this endorsement as an endorsement of privately developed cryptocurrency as well, temporarily reigniting China's cryptocurrency sector and crypto trading activities. Chinese authorities put a swift end to this, however, closing down all platforms that traded or provided services related to foreign cryptocurrency, including five China-based cryptocurrency exchanges that allow cryptocurrency to cryptocurrency exchange transactions.

BLOCKCHAIN TECHNOLOGY IN PUBLIC AND PRIVATE SECTORS

Despite this strict crackdown on privately developed cryptocurrency, blockchain technology is gaining rapid acceptance in China. In cracking down on cryptocurrency applications, the Chinese government has emphasized the distinction it sees between cryptocurrency and blockchain users. Users are warned not to conflate the two and reminded that the development of blockchain applications, as opposed to cryptocurrency, is widely encouraged. Organizations using blockchain technology in China or on a global basis should pay close attention to the distinction and seek detailed legal and regulatory advice where necessary.

There has been an explosion of blockchain-based solutions in the public and private sectors. One major project launched by the Chinese government is the blockchain-based cross-border financing platform implemented by the State Administration of Foreign Exchange ("SAFE") in March 2019. Similar to the Greater Bay Area Trade Finance Blockchain Platform, which was launched in 2018, the platform facilitates receivables financing and information verification for cross-border businesses and is now used by commercial banks and SAFE bureaus in 19 provinces and cities across China.

Other Chinese governmental projects include a smart contract application introduced by the Hangzhou Internet Court that assists the automation of contract execution and smart adjudication of cases, an identification platform in Shenzhen that automates identity verification of users of government services, and a logistic platform introduced by the Customs of Tianjin Province that facilitates cross-border transactions and payment.

Experts predict that blockchain has the potential to be applied in China in fields such as anticorruption, public security, public transportation, and crime investigation, and of course, as the backbone of the central bank's digital

currency in the near future. Many companies are also exploring the use of blockchain technology in the private sector, some with financial investment from local technology giants. Such applications range from product certification and verification, to invoicing and e-billing system, recording of intellectual property rights, and tracing and tracking of drug identity in pharmaceutical supply chains.

As blockchain applications grow in popularity, the performance of blockchain companies performance has taken on greater significance in the broader Chinese financial markets. In Shenzhen, an exchange-traded fund ("ETF") based on the performance of publicly listed blockchain companies was recently proposed. While this proposal is pending the China Securities Regulatory Commission's approval, the Shenzhen Stock Exchange launched in December 2019 a blockchain index reflecting the performance of the top companies with blockchain ventures. These developments signal new opportunities in the stock exchange, as well as optimism in the continued growth of the blockchain industry.

In the Catalogue for Guiding Industry Restructuring, which was issued by China's National Development and Reform Commission in October 2019 and took effect on the first day of 2020, blockchain information services approved by the Chinese government is labelled as encouraged industry.

REGULATIONS

With the expansion of blockchain activities naturally comes the expansion of the corresponding rules and regulations. The *Provisions on the Administration of Blockchain Information Services* ("Provisions") implemented by the Cyberspace Administration of China ("CAC"), a governmental agency that regulates, oversees, and controls the internet of China, specifically governs issues relating to blockchain and blockchain information services. For example, the Provisions grant the CAC the power to supervise and regulate all blockchain information services in China.

Companies seeking to provide blockchain information services in China, including websites or applications that utilize blockchain technology to provide information to the public, must register with CAC their blockchain information services, as well as any subsequent modifications to the services. Additionally, identity verification is required of all users, and service providers must not provide services to a user who refuses to comply with this requirement. Service providers must also retain records of contents, logs, and other information for at least six months and make them available to law enforcement upon request. The Provisions apply to both local and foreign companies that seek to provide blockchain information services in China.

Another new regulation that may be relevant to those looking to establish blockchain-related services in China is the new *Encryption Law of the People's Republic of China* ("Encryption Law"), which went into effect at the turn of this year. The law requires encryption products to adhere to technical and security standards to be set by the relevant Chinese regulatory authorities. As encryption is a core component underpinning cryptocurrency and blockchain, service providers and developers should adhere to the rules under the Encryption Law. Maintaining encryption standards is critical to the long-term success of blockchain technology as advances in quantum computing threaten to make existing encryption technology less secure. Encryption products with protection functionality relating to national security or the public interest are additionally subject to import licensing and export controls.

THREE KEY TAKEAWAYS

1. Chinese authorities have cracked down on firms involved in cryptocurrency and related activities.
2. Chinese authorities are encouraging the development of other blockchain applications, and there has been heavy investment in the industry from both the public and private sector.
3. Developers and providers of blockchain services must closely monitor Chinese legal developments relating to blockchain services.

CHAPTER VII
AI AND NFTs

The background of the page is a solid dark teal color. Overlaid on this are several large, overlapping, semi-transparent geometric shapes in various shades of blue and teal. These shapes include rectangles and chevrons, some pointing right and some pointing left, creating a layered, architectural effect. The shapes are arranged in a way that they appear to recede into the distance, with some being more prominent than others.



WHICH AI COMPONENTS ARE COPYRIGHT PROTECTABLE AND WHICH ARE NOT?

MARCH 2022 COMMENTARY

IN SHORT

The Situation: The growing ability of artificial intelligence (“AI”) systems to generate outputs of various kinds with little or no human contribution presents fundamental questions for copyright law, which has traditionally been built around the protection of human ingenuity and creativity.

The Background: AI involves technology that does not simply process data at the request of human operators, but which is able to learn from that data in order to make effective decisions and judgments autonomously. With the rapid increase in complexity of tasks AI can master, the protectability of its outputs is of increasing commercial significance.

Looking Ahead: Although further developments are anticipated, courts worldwide remain hesitant (and in some cases firmly opposed) to embracing AI as an “author” in its own right. Given this, it is especially important for businesses in this space to protect the underlying software, algorithms, and components that power their AI through conventional means.

BACKGROUND

On February 14, 2022, the Review Board of the U.S. Copyright Office denied a second request for reconsideration regarding a refusal to register artwork created by AI. Importantly, the application for registration indicated that the artwork was created “autonomously” by “a computer algorithm running on a machine.” The applicant did not assert that the work was created with *any* contribution from a human author.

The decision addresses and denies the question of whether AI can be an author for copyright purposes. The decision, however, does not touch the question of whether and, in particular, what degree of involvement of AI in the

creation process renders the output unprotectable under copyright law.

The Review Board’s decision was not all that surprising. In the United States, the Copyright Act protects “original works of authorship” that are fixed in a tangible medium of expression. 17 U.S.C. § 102(a). Case law and commentary analyzing the authorship question in non-AI contexts have long suggested that a human is required for copyright protection. See e.g., *Burrow-Giles Lithographic Co. v. Sarony*, 111 U.S. 53, 57-59 (1884) (holding that an author is “he to whom anything owes its origin; originator; maker; one who completes a work of science or literature”; describing a copyright as “the exclusive right of a man to the production of his own genius or intellect”); *Urantia Found. v. Kristen Maaherra*, 114 F.3d

955, 957-59 (9th Cir. 1997) (holding that a book containing the words “‘authored’ by non-human spiritual beings” can only gain copyright protection if there is “human selection and arrangement of the revelations”); *Naruto v. Slater*, 888 F.3d 418, 426 (9th Cir. 2018) (affirming dismissal of copyright claims brought by a monkey over selfies he took on a photographer’s unattended camera; noting that the Copyright Act refers to an author’s “children,” “widow,” “grandchildren,” and “widower,”—terms that “all imply humanity and necessarily exclude animals”).

THE SITUATION IN FRANCE, GERMANY, AND THE UK

The situation is similar in France, Germany, and in the UK where courts have never recognized any person other than a natural person as author of a copyrighted work.

The finding that AI cannot be an author for copyright purposes does not mean that AI-assisted outputs are void of any copyright protection. Works created by a human using software on a computer (e.g., Microsoft Word or Adobe Photoshop) are arguably protectable under copyright law. In its decision, the Review Board was careful to note that “the Board does not need to determine under what circumstances human involvement in the creation of machine-generated works would meet the statutory criteria for copyright protection.” Feb. 14 Decision, at 3 n.3.

English law provides that fully computer-generated works may enjoy copyright protection. It provides for a specific category for such works created “in circumstances such that there is no human author of the work” and defines the author as the “person” who has made the arrangements necessary for its creation. Such works are afforded 50 years of protection. The provision does not, however, directly address how a computer generated work could satisfy the classic requirement that copyrighted works be “original.” English courts measure originality by reference to characteristics typically associated with human intellect—namely skill, labour, and judgment. The UK Intellectual Property Office recently closed a consultation looking into the provision, asking respondents how AI-generated works should be protected and whether they should remain protected in their current form, under a different scheme, or at all. The results are yet to be published.

French and German courts also have yet to rule on what degree of human involvement might be sufficient to render AI-generated outputs protectable under the respective national copyright law. The more sophisticated an AI is the less likely it is that its outputs will be considered as work protected under copyright laws. In 2020, the European Commission published the final report on “Trends and Developments in Artificial Intelligence—Challenges to the

Intellectual Property Rights Framework,” confirming this finding at least for alpha numeric outputs (text). Other outputs, such as audio data and audio-visual outputs, may enjoy protection under related rights, and in the case of database protection, the sui generis rights might be available. Such protection does not hinge on originality. Of course, the software powering the AI and data used to train the AI also may enjoy copyright protection.

CHINESE COURTS AND “HUMAN INTELLECT IMPRINTS”

In China, although it is not clearly provided in current copyright law if AI-generated works are copyrightable, the Chinese courts have taken some initial positions by noting differences of AI-generated works with or without human involvement, and in some decisions recognized that AI-generated aspects with human intellect imprints could be protectable under certain conditions. For instance, the Nanshan District People’s Court in Shenzhen ruled in what was featured as “China’s first AI case”—*Tencent v. Yingxun* (2020)—that an article generated by Tencent’s team by using “Dreamwriter” software has a certain degree of originality, and the process of the generation shows the “intelligent creation” of Tencent’s team, and as such should be protected under the Chinese Copyright Law.

This case certainly sends signals to incentivize the AI industry from a policy perspective. On the other hand, for AI-generated aspects without human involvement, e.g., any works generated by algorithms automatically evolved by AI through deep or machine learning, it remains to be seen how the copyright law will be developed to address copyrightability of such works. At least at the current stage, some Chinese courts continue to emphasize that creation and completion by natural persons should still be a prerequisite for works to be copyrightable.

TWO KEY TAKEAWAYS

1. In practice, many works involving AI will still benefit from copyright protection where the primary author remains a human, however the degree of human involvement required for this remains uncertain in several jurisdictions.
2. Given the rapid growth seen in AI-generated and AI-assisted works, further developments in this area of law are anticipated.



REGULATING ARTIFICIAL INTELLIGENCE: EUROPEAN COMMISSION LAUNCHES PROPOSALS

APRIL 2021 COMMENTARY

The European Commission has proposed a regulation for how AI systems and their outputs can be introduced to and used in the European Union. The proposed AI Regulation is open to public consultation until 22 June 2021, and needs review and approval by the EU Parliament and the Council. If adopted, it would condition how AI systems are commercialized and used in the EU and could lead to global repercussions, as with the European General Data Protection Regulation. This Commentary summarizes the main building blocks of the proposed regime.

IN SHORT

The Development: On 21 April 2021, the European Commission (“Commission”) unveiled a proposal for a “Regulation laying down harmonized rules on Artificial Intelligence” (“AI Regulation”), which sets out how AI systems and their outputs can be introduced to and used in the European Union (“EU”). The AI Regulation is accompanied by a proposal for a new Regulation on Machinery Products, which focuses on the safe integration of the AI system into machinery, as well as a new Coordinated Plan on AI outlining the necessary policy changes and investment at Member State level to strengthen the EU’s leading position in trustworthy AI.

Background: The draft AI Regulation is part of a wider regulatory agenda in the EU focusing on availability and use of industrial data. Reflecting input from various [stakeholders](#), it aims to establish a European model for the development and use of AI systems that ensures an EU market for AI systems that balances related benefits and risks. Among other things, the draft AI Regulation broadly defines AI systems, specifically prohibits certain uses of AI systems (such as social scoring by public authorities) and foresees a regime for introducing “high risks” AI in the EU.

Looking Ahead: If adopted by the EU Parliament and the Council (which could take two to three years), the proposed AI Regulation would condition how AI systems (or products integrating AI) are commercialized and used in the EU and could lead to global repercussions, as with the European General Data Protection Regulation (“GDPR”). Organizations exploring, developing or using AI systems should consider contributing to the public consultation which is open until 22 June 2021. In any event, they should closely follow these developments which, if adopted, will apply to their activities in addition to key regulations such as the GDPR and possibly the proposed [Digital Services and Digital Market Acts](#).

PROPOSED AI REGULATION

The draft AI Regulation introduces a set of rules, following a risk-based approach, to establish the conditions for an ecosystem of trust regarding the placing on the market, putting into service and use of AI systems in the EU. The main building blocks of the proposed regime are summarized below.

Potential extra-territorial scope: The draft AI Regulation would apply to providers placing on the market or putting into service AI systems in the EU, irrespective of the location of these providers, to all EU users of AI systems; and to both

providers and users of AI systems located outside the EU if the output produced by the AI system is used in the EU.

Wide definition of AI: The draft AI Regulation broadly defines AI systems as all software developed with techniques and approaches such as “machine learning”, “logic- and knowledge-based” and “statistical” approaches, that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments in which they interact.

Prohibited AI practices: The draft AI Regulation proposes to ban AI practices that consist of (i) deploying subliminal techniques beyond a person’s consciousness, or exploiting the vulnerabilities of a specific group of persons, in order to distort these persons’ behavior in a manner that causes or is likely to cause them harm; (ii) social scoring by public authorities; and (iii) using real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless justified for a targeted search for victims of crimes, the prevention of threats to people’s lives and physical safety or of terrorist attacks, and the detection and identification of perpetrators of serious crimes.

Focus on “high-risk” AI systems: The draft AI Regulation introduces a specific regime for placing high-risk AI systems on the market or putting these into service. A number of AI applications qualify as such under the draft AI Regulation, including safety components of products or products covered by existing EU product safety legislation (e.g., for machinery, toys, radio equipment, cars and other types of vehicles, and medical devices) when subject to third-party conformity assessment. High-risk AI systems also include so-called “stand-alone AI systems” used for:

- “Real-time” and “post” remote biometric identification of natural persons;
- Safety in the management and operation of critical infrastructures;
- Educational and vocational training (access to institutions or student assessments);
- Recruiting or making other human resources decisions;
- Evaluating creditworthiness of persons;
- Evaluating a person’s eligibility for public assistance benefits and services;
- Enforcing laws in ways that may interfere with a person’s fundamental rights;
- Processing and examining asylum and visa applications and border control management; and
- Assisting judges in researching and interpreting facts and the law and in applying the laws to the facts.

The list of high-risk AI systems appears comprehensive and covers applications in various industries like banking and finance, social media, HR, and public services, but the Commission could update these.

Qualification as a high-risk AI system triggers a series of mandatory requirements, and compliance with these must be assessed before the products are placed on the market or put into service. These obligations include:

- Establishment of an adequate risk management system;
- Use of high quality training, validation and testing data sets;
- Preparation of technical documentation providing all necessary information on the system and its purpose to assess its compliance with the requirements;
- Development of logging capabilities enabling automatic recording to ensure traceability of the functioning of the system;
- Provision of appropriate transparency on the operation of the AI system and clear information to users;
- Guarantee of human oversight to minimize risk; and
- Attainment of a high level of accuracy, robustness and cybersecurity.

Providers of high-risk AI systems must assess compliance with these requirements in accordance with the conformity assessment procedures set out in the draft AI Regulation. Depending on the type of system concerned, these procedures can either take the form of a self-assessment or a third-party assessment through the involvement of a notified body.

High-risk AI systems that are deemed to comply with the mandatory requirements following assessment by their providers should bear the “CE” quality marking to indicate their conformity with European rules. Stand-alone high-risk AI systems must also register with a publicly available EU database on high-risk AI systems.

In addition to the above obligations borne by providers, the draft AI Regulation also imposes obligations on importers, distributors, and users of high-risk AI systems to ensure that these products comply with regulatory requirements before their placing or making available on the market and to ensure safe use of the products.

Non-high-risk AI systems: Unlike high-risk AI systems, the draft AI Regulation regulates non-high-risk AI systems only to a limited extent by imposing transparency obligations for such AI systems in order to protect the users of, or persons exposed to, such technology. This covers AI intended to interact with natural persons, emotion recognition systems, a biometric categorization systems, and deepfakes. All

other AI systems can be developed and used without additional legal obligations.

Measures in support of innovation: To promote innovation, the draft AI Regulation would enable national regulators to establish regulatory sandboxes schemes and require Member States to provide certain services and facilities to small-scale providers, start-ups, and users.

Enforcement: The draft AI Regulation delegates most enforcement powers to Member States, who will designate competent EU Member State authorities (most likely the data protection authorities) and determine the penalties applicable to infringements of the AI Regulation. Notably, despite Member State powers to decide on penalties, the draft AI Regulation provides that failure to comply with certain sensitive provisions (i.e., prohibited AI practices and high quality of data sets) will result in maximum fines of up to EUR 30 million or 6% of a company's worldwide annual turnover. Non-compliance with any other requirements applicable to AI systems would result in fines of up to EUR 20 million or 4% of a company's worldwide annual turnover.

National monitoring and enforcement will be supervised by a contemplated European Artificial Intelligence Board, whose role will be to facilitate an effective and harmonized implementation of the draft AI Regulation e.g., through the issuance of recommendations.

MACHINERY REGULATION

The draft Machinery Regulation complements the draft AI Regulation and is intended to replace the Machinery Directive. It aims at ensuring a safe integration of the AI system into machinery as a whole, towards safeguarding against compromising the safety of the overall machinery for users and consumers. Businesses would need to undertake only one conformity assessment for both the AI Regulation and the Machinery Regulation. The draft Machinery Regulation would also respond to market needs by bringing greater legal clarity to current provisions and simplifying the administrative burden and costs for companies.

NEXT STEPS

The European Parliament and the Council of the EU will now review and discuss the Commission's proposals, which could result in modifications. Both institutions must approve the final text under qualified majority before the AI Regulation and the Machinery Regulation take effect. This process could take two to three years.

A GLOBAL TREND

This EU initiative takes place within a broader global discussion on the need to adopt AI-specific rules. For example, in November 2020, the U.S. White House, through its Office of Management and Budget, issued Guidance for Regulation of AI Applications, which establishes a framework for federal agencies to assess potential regulatory and non-regulatory approaches to emerging AI issues. All federal agencies with authority over these issues are directed to provide compliance plans by May 2021. Additional U.S. AI-driven initiatives concern the use of AI in the Federal Government and the creation of a new National AI Initiative Office for federal AI coordination, which may play an important role in the governance of AI.

FIVE KEY TAKEAWAYS

1. The Commission has released a proposal to define the first EU-wide regulatory framework on AI. The proposed centerpiece AI Regulation aims to guarantee user safety and safeguard fundamental EU values and rights, while strengthening AI uptake and innovation across the EU. The proposed AI Regulation would not require further implementation into each national law of the Member States. However, certain grandfathering rights would apply for legacy AI systems that are not subject to significant changes in their design or intended purpose.
2. The draft AI Regulation deals with core considerations such as defining AI and high-risk applications, regulatory obligations for providers of AI systems, and the conformity assessment of high-risk AI applications. This ensemble would implicate a broad cross-section of industries.
3. The draft AI Regulation proposes to ban certain uses of high-risk AI systems altogether, while making others subject to mandatory requirements and increased scrutiny.
4. Failure to comply with the draft AI Regulation could result in significant administrative fines of up to EUR 30 million or 6% of a company's annual worldwide turnover.
5. The proposed AI Regulation could create a new impetus towards increased enforcement and advocacy for safety and user rights in all Member States, as influenced by the envisaged European Artificial Intelligence Board.



IP PROTECTION OF ARTIFICIAL INTELLIGENCE IN EUROPE: TAILOR-MADE SOLUTIONS REQUIRED

APRIL 2020 COMMENTARY

IN SHORT

The Situation: The use of artificial intelligence (“AI”) enables important transformative developments across different industries and research areas.

The Result: As significant resources are invested, Intellectual Property (“IP”) protection is sought for technological aspects of an AI solution and the resulting work product. Several European IP rights are available to choose from.

Looking Ahead: The landscape for patenting AI innovations is still developing. The European Patent Office (“EPO”) has addressed some aspects of AI patenting in its updated examination guidelines, though case law from the EPO Boards of Appeals (“BoA”) and national patent offices on fundamental questions may be years away. The same applies to the new EU trade secret directive and its various implementations into national law. In most cases, to maximize IP protection, a combination of IP rights suitable for different aspects of an AI innovation should be considered.

INTRODUCTION

IP institutions around the world are addressing a variety of issues associated with AI (see “[AI and the Biopharmaceutical Industry](#)”). European stakeholders, i.e. the EPO, the European Commission, national governments and IP offices have launched initiatives that may impact IP protection policies of AI innovations. The latest developments and tactical considerations are summarized below.

CHOICE OF IP RIGHTS

1. What May Be Protected?

The general workflow of constructing an AI model solution for a defined problem includes the acquisition/preparation of training data, the design of an appropriate model architecture (e.g. choosing suitable AI algorithms, setting initial parameter values), model training, evaluation, and optimization. Additionally, large high-quality, representative training datasets are extremely important for reliable performance of an AI model when processing new data.

Business value may therefore be found in protecting (i) AI models and/or algorithms; (ii) software in which the models/algorithms are embedded; (iii) training, evaluation and/or optimization strategies; (iv) training data; and (v) result data (i.e. work product). IP protection may be sought for all or a subset of these potential assets.

While copyright essentially only protects source code written by a programmer, further IP rights suitable for other aspects of an AI innovation are discussed below.

2. European Patents

A. General Principles

Although mathematical models and algorithms are not patentable under the European Patent Convention (“EPC”), AI inventions are generally patentable as a subgroup of computer-implemented inventions (“CIIs”) (see “[Patenting Artificial Intelligence and Machine Learning Innovations in Europe](#)”).

According to established EPO case law, inventiveness can be assessed by considering only those features that contribute to a technical character of an invention (G-VII, 5.4 of the Guidelines for Examination at the EPO). However a non-technical feature (e.g. algorithm), which interacts with technical features to solve a technical problem, should also be considered (COMVIK, T 641/00). Protectable subject matter differs from country to country depending on what it is directed to (e.g. product vs. method) and the technical field.

B. Latest EPO Case Law on AI Patenting

In a recent decision (T 697/17 in October 2019), the EPO’s BoA “dissected” existing case law and emphasized that to identify technical contribution it is necessary to examine if a non-technical feature under dispute was chosen based on technical considerations aimed at achieving a technical effect. If going “*beyond ‘merely’ finding a computer algorithm to carry out some procedure*” such technical considerations may result in technical contribution. In T 731/17 in January 2020, the same BoA further addressed the assessment of technical contribution in line with its previous opinion.

When drafting a patent application in the CII or AI field, it is important to identify technical considerations and motivations behind non-technical features that contribute to the solution of a technical problem.

C. AI as an Inventor

Earlier this year, the EPO published reasoned decisions on the refusal of two patent applications (EP18275163; EP18275174) designating AI as an inventor. The EPO concluded that for the mandatory designation of an inventor for a European patent application the inventor must have a legal personality.

3. Utility Models

In a plurality of countries technical inventions can also be protected by utility models, sometimes called Utility Certificates (see “[French PACTE Act: Provisional Patent Application and the Evolution of the Utility Certificate](#)”). Protectable subject matter differs from country to country depending on the technical field and the type of subject matter (product vs. method). The requirements for acquiring a utility model are in most countries less stringent. Lacking substantive examination in most countries, the registration and publication process is simpler, faster, and cheaper. Utility models should be considered as an expeditious, less costly way to obtain IP protection for often “quickly” outdated AI inventions.

For example, in Germany it is possible to “branch-off” a utility model from an earlier patent application while maintaining priority and the filing date of the patent application. The “branch-off” utility model may be registered in a few weeks. This strategy may be considered to obtain an enforceable IP right while the patent application is examined.

4. Trade Secrets

Directive EU 2016/943 has widely harmonized trade secret protection across the EU. An owner is entitled to protection against unlawful acquisition and use of a trade secret and is entitled to damage claims in case of misappropriation.

Trade secrets may provide the broadest scope of IP protection. To rely on it, the directive requires an owner to implement internal trade secret policies and adequate measures to protect know-how. Relevant technological information should be documented to prove possession of the know-how in case a litigation arises.

FIVE KEY TAKEAWAYS

1. AI technologies have a potential to generate immense economic value and give rise to entirely new services. It is advisable to companies developing and implementing AI solutions to obtain legal exclusivity to secure assets.
2. European legislation provides options to choose from when building a strategic portfolio of IP rights.
3. Patent protection may be obtained for application of AI in solving a technical problem. The patent drafter should keep in mind that identifying technical considerations and motivations may be important in establishing technical contribution of an AI algorithm or model.
4. In various countries, like France and Germany, a utility model system may be used to quickly obtain an enforceable IP right, e.g. while the related patent application is still under examination.
5. Trade secrets provide the broadest IP protection. To rely on trade secret protection, an owner has to implement related internal policies and adequate protective measures.



OCTOBER 2022 ALERT

The Artificial Intelligence Bill of Rights sets forth voluntary guidelines that companies utilizing or developing technology with artificial intelligence can follow to protect users.

On October 4, 2022, the White House Office of Science and Technology Policy published the blueprint for an AI Bill of Rights (the “AI Bill”), with the stated purpose of protecting the public from harmful outcomes or harmful use of technologies that implement artificial intelligence (“AI”). While AI is a powerful technology that has transformed and improved many aspects of day-to-day living, its implementation has the potential to lead to unintended and sometimes negative consequences.

The AI Bill’s framework applies to companies with “(1) automated systems that (2) have the potential to meaningfully impact the American public’s rights, opportunities, or access to critical resources or services.” Companies that fall under this framework are encouraged to follow the AI Bill’s five principles:

1. **Safe and Effective Systems.** Companies should ensure automated systems are designed to protect users from harm. To achieve and guarantee this, automated systems should undergo regular monitoring designed to identify and mitigate safety risks.
2. **Algorithmic Discrimination Protections.** Companies should emphasize equity when developing algorithms through use of representative data and by conducting proactive equity assessments. Discriminatory uses of algorithms and algorithms that generate discriminatory results should be abolished and prohibited.

3. **Data Privacy.** Users sharing their data should have agency over how their data is used and be protected from abusive data practices. As such, companies should include built-in data protections and limit collection to data that is “strictly necessary for the specific context.”
4. **Notice and Explanation.** Users should be notified when an automated system is in use, and accessible plain language should describe how and why such a system contributes to outcomes that impact users.
5. **Human Alternatives, Consideration, and Fallback.** Companies should provide users with the option to opt out from automated systems and alternatively provide access to a human consultant, where appropriate.

While the AI Bill only sets forth voluntary guidelines, it sets the stage for future legislation and regulations surrounding the use and implementation of AI. More details can be found [here](#).



NFTs: U.S., EU, AND UK KEY COPYRIGHT CONSIDERATIONS

MAY 2022 COMMENTARY

IN SHORT

The Situation: The current non-fungible token (“NFT”) market presents exciting new opportunities and important intellectual property (“IP”) considerations. In this first of two *Jones Day Commentaries* exploring the interaction of IP with the current crop of NFTs, the focus is on copyright issues.

The Result: Owners, sellers, and prospective buyers of NFTs, as well as owners of the underlying material, need to be aware of potential copyright risks associated with this fledgling market.

Looking Ahead: The related practice of trading NFTs accentuates the need for existing IP issues in this area to be tested in courts and commercially.

NFTs are verifiable cryptographic tokens, which can act as a form of digital receipt. NFTs can also be used to evidence the authenticity, ownership, and provenance of real-world items, such as artwork and real property, or digital files including an image, GIF, or tweet. NFTs raise material copyright concerns if the NFT contains a digital copy of an asset that might amount to an unauthorized reproduction and thus constitute infringement. In such a situation, the existing copyright owner of that asset could send a take-down notice or bring an action against both the person(s) making the unauthorized reproduction, as well as the platform hosting or trading the infringing content.

NFTs that infringe on copyrighted works can also create practical difficulties for enforcement where, for example, the NFT draws inspiration from a real-life work without explicitly copying it. Given the escalating number of NFT marketplaces, it is an immense burden on rights holders to continuously monitor unauthorized use.

KEY COPYRIGHT CONSIDERATIONS

To purchase an NFT is to buy an authentication of ownership of an asset as a digital file, but it does *not* necessarily transfer ownership of the underlying asset itself. NFTs come in different forms (and the terms of ownership will vary), but the remainder of this piece focuses on the most common, current use case where a buyer of a NFT acquires a proprietary right to an underlying work and a digitally authenticated certificate that verifies ownership.

Most NFTs contain a URL link to a file, with the buyer obtaining merely a license of noncommercial usage rights, such as displaying the file for personal use or resale. The creator of the underlying file can determine how to generate profit through a so-called “smart contract.” The terms of these smart contracts include those allowing buyers to co-own an NFT, the creator being able to sell multiple NFTs for one file, and a percentage of profits owed to the creator for any prospective sales. Typically, the creator will retain all intellectual and creative rights to the work, including copyright and production rights to make and sell copies or iterations

of the work. An NFT simply proves that the buyer is the owner of *that* work, and the terms of ownership will vary among NFTs.

Caveat Emptor—Buyers Beware!

Earlier this year, a group of investors called Spice DAO, operating as a tokenized community organization, purchased at auction a rare, script bible from legendary filmmaker Alejandro Jodorowsky setting out how he planned to film the Frank Herbert sci-fi classic *Dune*. The Spice DAO community paid an eye-watering \$3 million for the book, intending to monetize it by converting each page of the script book into an NFT for sale and producing an original animated series based on the script. The problem was they did not own the copyright to do any of this. They mistakenly believed that, in purchasing the script bible, they were acquiring the copyright to the script and the underlying story and characters, when in fact all they had acquired was the physical book itself. The lack of understanding in the marketplace regarding IP and NFTs is, perhaps, unsurprising when considered in light of this case, given that such a large community of people had so fundamentally misunderstood the nature of copyright and the exploitation of such.

Copyright Infringement

Copyright infringement has become a source of debate with NFTs, as current U.S., EU, and UK IP legislation does not specifically account for cryptographic digital work. At the heart of the debate is the fact that the current crop of NFTs are typically not “works” within the usual meaning of copyright law but rather a digital receipt of *ownership* or a chain of title of an underlying work. NFTs are created by a process called “minting,” in which metadata is written into a blockchain, but which typically does not reproduce or modify any underlying work (e.g., a photograph).

IP infringement in relation to NFTs is likely to arise in one of two circumstances:

1. Minting an NFT for an underlying protected work, but where the online seller does not own the intellectual property rights therein (see *Miramax v. Quentin Tarantino*, discussed below); and
2. Minting an NFT where the underlying work is created by the online seller, but it contains an element of reproduction or outright copying of another’s intellectual property.

Unauthorized copying (and associated acts) of any underlying work that is attached to an NFT may constitute infringement under U.S., EU, and UK copyright law. While the actual minting of an NFT is an act not contemplated by the existing legislation, where it involves the unauthorized reproduction of a copyright work, it will likely constitute an infringing act, albeit one involving a new medium.

Copyright infringement is therefore relevant only if the NFT contains a digital copy of an asset that might amount to an unauthorized reproduction. In such a situation, a claimant has means to issue a take-down notice or can bring an action against both the person(s) making the unauthorized reproduction, plus the platform that is hosting the unauthorized content or offering it for sale or exchange, typically an NFT marketplace. Going after the marketplace may have a more immediate result (i.e., the NFT being removed from trading); however, this may not deter the individual from minting the same NFT on an alternative platform, particularly given the increasing number and diversity of NFT-related sites.

An NFT owner will need to acquire an assignment or license of the subsisting rights from the original creator of the work to be able to reproduce, or otherwise deal with, the work. As there is typically no owner verification process on many NFT marketplaces, issues have arisen with purported NFT sellers (either knowingly or unknowingly) not owning the intellectual property rights necessary to deal with the underlying work.

CASES TESTING COPYRIGHT INFRINGEMENT VIA NFT TRADING

Miramax v. Quentin Tarantino

In December 2015, Quentin Tarantino sought to mint an NFT of unused content from the Miramax film *Pulp Fiction*. Miramax alleged breach of contract and that Tarantino had infringed its copyright and trademark rights. Miramax filed a lawsuit against Tarantino in November 2021. While the lawsuit is pending, Tarantino had gone on to sell his first NFT for \$1.1 million. The case will follow the question as to whether U.S. copyright law protects the right to convert a copyrighted work into an NFT. Also at issue is whether Tarantino’s right to “screenplay publication” under his assignment of work to Miramax in 1993 extends to or is encompassed in selling an NFT of such screenplay content.

Art Wars

Similarly, in November 2021, images of *Star Wars* helmets from the “Art Wars” exhibition in London were sold as a collection of 1,138 unique NFTs by Ben Moore, the founder of the exhibition. These helmets were painted by artists including Dinos Chapman, Anish Kapoor, and David Bailey, and after the collection was put on sale on November 22, 2021, almost \$7 million had been transferred on NFT site OpenSea. The NFT page on OpenSea was removed in November 2021 following a copyright infringement notice, and it is reported that approximately 12 of the artists are preparing to file a lawsuit.

PRACTICAL IMPLICATIONS OF ENFORCEMENT

There is no simple solution for addressing NFTs that infringe IP rights. As noted above, pseudonymized NFT creators can determine whether they create one or multiple NFTs, whether to offer a co-ownership structure, the rights contained in the smart contract, and whether to create direct copies or iterations of the work. In addition, NFTs are extensible and can be combined with other NFTs to create a third unique NFT.

The underlying works of some NFTs may also draw inspiration from real-life works but not explicitly copy the work. This makes determining the outcome of an infringement claim uncertain, although such issues are not new in copyright law. It is also unclear what the position would be in respect of unauthorized NFTs that have already been sold to a bona fide purchaser, although it is expected that the law will remain consistent in this regard.

Given the escalating number of NFT marketplaces, it is an immense burden on copyright holders to continuously monitor unauthorized use. Moreover, the creation, sale, and trading of NFTs is often unregulated under local laws, and the transaction is recorded on a public decentralized database. These issues make the “tracking” exercise for copyright infringement even more extensive.

CONCLUSION

While some commentators question whether the current NFT boom can continue, it is likely that they will present unique intellectual property issues and opportunities in the short term. Over the longer term, we are likely to see more NFT use cases and emerging best practices for engaging with rights holders. In the meantime, it will be interesting to see how the courts apply existing and long-standing principles of copyright law to the new medium of NFTs.

FOUR KEY TAKEAWAYS

1. NFTs create new opportunities for creators in terms of multichannel revenue sources, control over the terms of the transaction via a smart contract, and increased prominence in a new industry. However, creators should equally be aware of the risks of infringement and, in particular, verify that they own the necessary rights in the underlying work attached to the NFT.
2. The current U.S., EU, and UK law governing the protection and enforcement of copyright requires testing in this sphere.
3. Copyright owners should actively monitor and enforce their rights in the NFT space.
4. While it is uncertain whether the current NFT boom will last, it is likely that the NFT market will develop over time, impacting the verification and ownership of artistic creations in the future, which presents both opportunities and threats to IP owners.



NFTs: KEY U.S. LEGAL CONSIDERATIONS FOR AN EMERGING ASSET CLASS

APRIL 2021 COMMENTARY

Non-fungible tokens (“NFTs”) have captured headlines in the already fast developing, innovator-driven space of blockchain technology. Although the technology that makes NFTs possible has been around for several years, U.S. regulations and laws have remained mostly unchanged until recently. Typically used to describe a DLT token which represents a unique asset (and is therefore not interchangeable), NFTs are particularly being used by creators and artists exploring ways to commercialize and directly monetize their work. However, others are looking to take NFTs even further and are testing how to apply the technology to other fields, such as finance. Only time will tell whether NFTs are a fad or passing phenomenon; regardless, the regulatory and legal issues they present must be addressed in the here and now.

The Situation: Non-fungible tokens are an emerging digital asset class that present a unique set of commercial, regulatory, and other legal considerations.

The Result: The current U.S. regulatory and legal framework is slowly catching up to the developing technology. Key legal issues include how NFTs can be categorized, intellectual property rights, anti-money laundering and sanctions implications, cybersecurity concerns and state laws governing virtual currencies.

Looking Ahead: As the asset class matures, U.S. regulations and laws are catching up to the developments and increased interest in the technology—with other applicable global regulatory regimes already in place. Investors, financial services and fintech companies in this space should consider key legal issues and make careful plans for exploring potential opportunities in this space.

NFTs, or non-fungible tokens, are an emerging digital asset class that have captured the attention of consumers and investors alike. Although the technology that makes NFTs possible has been around for several years, NFTs have very much emerged into public consciousness in 2021. Celebrities, creators, and athletes are investing in NFT technology and exploring ways to commercialize their brand, image, or work through issuing NFTs. While this asset class is in its nascent stages, the legal and regulatory issues they present are very real. Below we briefly describe NFTs and some of the most relevant U.S. legal issues.

What are NFTs?

In general terms, an NFT is a digital asset, based on computer code and recorded on a blockchain ledger to prove ownership and authenticity of a unique asset. Its “non-fungible” nature distinguishes an NFT from other digital assets. Most other blockchain tokens are created to be fungible or “interchangeable.” For example, two different bitcoin ledger entries are interchangeable, and being the holder of either allocation would give the owner the same rights as the other. Almost anything can be represented by an NFT providing it is a unique asset—for example, real property titles, cars, houses, and other merchandise, as well as digital assets such as images, documents, videos, and tweets. In one recent case, a unique digital artwork represented by an NFT was auctioned off at Christie’s for \$69 million.

However, NFTs are not used for fractionalized ownership—where the ownership of a single asset such as a property or artwork is divided into tokens allowing each holder to own a small piece of a single asset. At its essence, NFTs bring unique assets into the digital space and make ownership of that asset verifiable.

In technical terms, NFTs are often created on the Ethereum blockchain through the ERC721 token standard written in the Solidity programming language. NFTs are now also being created on the EOS, Cardano, Flow, and Tron blockchains.

What Are Some Key Legal Considerations Surrounding NFTs?

The existing regulatory and legal environment was not designed to accommodate digital assets, including NFTs. Nonetheless, there are some key issues that have emerged while investors, financial services and fintech companies, and other commercial interests explore this space. Simply stated, there is no “free lunch” on the regulatory front for NFTs, and this asset class also presents other commercial and legal issues—many of which have current solutions, but may require compromises:

Will an NFT be Treated as a Commodity or Security (or Something Else) in the U.S.?

By their nature, NFTs can be linked to a variety of different assets and represent numerous rights and obligations, making them challenging to classify. Although regulators so far have not provided official guidance about NFTs, it is possible that an NFT could be considered a “commodity” under the Commodity Exchange Act (“CEA”), which defines the term to include several enumerated items and a catch-all for “all other goods and articles.” The Commodity Futures Trading Commission (“CFTC”) has also stated that the “commodity” definition includes cryptocurrencies, like Bitcoin and Ether, as well as renewable energy credits, emission allowances, and other intangible items. NFTs share some similarities with cryptocurrencies in the sense that they too are purchased, sold, and held using blockchain technology.

If an NFT is considered a commodity, the CEA may apply in one of two possible ways. First, the CEA’s general prohibitions on deceptive and manipulative trading may apply to NFT transactions effected on a “spot” basis, i.e., fully-funded, unleveraged transactions. If an NFT is offered on a margined or leveraged basis, however, additional requirements could apply—including the requirement to trade the NFT solely on a registered derivatives exchange—unless the transaction results in the “actual delivery” of the NFT within 28 days. The CFTC recently issued an interpretation on “actual delivery” for digital assets used as a medium of exchange that can be helpful in considering these issues.

Looking beyond the CEA, many NFTs available on the market today appear unlikely to be considered “securities” under the federal securities laws for a number of reasons. An NFT could be considered a security, however, if it were designed to provide an expectation of profit to the buyer based on the efforts of others and were marketed as such. One potential example of such an arrangement could be a “fractional” NFT (“f-NFT”), where an investor would share a partial interest in an NFT with others. Depending on the facts and circumstances, f-NFTs could be considered an “investment contract” under the Howey Test.

If an NFT (or fNFT) is considered a security, then common securities law issues would be present—e.g., registration or exemption of the offering under the Securities Act of 1933; registration of the sellers of those instruments as broker-dealers under the Securities Exchange Act of 1934 (“Exchange Act”); registration of the marketplaces on which the instruments are sold as securities exchanges under the Exchange Act; securities law liability for material omissions or misstatements and insider trading; restrictions on short sales and market stabilization around an initial offering; and so on.

What Intellectual Property Rights are Transferred in a Sale of an NFT?

In general, the rights that accompany an NFT are determined by the seller of the NFT. NFTs contain metadata that describe the corresponding assets to which they are bound. For many NFTs available today, each asset underlying the NFT is created by someone who owns intellectual property rights in the asset and decides what rights to grant the NFT buyer. If the issuer of an NFT is a content creator, then the issuer will have all rights in the content and can create NFTs that correspond to that content assigning any of those rights to a buyer—for example, the right to use, copy, display, and modify the content. If an issuer obtains content from a creator, then the issuer would only receive the rights such creator assigned or licensed to the issuer, and will only be able to assign or license those limited rights to the buyer. Common issues that could arise in NFT transactions include ensuring that sufficient transfer, assignment, or licensing language (including any restrictions on the buyer's right of use) is included in a sale to effect the transfer of rights in the manner intended by the parties to the sale.

Are NFTs Subject to Federal Anti-Money Laundering Laws and What About U.S. Sanctions?

The Financial Crimes Enforcement Network (“FinCEN”) is the bureau of the U.S. Department of Treasury with regulatory authority over the financial system to combat money laundering under the Bank Secrecy Act (“BSA”) and other related laws. To date, FinCEN has not issued guidance specific to NFTs, but it has published guidance generally about how the BSA and FinCEN regulations relate to virtual currencies that could apply to NFTs. One question is whether FinCEN regards NFTs to be “value that substitutes for currency.” If NFTs are considered substitutes for currency, then FinCEN could consider NFTs to be subject to the BSA and FinCEN regulations. Since many NFTs are more like digital representations of ownership in unique assets than value that substitutes for currency, however, it seems that many NFTs available on the market should not be subject to FinCEN’s oversight. Depending on the facts and circumstances, certain other business activities related to the transfer, sale, and custody of NFTs may implicate FinCEN regulations.

The Office of Foreign Assets Controls (“OFAC”) administers most U.S. sanctions programs. Similar to FinCEN, OFAC has not provided guidance specific to NFTs, but it has explained that U.S. sanctions apply to digital transactions and currencies in ways similar to traditional activities. Further, OFAC has pursued enforcement actions involving cryptocurrency transactions and blockchain technology. The possibility of persons subject to U.S. sanctions participating or benefiting, directly or indirectly, from activities involving NFTs

present the primary avenue of risk exposure; moreover, NFTs present circumstances that OFAC has identified in other scenarios as presenting heightened risks for potential violations. While details will vary with different structures, the potential lack of transparency and decentralization associated with the use of blockchain technologies can present difficulties in preventing sanctioned persons from participation. Further, NFTs may present many of the same issues that OFAC recently identified as associated with artwork, including a high degree of anonymity, the use of intermediaries, concealability, and subjective valuation. Given these considerations, those participating in NFT transactions should pay heed to sanctions considerations.

Are NFTs Subject to State Laws Governing Virtual Currency or Money Transmission?

Given the superficial similarities between NFTs and some virtual currencies, it is reasonable to consider whether NFTs are subject to state laws governing virtual currency or money transmission. To date, no state regulator with oversight of virtual currency or money transmission has issued guidance directly about NFTs. Depending on how a particular state defines money transmission, it is possible that some may try to claim regulatory oversight over certain NFTs or certain business activities related to NFTs.

In addition, some states have passed laws addressing the operation of companies engaged in virtual currency businesses. New York and Louisiana are two examples. Each state has a list of activities it deems under its laws to constitute virtual currency business activities, which can include for example: exchanging, transferring, controlling, administering, or issuing virtual currency. Both states require companies that engage in such activities to obtain a license or charter and post surety bonds or fund an account for the protection of customers. Depending on the characteristics of the NFT, it is possible that either state could try to apply its virtual currency law to the NFT marketplace. However, many current NFTs available on the market should not be subject to those statutes.

Do NFTs Give Rise to Unique Cybersecurity Concerns?

As a fully digital and potentially valuable asset, NFTs likely will be targeted with greater frequency by cybercriminals for financial gain. Centralized NFT marketplaces that store private keys may prove especially attractive. By obtaining the private key associated with an NFT, a malicious actor can access, move, and sell the NFT without authorization from the NFT's rightful owner. And once stolen, given the decentralized and immutable nature of blockchain-based transactions, the NFT is not so easily returned.

An online NFT marketplace recently acknowledged that a small number of its user accounts were compromised in so-called “account takeovers” in which an unauthorized third party acquired the credentials (e.g., passwords) needed to access user accounts. The incident highlights a key vulnerability inherent in all user-facing online platforms—users inevitably may be the most common point of compromise and are susceptible to phishing attempts, brute force attacks, and other tactics designed by malicious actors to obtain account credentials.

To mitigate the risk of loss and legal exposure, NFT platforms should consider administrative, technical, and physical safeguards, such as multi-factor authentication to better protect the security of private keys and account access credentials, need-based access controls, periodic risk assessments, and written policies that clearly document the same.

The inherently cross-border nature of NFTs also raises complex issues of applicable law and regulation that may arise if NFTs are sold globally, and it should be noted that other jurisdictions already have regulatory regimes which will be relevant to NFTs (such as the EU’s proposed Markets in Crypto-Assets Regulation) which we will address in a follow up publication.

This is a dynamic space that should be monitored as the asset class evolves, markets develop, and the law and regulations begin catching up. But enough is known today about the key issues, such as those set forth above, to develop careful plans for exploring potential opportunities in this space.

FOUR KEY TAKEAWAYS

1. NFTs are an emerging asset class that have captured the attention of consumers and investors in the U.S., but have outpaced the regulatory and legal framework.
2. Key to understanding the use and value of any NFT are the intellectual property rights granted, for example, the right to use, copy, display, and modify the content.
3. There is no direct state regulatory guidance on NFTs, though a few states have created laws that could hold NFTs under their purview. FinCen has not issued any guidance specific to NFTs, but it has published guidance generally about how the BSA and FinCEN regulations relate to virtual currency that could apply to NFTs.
4. NFTs likely will be targeted with greater frequency by cybercriminals for financial gain or by persons otherwise restricted from traditional markets. NFT platforms need robust controls to guard against such risks.



U.S. SUPREME COURT ENDS DECADE-LONG SOFTWARE COPYRIGHT BATTLE: GOOGLE WINS

APRIL 2021 ALERT

U.S. Supreme Court holds that Google's use of a small fraction of Oracle's Java SE API code for its Android platform is a fair use under copyright law.

On April 5, 2021, the U.S. Supreme Court ended a more than 10-year battle between Google and Oracle over copyright infringement claims concerning Google's Android mobile platform and Oracle's Java programming language. In a 6-2 opinion authored by Justice Breyer (Justice Barrett did not participate), the Court held that Google's use of a small fraction of Oracle's Java SE API code for its Android platform was protected under copyright's fair use doctrine. Although ruling for Google on fair use, the Court did not address the question of whether Oracle's API declaring code was entitled to copyright protection, instead assuming "for argument's sake" the code was copyrightable.

The Court's ruling resolves what some have called "the copyright case of the decade." It all began when Google used some of Oracle's Java application programming interfaces ("APIs") to develop its Android smartphone platform, which Google introduced in 2007. (APIs are prewritten packages of code that allow software programs to interact.) Oracle sued Google in 2010, seeking as much as \$9 billion in damages and accusing Google of copying roughly 11,500 lines of declaring code from the Java SE API (about 0.4% of the total Java API code) in the Android platform.

Before making its way to the Supreme Court, the case was tried twice before the district court and heard twice by the Federal Circuit. After the first trial, the district court held that the Java SE API code was not copyrightable. The Federal Circuit, however, reversed that decision in 2014 and remanded for a jury trial on fair use. At the second trial, the jury found for Google on fair use. The Federal Circuit reversed that decision as well in 2018. The Supreme Court's decision throws out the Federal Circuit's 2018 decision in its entirety.

The Court held that fair use, while a "mixed question of fact and law," should be treated and reviewed as "a legal question, de novo." It went on to conclude that Google's incorporation of a portion of the Java SE API was "a fair use of that material as a matter of law" because "Google reimplemented a user interface, taking only what was needed to allow users to put their accrued talents to work in a new and transformative program." Justice Thomas, joined by Justice Alito, dissented and disagreed with the result, stating that they would have held the Java SE API declaring code copyrightable and further opining that the Court should have decided that question rather than simply assuming copyrightability, because consideration of that question informs whether use of a copyrighted work is fair. The Court's decision is likely to have a significant impact in the application of the fair use doctrine in software cases going forward.



APRIL 2022 COMMENTARY

IN SHORT

The Situation: State securities regulators in Texas and Alabama filed two first-of-their kind enforcement actions against a company selling non-fungible tokens (“NFTs”) to operate casinos in a metaverse.

The Result: The cease and desist orders issued against the company allege various state law violations, including making deceptive and misleading representations to investors that constitute fraud and offering NFTs as securities to the public without first registering them with the state commissions.

Looking Ahead: As regulatory agencies continue to monitor developing technologies, expect to see more enforcement actions in the United States alleging that companies are promoting and selling products that run afoul of regulations.

In two first-of-their-kind enforcement actions relating to NFTs, securities regulators in Texas and Alabama ordered a Cyprus-based online casino developer and its founders to cease and desist selling NFTs that allegedly were marketed and sold as securities. The Texas [order](#), dated April 13, 2022, alleges that the company and its cofounders offered 11,111 NFTs in an unregistered and fraudulent securities offering to raise funds to operate virtual casinos in a metaverse. The Alabama Securities Commission, with the help of the Kentucky Department of Financial Institutions, simultaneously issued a similar [order](#) against the company and its founders.

According to a [statement](#) issued by the Texas State Securities Board, the company and its founders marketed their NFTs—which they named “Gambler” and “Golden

Gambler”—as investment opportunities and promised potential buyers a share in the virtual casino’s profits, forecasting as much as \$81,000 annually. The statement further claims that the company told potential buyers that its NFTs were not regulated as securities because securities laws did not apply to NFTs.

The company allegedly planned to use a portion of the proceeds from its NFT sales to purchase “land” to operate virtual casinos in platforms like Decentraland, Sandbox, Infinity Void, and NFT Worlds, which are metaverse platforms. Metaverse casinos operate just like real casinos, except in virtual worlds. Using virtual reality avatars, customers can enter metaverse casinos and play casino games using cryptocurrencies. According to the allegations made by Texas and Alabama authorities, marketing materials

promised owners of Gambler and Golden Gambler NFTs that they would receive monthly payments based on the profitability of the metaverse casinos.

The Texas order alleges that Gambler and Golden Gambler NFTs are securities under Texas securities laws and should have been registered before being offered to the public. The order further claims the company misled the public through deceitful and fraudulent statements concerning these products. This is the first time that securities regulators have issued cease and desist orders related to an NFT offering for a platform in a metaverse, but it is likely not the last. The Texas State Securities Board states that it has identified other securities offerings in metaverse platforms and is coordinating with other states to investigate and possibly pursue enforcement actions.

FOUR KEY TAKEAWAYS

1. State securities regulators in Texas and Alabama have targeted NFTs that were allegedly marketed and sold as securities offerings. They are actively monitoring all types of digital assets for unregistered and fraudulent securities offerings. Other state securities regulators are likely to follow suit against companies operating in a metaverse that do not comply with state securities laws.
2. State and federal securities laws in the United States can apply to non-U.S. companies. Products on distributed ledgers and metaverse platforms are readily accessible by people around the world, which underscores the global regulatory risks of companies that do business in this space.
3. While most NFTs that are popular in the market currently do not have features making them securities under United States federal or state law, depending on the rights associated with them and how they are marketed, it is possible that they could be structured as securities offerings.
4. Companies operating in this space should engage qualified legal counsel to review their products and marketing plans to advise on any risks.



EUROPEAN COMMISSION UNVEILS SWEEPING PROPOSALS TO REGULATE THE DIGITAL SECTOR

JANUARY 2021 COMMENTARY

IN SHORT

The Development: The European Commission (“EC”) recently released two long-awaited legislative proposals, the Digital Services Act (“DSA”) and Digital Markets Act (“DMA”), that would significantly increase the EC’s regulatory oversight of online platform companies (previewed in our [June 2020 Commentary](#)).

Background: The EC and Member State antitrust authorities have investigated whether certain conduct of online platforms is anticompetitive, including for example, sharing user data across distinct online services, preferencing a platform’s own products above competing businesses on the platform, or using data from businesses on the platform to compete against those businesses.

Looking Ahead: Whether such conduct harms competition, or whether the antitrust laws are the proper way to address perceived harm, remains controversial. If enacted, the DMA would end the debate in the European Union, empowering the EC to enforce new regulations, backed with substantial fines and other remedial powers. The DSA and DMA will be taken up in the European Parliament and the Council of the European Union before they become law, a process that could take two years.

DIGITAL SERVICES ACT

The draft [Digital Services Act](#) (“DSA”) would update the European Union’s online trade laws, which were last updated more than 20 years ago, to address changes in digital and online services in the intervening years. The draft DSA would introduce new obligations to monitor and filter content appearing on platforms that would apply to all digital services companies that act as intermediaries in connecting consumers with goods, services, and content.

The extent of the obligations will depend on the type of services that the company provides, as well as its user base. For example, different rules will apply to companies that offer intermediary services, hosting services, and online platform services. Online platforms with a particularly large user base, defined as at least 45 million users in the European Union, representing about 10% of the EU population, will also be subject to distinct obligations.

The DSA establishes new obligations on digital services companies to combat certain illegal content that users post on the platform. The DSA rules would empower users to notify the platform of illegal content (e.g., copyright infringement, counterfeit products, hate speech) on their services, require platforms to process notices of illegal content, implement procedures to help trace sellers of illegal goods, and adopt more transparency related to online advertising, such as identifying the person on whose behalf the advertisement is displayed and the parameters used to determine the recipient.

The DSA delegates most enforcement powers to competent EU Member State authorities to be designated by Member States (possibly among existing regulators for telecommunications, media, competition or consumer protection regulators) and with one authority keeping the role of Digital Services Coordinator. However, the EC will have exclusive authority over large online platforms. If implemented, failure to comply with the DSA could result in maximum fines of up to 6% of the company’s worldwide annual income or turnover.

Digital Markets Act

The draft [Digital Markets Act](#) (“DMA”) introduces rules for online platforms that act as “gatekeepers” in the digital sector to prevent those companies from imposing allegedly unfair conditions on businesses and consumers. Examples of potentially covered platforms include providing cloud computing services, online social networking services, video-sharing platform services, and number-independent interpersonal communication services.

In general, the DMA sets forth three qualitative criteria that determine whether a company is a gatekeeper. The DMA also associates each qualitative criteria with financial and/or user base thresholds, which, if met, trigger an obligation to make a filing with the EC within three months of crossing all three of the thresholds.

#	Qualitative Criteria	Filing Presumption
1	The company is an “important online gateway for business to reach end users.”	The company has more than 45 million monthly active end users established or located in the European Union, and had more than 10,000 yearly active business users established in the European Union in the last financial year.
2	The company has a “significant impact on the internal [European Economic Area (“EEA”)] market.”	The company’s annual EEA turnover is at least €6.5 billion or the company’s average market capitalization or fair market value is at least €65 billion, and it provides one of the services concerned in at least three Member States.
3	The company has an “entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future.”	Threshold #2 was met in each of the last three financial years.

Even if a platform company’s operations cross the numerical thresholds above, it may rebut the presumptions by showing that it does not meet the DMA’s qualitative definition of a gatekeeper. Within 60 days of receiving a complete filing, and considering facts and arguments presented by a filer about the DMA’s qualitative thresholds, the EC must release its decision about whether it thinks the filer qualifies as a gatekeeper. A company may seek judicial review of the EC’s gatekeeper determination in the Court of Justice of the European Union.

The DMA also empowers the EC to identify a gatekeeper even if the quantitative filing thresholds are not met. The EC considers criteria such as the size of the provider, entry barriers derived from network effects, and user lock-in.

Qualification as a gatekeeper triggers a series of regulations, and noncompliance risks substantial fines. These obligations include granting smaller rivals access to and interoperability with hardware and software needed to offer their services, and informing the EC of any planned acquisitions in the digital sector, including small acquisitions that would otherwise fall below the EC’s merger review thresholds.

The DMA also would prohibit gatekeepers from engaging in certain conduct that has been or is the subject of EC or Member State investigations. While those investigations remain controversial, the DMA would prohibit gatekeepers from:

- Implementing most-favored-nation (“MFN”) clauses that prevent business users from offering the same products at different prices or conditions through third-party online intermediation services;
- Combining personal data across services without prior consent of the end users;
- Preferencing the gatekeepers’ own products or services over the products or services of competing businesses that also use the platform;
- Using nonpublic data collected from the platform’s business users to compete against those business users; and
- Requiring business users to use the gatekeeper’s identification service.

The DMA empowers the EC to designate which companies are gatekeepers, investigate and sanction violations, develop rules that specify the manner of compliance with certain DMA obligations, and establish additional gatekeeper regulations on top of the rules in the DMA.

If a company fails to comply with the proposed new rules it could face fines of up to 10% of their global annual revenue. In the case of “systematic infringements,” the EC could also impose behavioral or structural remedies, such as divestiture of a whole business or parts of it (e.g., forced sale of business units, assets, intellectual property, or brands). Contrary to the initial draft, the revised DMA would not permit the EC to order structural remedies such as divestitures in the absence of a violation.

NEXT STEPS

The European Parliament and the Council of the European Union will now review and discuss the EC’s proposal, which could result in changes. Both institutions must agree on the final text under qualified majority at the Council before the DSA or DMA take effect. If adopted, the DSA and DMA would become applicable across the European Union, and would not need separate approval in Member States.

GLOBAL REGULATION IS NOT A FOREGONE CONCLUSION

There is not a global consensus about whether regulatory intervention is necessary, or what regulation is warranted. For example, in a speech in February 2019, the Assistant Attorney General (“AAG”) for the U.S. Department of Justice Antitrust Division (“DOJ”) cautioned against “misplaced” and “extreme views” that would propose new rules to regulate online platforms and displace the long-standing global consensus “consumer welfare” standard in antitrust reviews. In a nutshell, under the consumer welfare standard, antitrust enforcers intervene in markets or acquisitions only if the conduct harms consumers in a relevant market.

DOJ noted that digital platforms have grown, in part, because they provide innovative and disruptive services that consumers like. According to DOJ, antitrust enforcement should not concern itself with “how big the platform is, but whether what the platform is doing harms competition.” Although DOJ agreed that concerns over privacy, notice, and unauthorized use of data should be discussed, it discouraged the use of the antitrust laws to address policy issues that do not result in collusive or exclusionary conduct.

FIVE KEY TAKEAWAYS

1. If passed, the DSA will create new obligations on online platform companies to regulate or eliminate certain illegal content posted by users of their services.
2. The DMA would impose new conduct regulations on companies that operate as “gatekeepers” between businesses and consumers. The regulations include access and interoperability obligations, and notifying the EC of acquisitions that do not otherwise meet EC merger thresholds.
3. The DMA also would prohibit gatekeeper online platforms from imposing MFN clauses, combining user data across services without user consent, preferencing their own products, and using data from businesses on the platform to compete against those businesses.
4. In recent years, the EC and Member State antitrust authorities have launched investigations of online platforms alleging that certain conduct above violated the European Union’s abuse of dominance rules. Those theories of harm are controversial and have not been fully tested in the courts. The DMA would circumvent development of EU law in this area and end the discussion.
5. Antitrust authorities in a number of other countries have investigated similar issues in the digital sector, and a harmonized global approach seems unlikely (see our [White Paper](#) on the United Kingdom’s approach). Online platforms or companies that do business with them should consider the impact of these proposed rules given the global nature of many online platforms. In some cases, the “most restrictive” regime may have an outsized and extraterritorial effect.

JONES DAY GLOBAL TEAM AND AUTHORS

United States



Abradat Kamalpour
Partner, Architect
FinAccelerate
San Francisco



Jayant W. Tambe
Partner, Practice Leader
Financial Markets
New York



Brett P. Barragate
Partner, Chair of Americas
Region Financial Markets
Practice
New York



David C. Kiernan
Partner-in-Charge
Northern California
San Francisco/Silicon Valley



Karen P. Hewitt
Partner-in-Charge
California Region
San Diego



Aaron L. Agenbroad
Partner-in-Charge
San Francisco
San Francisco



Ryan J. Andreoli
Partner
New York



David E. Aron
Counsel
Washington



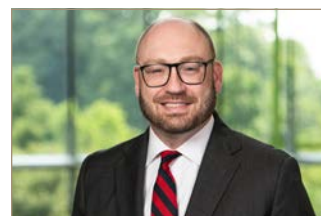
Dean C. Bachus
Partner
Chicago



Bethany K. Biesenthal
Partner
Chicago



Amy Colwell Breslow
Of Counsel
Washington



Nathan S. Brownback
Of Counsel
Washington



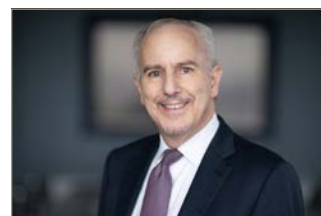
James Burnham
Partner
Washington



Michael R. Butowsky
Of Counsel
New York



Timothy Curry
Partner
Silicon Valley/San Francisco



Richard DeNatale
Partner
San Francisco

JONES DAY GLOBAL TEAM AND AUTHORS

United States



Kimberly A. Desmarais
Partner
New York



Antonio F. Dias
Practice Leader
State Attorney General
Enforcement,
Investigations & Litigation
Miami/Washington



An P. Doan
Partner
Silicon Valley



Laura E. Ellsworth
Partner-in-Charge of
Global Community Service
Initiatives
Pittsburgh



John G. Froemming
Partner
Washington



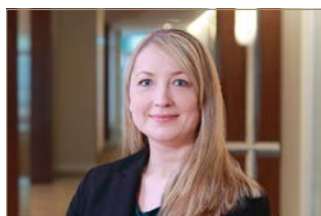
Dorothy N. Giobbe
Of Counsel
New York



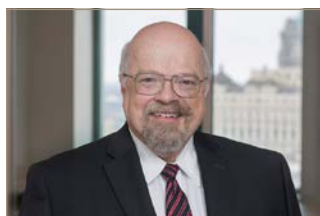
Joseph A. Goldman
Practice Leader Tax
Washington



Harold K. Gordon
Partner
New York



Angela R. Gott
Partner
Cleveland



Gerald M. Griffith
Partner
Chicago/Detroit



David A. Grubman
Partner
Pittsburgh



Michael P. Gurdak
Partner
Washington



Lori Hellkamp
Partner
Washington



Brian Hershman
Partner
Los Angeles



Stephen D. Hibbard
Partner
San Francisco



Kelsey A. Israel-Trummel
Partner
San Francisco

JONES DAY GLOBAL TEAM AND AUTHORS

United States



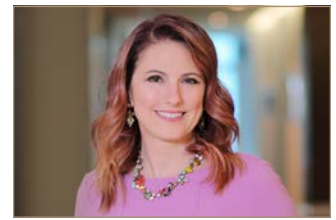
Andrea Weiss Jeffries
Partner
Los Angeles



Jason Jurgens
Partner
New York



Edward T. Kennedy
Practice Leader Tax
New York



Carrie L. Kiedrowski
Partner
Cleveland



Henry Klehm III
Practice Leader
Securities Litigation &
SEC Enforcement
New York



Keith M. Kollmeyer
Partner
Boston



Carl A. Kukkonen III
Partner
San Diego/Silicon Valley



Sarah L. Levine
Partner
Washington



Ka-on Li
Partner
Silicon Valley



Jerry C. Ling
Partner
San Francisco



James P. Loonam
Partner
New York



Margaret I. Lyle
Of Counsel
Dallas



Teresa A. Maloney
Partner
San Francisco



Joan E. McKown
Partner
Washington



Daniel J. McLoon
Practice Leader
Cybersecurity, Privacy &
Data Protection
Los Angeles



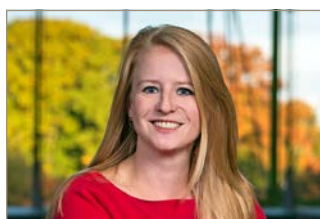
Joseph Melnik
Partner
Silicon Valley

JONES DAY GLOBAL TEAM AND AUTHORS

United States



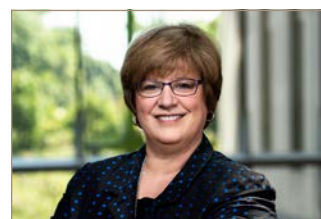
Dennis F. Murphy Jr.
Of Counsel
Cleveland



Lindsey M. Nelson
Partner
Washington



Mahesh V. Parlikad
Partner
New York



Laura S. Pruitt
Partner
Washington



Brian C. Rabbitt
Partner
Washington



Jeff Rabkin
Partner
San Francisco/Silicon Valley



Anna E. Raimer
Partner
Houston



Mark W. Rasmussen
Partner
Dallas



Cameron A. Reese
Partner
San Diego



Lisa M. Ropple
Practice Leader
Cybersecurity, Privacy &
Data Protection
Boston



Schuyler J. Schouten
Partner
Washington



Joseph B. Sconyers
Partner
Boston



Ronald W. Sharpe
Partner
Washington



Howard F. Sidman
Partner
New York



Evan P. Singer
Partner
Dallas



Courtney Lyons Snyder
Partner
Pittsburgh

JONES DAY GLOBAL TEAM AND AUTHORS

United States



Joshua B. Sterling
Partner
Washington



Jennifer L. Swize
Partner
Washington



Emily J. Tait
Partner
Detroit



Craig A. Waldman
Partner, Practice Leader
Antitrust & Competition Law
Washington



Samuel L. Walling
Partner
Minneapolis



Jennifer C. Waryjas
Counsel
Chicago



Meredith M. Wilkes
Partner
Cleveland



Michael J. Wynne
Partner
Chicago



D. Grayson Yeargin
Partner
Washington



Rita J. Yoon
Partner
Chicago



Corey L. Zarse
Partner
Chicago

JONES DAY GLOBAL TEAM AND AUTHORS

EMEA



Bernard E. Amory
Practice Leader
Antitrust & Competition Law
Brussels/London



Eric Barbier de La Serre
Partner
Paris



Renaud Bonnet
Practice Leader
Private Equity
Paris



Charlotte Breuvert
Partner
Brussels



Alban Caillemer du Ferrage
Partner
Paris



Marta Delgado Echevarría
Partner
Madrid



Laurent De Muyter
Partner
Brussels



Yvan Desmedt
Partner-in-Charge
Amsterdam
Amsterdam/Brussels



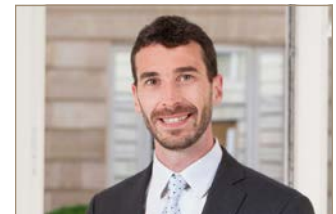
Giles P. Elliott
Partner
London



Leon Ferera
Partner
London



Michael R. Fischer
Partner
Frankfurt



Eduoard Fortunet
Partner
Paris



Marco Frattini
Partner
Milan



Patrizia Gioiosa
Counsel
Milan



Philippe Goutay
Partner
Paris



Michèle Grégoire
Partner
Brussels

JONES DAY GLOBAL TEAM AND AUTHORS

EMEA



Jean-Gabriel Griboul
Partner
Paris



Lewis Grimm
Partner
London



Jakob Guhn
Partner
Düsseldorf



Olivier Haas
Partner
Paris



Jörg Hladjk
Partner
Brussels



Andreas Holzwarth-Rochford
Partner
Frankfurt



Mark Jones
Partner
London



Aidan Lawes
Of Counsel
London



Jonathon Little
Partner
London



Javier López Antón
Partner
Madrid



Heather Martin
Of Counsel
Dubai



Iván Martín-Barbón
Of Counsel
Madrid



Edward J. Nalbantian
Of Counsel
London/Paris



Daniel Partovi
Partner
Dubai



Elizabeth A. Robertson
Of Counsel
London



Natalia Sauszyn
Of Counsel
Paris

JONES DAY GLOBAL TEAM AND AUTHORS

EMEA



Stefan Schneider
Partner
Munich



Sheila L. Shadmand
Partner-in-Charge Middle
East/Africa Region
Dubai



Patrick G. Stafford
Practice Leader
Private Equity
London



Rebecca Swindells
Partner
London



Mario Todino
Partner
Brussels



Alexandre G. Verheyden
Partner-in-Charge Brussels
Brussels



Undine von Diemar
Partner
Munich



Philipp Werner
Partner
Brussels



Nick Wittek
Partner
Frankfurt

JONES DAY GLOBAL TEAM AND AUTHORS

Asia/Pacific



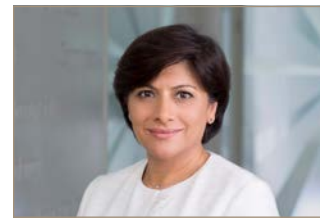
Jennifer Chambers
Partner
Sydney



Joanne M. Dwyer
Of Counsel
Brisbane



Haifeng Huang
Partner
Hong Kong/Beijing



Sushma Jobanputra
Partner-in-Charge Singapore
Singapore



Tim L'Estrange
Partner
Melbourne/Sydney



Daniel Moloney
Partner
Melbourne



Holly Sara
Partner
Sydney



Hemang Shah
Partner
Sydney



Wilson L.K. Sung
Of Counsel
Hong Kong



Evan J. Sylwestrzak
Of Counsel
Perth



Isaac West
Partner
Brisbane



Lucas Wilk
Partner
Perth

JONES DAY GLOBAL TEAM AND AUTHORS

Latin America



Artur Badra
Of Counsel
São Paulo/Madrid



Guillermo Larrea
Of Counsel
Mexico City



Luis Riesgo
Partner-in-Charge
Spain/Latin America Region
São Paulo

Additional Jones Day Authors and Contributors

Arjun Singh Ahuja
Associate
Irvine

Anthony J. DeRiso III
Associate
New York

David A. Feirstein
Associate
Irvine

Céalagh P. Fitzpatrick
Associate
New York

Jonathan D. Guynn
Associate
Dallas

Nick McCauslin
Associate
Cleveland

Dennis F. Murphy Jr.
Associate
San Francisco

Jareli Reynoso Gutierrez
Associate
Silicon Valley

Grace E.K. Rouser
Associate
Minneapolis

Elijah C. Stone
Associate
Dallas

Michaela Yip
Associate
Atlanta

Anthony J. Bautista
Associate
Los Angeles

Amanda L. Dollinger
Associate
New York

Parker J. Feldman
Associate
Detroit

Cameron J. Gable
Associate
San Diego

Robert Levent Hergüner
Associate
Washington

Megan L. McKeown
Associate
Houston

Graziella Pastor
Associate
New York

Diane Richebourg
Associate
Paris

Rebecca C. Searle
Associate
Houston

Collin L. Waring
Associate
Dallas

Ryan D. Class
Associate
Boston

Casey Duckworth
Associate
San Diego

Tyler Fields
Associate
Los Angeles

Olga Gidalevitz Ph.D.
Associate
Chicago

Max Kober
Associate
Munich

Hannah Mehrle
Associate
Cleveland

Fernando Pastore
Associate
São Paulo

Oliver D. Roberts
Associate
Dallas

Gurneet Singh
Associate
Silicon Valley

Brittany Wiegand
Associate
Chicago

Seth Cleary
Associate
Dallas

Monique Eloi
Associate
Miami

Michael G. Fischer
Associate
Washington

Gerry R. Griffith
Associate
Dallas

Christina Mastrucci Lehn
Associate
Miami

Walter A. Mostowy
Associate
Silicon Valley

John Paul Putney
Associate
Pittsburgh

Rita M. Rochford
Associate
Cleveland

Charles Smith
Associate
Paris

Kevin Han Yang
Associate
Silicon Valley



www.finaccelerate.com | finaccelerate@jonesday.com

Jones Day publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our website at www.jonesday.com. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.