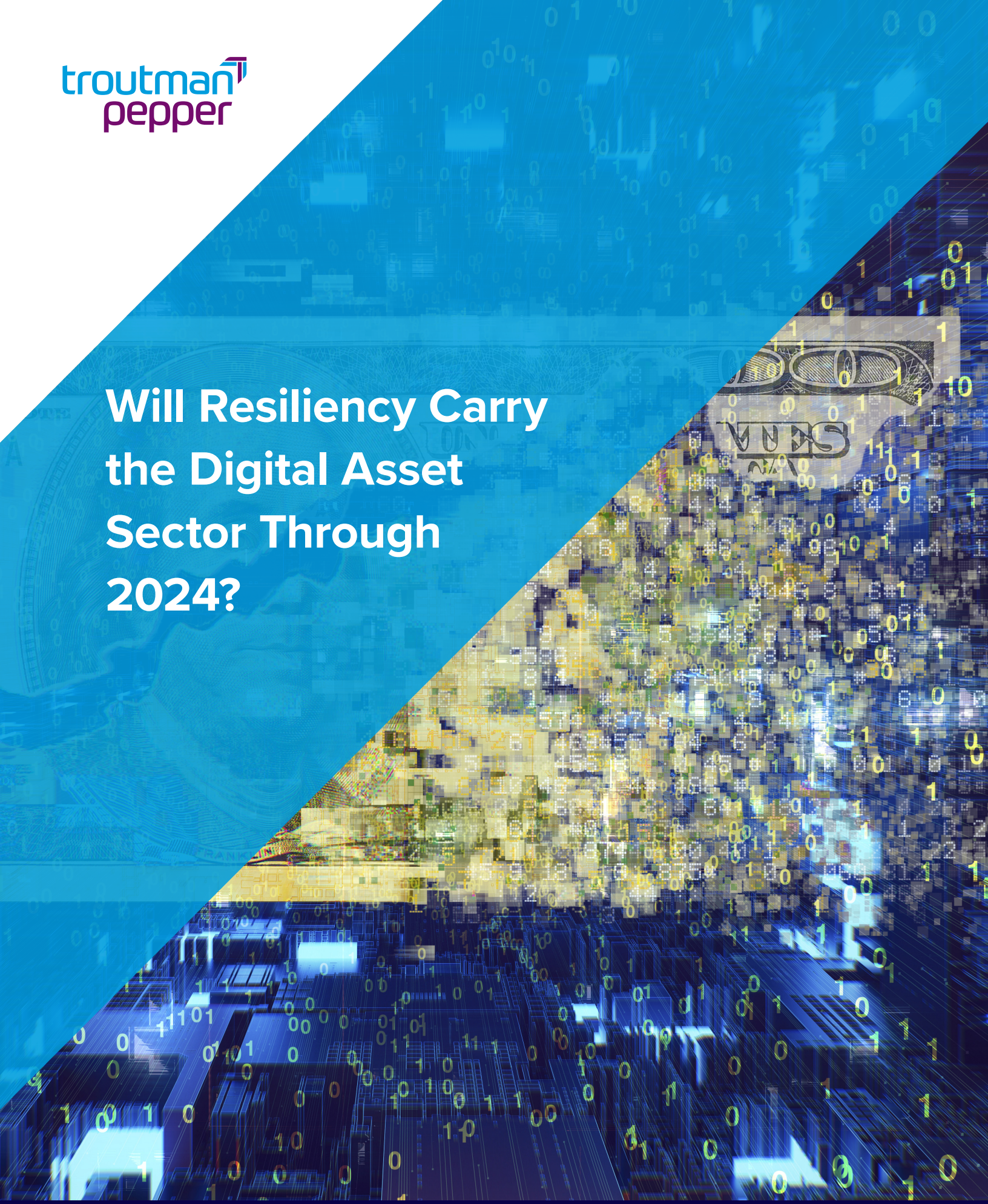
troutman pepper

Will Resiliency Carry the Digital Asset Sector Through 2024?



troutman.com

Will Resiliency Carry the Digital Asset Sector Through 2024?

Introduction

If 2022 was "The Year of Turmoil," then the digital asset industry experienced "The Year of Resiliency" during 2023. Amidst cataclysmic events such as the bankruptcy-driven dissolutions of several digital asset financial services companies, various bank failures, the criminal trial of FTX's ex-CEO Sam Bankman-Fried, and the U.S. government's imposition of a $4.7 billion fine against Binance, the world's largest digital asset exchange, the digital asset market did not falter. Instead, it has recaptured more than 50% of the market capitalization it lost during 2022, pushing that figure to $2.59 trillion, which is only $0.41 trillion less than its all-time high market capitalization value of $3 trillion achieved during November 2021. Although fiscal stability is a pragmatic metric, the digital asset industry's staying power is better evidenced by the increased regulatory activity of the state legislatures and the federal agencies.

Following the footsteps of New York, California and Louisiana enacted comprehensive digital asset licensing frameworks during 2023. At the federal level, Congress introduced several digital asset-related bills, but none have been enacted. Even so, 2023 was an eventful year for the Federal Reserve, which released numerous guidance documents related to digital assets and published a whitepaper on the potential impact of tokenization, signifying the Fed's possible change of heart towards the future integration of digital assets and distributed ledger technology (DLT) into the traditional financial system.

Yet, 2024 is an election year. Whether Congress's legislative inaction will cease or continue will, in some part, depend on the outcome of this event. Many believe federal guardrails are critical to propelling the digital asset industry from the "Wild Wild West" to the "Land of Legitimization," but clearly state legislatures do not intend to wait for Congress. While they have continuously pressed forward, they have often proposed legislation that adopts a federal framework we anticipate will continue to be used by the plaintiffs' bar to rectify digital asset-related consumer harm: the Electronic Fund Transfer Act and Regulation E. This, coupled with the Consumer Financial Protection Bureau's ostensible bid to regulate the digital asset market through its recently finalized Larger Participant Rulemaking for General-Use Digital Consumer Payment Applications, should make the remainder of 2024 and beyond an interesting time.

In this issue

Federal Regulatory Action

Federal Reserve Board of Governors, Federal Deposit Insurance Corporation, and Office of the Comptroller of Currency

Joint Statement on Crypto-Asset Risks to Banking Organizations

On January 3, 2023, the Office of the Comptroller of Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Federal Reserve Board of Governors (Fed) released a Joint Statement on Crypto-Asset Risks to Banking Organizations. Published just two months after the collapse of FTX during November 2022, the immediacy of the statement signified the Fed's continuing aspiration to maintain a clear line of separation between the digital asset financial services sector and the U.S. banking system. Although the statement articulated that "[b]anking organizations are neither prohibited nor discouraged from providing banking services to customers of any specific class or type," within the same paragraph, it implicitly rejected that directive and clarified that the "[Fed, OCC, and FDIC believe] 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."

Federal Reserve Board of Governors

Policy Statement on Section 9(13) of the Federal Reserve Act

On January 27, 2023, the Fed redirected its attention from national banks (which are chartered and regulated by the OCC) to state member banks by issuing a Policy Statement on Section 9(13) of the Federal Reserve Act. The statement revealed the Fed's adoption of a rebuttable presumption that the activities a state member bank may engage in are limited to only those activities that a national bank may engage in as principal, unless otherwise authorized by federal statute or Part 362 of the FDIC's regulations. By design, the statement focused on the permissibility of certain "crypto-asset-related activities" and informed state member banks of the expectation to analyze "federal statutes, OCC regulations, and OCC interpretations to determine whether an activity is permissible for national banks." If neither existing OCC nor FDIC regulations permit a state member bank to engage as principal in a certain activity, then the state member bank may seek approval from the Fed under §208.3(d)(2) of Regulation H. In this situation, a state member bank may rebut the presumption if it provides a clear and compelling rationale for the need to engage in the proposed activity and provides robust plans for managing the risks of the proposed activity in accordance with principles of safety and soundness.

Presently, state member banks seeking to hold digital assets as principal face a seemingly insurmountable burden of persuasion, considering the Fed "has not identified any authority permitting national banks to hold most crypto-assets, including bitcoin and ether," and believes that "issuing tokens on open, public, and/or decentralized networks, or similar systems is highly likely to be inconsistent with safe and sound banking practices." Interestingly, the Fed acknowledged that the policy statement does not prohibit a state member bank from providing digital asset custodial services so long as the state member bank provides that service in a safe and sound manner and in compliance with all applicable laws, including law related to anti-money laundering (AML) and combatting the financing of terrorism (CFT).

Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities

On February 23, 2023, the Fed, the OCC, and the FDIC issued a Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities. In complete alignment with the Fed's policy statement, the liquidity statement highlighted the Fed's logical concern that a bank with a high concentration of demand deposits largely consisting of digital assets may be susceptible to heightened liquidity risks. Digital asset stakeholders often tout fluidity and expedience as positive factors that distinguish DLT from the traditional banking system. However, as the Fed noted, a system that provides for seamless inflows and outflows of liquidity can be a gift and a curse. The "double-edged sword" dynamic of this issue is aptly evidenced by the ensuing collapses of Signature Bank and Silicon Valley Bank, two digital asset-friendly national banks that witnessed a combined $63.1 billion in net deposit outflows during March 2023. According to the FDIC, during the final hours of March 10, 2023 alone, Signature Bank experienced a pronounced run on deposits totaling $18.6 billion. The instantaneous settlement functionality of digital assets was not the direct cause of these bank runs, but rather, a proximate cause as surging inflation and devaluation of Treasury bonds (which the affected banks had to sell at steep losses to raise cash to pay their depositors) acted as the principal catalysts.

To mitigate the risks associated with maintaining deposit accounts for digital asset-related entities, the liquidity statement enumerates several risk management practices that banks may integrate into their existing business models: (1) assessing potential concentration or interconnectedness across deposits from digital asset financial services companies and any associated liquidity risks; (2) incorporating the liquidity risks or funding volatility associated with deposits received from digital asset financial services companies into contingency funding planning, including liquidity stress testing; and (3) performing robust due diligence and ongoing monitoring of digital asset financial services companies that establish deposit accounts, which should include assessing any representations by those digital asset financial services companies to their end customers.

Novel Activities Supervision Program

On August 8, 2023, the Fed announced the creation of its Novel Activities Supervision Program. The program is essentially a supervisory risk-assessment tool of the Fed, geared towards monitoring several activities conducted by banks subject to the Fed's supervision. These activities include: (1) bank-fintech partnerships in which a fintech provides end users with automated access to a bank's infrastructure; (2) general digital asset-related activities, which may include trading, lending, custodial services, and stablecoin issuance; (3) tokenization of securities or other asset classes; and (4) banks that are concentrated in providing traditional banking services to digital asset financial services companies. Under the program, the Fed intends to provide written notice to banking organizations whose novel activities will be subject to examination.

Supervisory Nonobjection Process for State Member Banks Seeking to Engage in Certain Activities Involving Dollar Tokens

Also on August 8, 2023, the Fed expanded on its discussion of permissible state member bank activities in a Supervisory Nonobjection Process for State Member Banks Seeking to Engage in Certain Activities Involving Dollar Tokens. The dollar token statement announced the Fed's development of a process for state member banks, which are permitted to engage in any activities

that national banks are permitted to engage in, to obtain supervisory nonobjection letters from the Fed to issue, hold, transact, or facilitate payments of dollar tokens, which the Fed defined as "tokens denominated in national currencies and issued using distributed ledger technology or similar technologies to facilitate payments." (Stablecoins).

Under the OCC's Interpretive Letter 1174, a national bank may use stablecoins to perform bank-permissible functions, such as payment activities. Therefore, in accordance with the Fed policy discussed earlier, state member banks can also engage in this activity. However, the dollar token statement clarified that state member banks must perform certain tasks before engaging in stablecoin-related activities: (1) provide notice to its lead supervisory point of contact at the Fed of the bank's intention to engage in a stablecoin-related activity; (2) describe the stablecoin-related activity the bank intends to engage in; and (3) demonstrate that the bank has established appropriate risk management practices for the proposed stablecoin-related activity. In reviewing a state member bank's request for a nonobjection letter, the Fed will focus on operational risks, cybersecurity risks, liquidity risks, illicit finance risks, and consumer compliance risks.

Tokenization: Overview and Financial Stability Implications

On September 26, 2023, the Fed released its final digital asset-related publication of the year and examined a functionality of DLT that will likely play an important role in the digital asset industry's quest to surmount the frequent criticisms it has weathered over the years: tokenization. At the root level, a digital asset is encrypted data within a DLT-based system. In practice, when Individual A transfers a digital asset to Individual B—whether a stablecoin, Bitcoin, or an NFT—Individual A is merely relinquishing his or her right of ownership to that digital asset. In this process, the transferred digital asset does not traverse a DLT and magically find its way into the digital wallet of Individual B. Instead, the validators responsible for maintaining the DLT's transaction history modify the DLT's ledger to reflect that Individual B is the current owner of the transferred digital asset. DLT serves as the rails of the digital asset industry. It effectuates instantaneous transference and settlement of encrypted data. But data, in the form of ownership, can manifest in a variety of ways: (1) right of ownership to an equity; (2) right of ownership to real estate; (3) right of ownership to a Picasso painting; (4) right of ownership to musical royalties; and (5) right of ownership to a demand deposit maintained by a banking institution. Through conversion of these "rights of ownership" into irreplicable, digitized forms of encrypted data that can be freely transferred and received, asset classes that would otherwise remain illiquid and hampered by transactional friction will become viable stores of value and mediums of exchange for consumers and institutions alike. This is one area where tokenization truly shines.

Although it is a revolutionary concept, tokenization is still very nascent and the risks it poses to the stability of the traditional financial system must be considered. In this paper, the Fed is primarily concerned with runs on issuers of tokenized assets. For example, if a digital asset financial services company offers consumers tokenized gold backed by physical gold bullion that consumers may redeem in exchange for tokenized gold, issues of under-collaterization could arise leading to a situation in which the digital asset company does not have enough gold bullion on hand to meet redemption requests. Further, considering that digital asset markets never close, the Fed is concerned that timing mismatches in trading hours may lead to stress events.

Commercial Bank Examination Manual

During October 2023, the Fed amended its Commercial Bank Examination Manual to include Section 5330.1, which provides an overview of the digital asset-related activities of state member banks. The purpose of this section is to: (1) clarify the supervisory expectations regarding the notification of engagement in digital asset-related activities; (2) discuss legal permissibility concerns associated with a state member bank's engagement in digital asset-related activities; (3) describe the supervisory nonobjection process for state member banks seeking to engage in certain activities involving stablecoins; (4) discuss statements on digital asset-related risks to banking organizations; and (5) outline supervisory

considerations in assessing state member banks engaged in digital asset-related activities. Notably, this section contains summaries of the statements and novel activities program discussed above.

Federal Deposit Insurance Corporation

Throughout 2023, the FDIC frequently issued cease-and-desist letters to digital asset financial services companies that published advertisements implying that either the companies themselves were FDIC-insured or that digital assets maintained on their platforms were FDIC-insured. Importantly, based on the cease-and-desist letters, it appears the FDIC has adopted the position that any unqualified statement regarding FDIC deposit insurance — irrespective of its legitimacy — will constitute a false or misleading statement in violation of § 18(a)(4) of the Federal Deposit Insurance Act (FDI Act).

For example, the FDIC concluded that the following advertisement listed on the webpage of a digital asset financial services company was misleading in violation of the FDI Act:

> "U.S. Dollars held in your . . . fiat currency wallet are FDIC-insured up to $250,000 per account."

Although this representation is technically true in the sense that, if applicable, FDIC deposit insurance only applies to U.S. dollars and not digital assets, the statement is misleading to consumers because it does not clarify that: (1) the digital asset financial services company is not a "insured depository institution" as defined by the FDI Act; (2) the consumer's U.S. dollar balances at issue are being held in accounts maintained by an insured depository institution; and (3) the insured depository institution in which the digital asset financial services company has partnered with to offer its account product is the only institution that can provide consumers access to FDIC deposit insurance.

In another cease-and-desist notice the FDIC issued to a digital asset financial services company, the FDIC expressly noted that "[f]ailure to identify the [insured depository institutions] into which customers' funds will be deposited is . . . a material omission pursuant to 12 C.F.R. § 328.102(b)(5)."

If a digital asset financial services company publishes statements that violate § 18(a)(4) of the FDI Act, the FDIC will require the company to remove any statements that suggest the company is: (1) FDIC-insured; (2) digital assets are protected by FDIC deposit insurance; and/or (3) FDIC deposit insurance provides more than $250,000 in account protection. For statements related to "pass-through insurance" in which a digital asset financial services company partners with an insured depository institution to provide a checking account to its customers, the FDIC requires digital asset financial services companies to: (1) clearly and accurately identify the nature of the insurance being offered; and (2) identify the insured depository institution with which the company has a direct or indirect relationship for the placement of consumer deposits.

Looking Ahead

The FDI Act is clear: entities that are not insured depository institutions may not "represent or imply that any deposit liability, obligation, certificate, or share is insured by the [FDIC], if such deposit liability, obligation, certificate, or share is not insured or guaranteed by the [FDIC]." Digital asset financial services companies publish advertisements related to FDIC deposit insurance when offering a checking account product that is issued through an insured depository institution. In these instances, digital asset financial services companies should ensure that their marketing materials conspicuously clarify that they cannot provide FDIC deposit insurance, and instead, that consumers' accounts are FDIC-insured through their banking partners, which are insured depository institutions.

U.S. Department of the Treasury

Illicit Finance Risk Assessment of Decentralized Finance

On April 6, 2023, the U.S. Department of the Treasury (Treasury) published its first-ever DeFi Illicit Finance Risk Assessment, which explores how decentralized finance (DeFi) protocols may be used to "transfer[] and launder[] . . . illicit proceeds" by "exploiting vulnerabilities in the U.S. and foreign AML/CFT regulatory, supervisory, and enforcement regimes." The Treasury is concerned with the

lack of compliance with AML/CFT and sanctions obligations amongst DeFi protocols, which, in the Treasury's view, leads to a host of foreseeable consequences such as increased instances of untraceable criminal trafficking, ransomware attacks, garden-variety theft, and sophisticated scams. Notwithstanding these issues, in our view, the Treasury used the assessment to explain that even if a protocol is truly decentralized, the Bank Secrecy Act (BSA) imposes AML/CFT obligations on any entity that functions as a "financial institution" as defined in 31 U.S.C. § 5312(a)(2). Further, considering the cross-border nature and pseudonymity involved in blockchain transactions, the Treasury posits that "disintermediated" DeFi protocols, or DeFi protocols that fall outside the scope of the BSA's definition of "financial institution," are unlikely to choose to comply with existing U.S.-based AML/CFT obligations given the minimal implementation of AML/CFT standards on the international stage.

The Treasury acknowledges that lack of AML/CFT compliance can (and has been) somewhat curtailed by the importance of centralized fiat on- and off-ramps like digital asset exchanges. Presently, most merchants do not accept digital assets as a form of payment, so DeFi users must exchange their digital assets for fiat currency through an AML/CFT compliant intermediary to access the value of their holdings. Once a user's digital asset wallet address becomes linked to a platform that possesses Know-Your-Customer information associated with the user, the user's DeFi-related transactions become traceable due to the termination of pseudonymity. But if centralized entities fail to comply with AML/CFT obligations or do so in subpar fashion, this mitigation measure becomes much less effective. Interestingly, the Treasury gave an implicit nod to "zero knowledge proofs" to advance its goal of identifying otherwise anonymous transactions while preserving user privacy. Zero-knowledge proofs would permit a user of a DeFi protocol to verify some aspect of his or her identity (i.e., age, citizenship, credit score, sanctioned address, etc.) without divulging the information usually necessary to establish the truth of those identifiers. "Are you a U.S. citizen?" "Here, scan my government-approved QR code to find out." Through this innovation, the Treasury could theoretically monitor blockchain transactions for indicia of criminality without limitation.

Looking Ahead

It should come as no surprise that the Treasury believes the current AML/CFT regulatory framework is the "foundational mitigation measure to address illicit finance risks associated with DeFi services that are operating in the United States." This is because, for an agency whose mission is to safeguard the U.S.' economy from illicit actors, identity verification is paramount in the pseudonymous environments upon which DLT is built. Considering the assessment, creators of DeFi protocols should ensure they truly understand the Treasury's position: those engaged in activity covered by the BSA have AML/CFT obligations and all those subject to U.S. jurisdictions have sanctions compliance obligations, regardless of whether they meet the BSA's definition of "financial institution" and/or are truly decentralized.

Financial Crimes Enforcement Network

Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern

On October 19, 2023, FinCEN issued a Notice of Proposed Rulemaking (NPRM) that would require domestic financial institutions to conduct additional recordkeeping and reporting activities to monitor transactions that are reasonably suspected to involve convertible virtual currency (CVC) mixing.

The NPRM is a byproduct of FinCEN's first-ever usage of its Section 311 authority under the USA PATRIOT Act to designate an entire class of transactions within, or outside of, the United States as a primary money laundering concern. Under Section 311, FinCEN has the authority to require any domestic financial institution to maintain records and file reports regarding any transaction class that FinCEN deems to be a primary money laundering concern.

The activity that fueled the NPRM is CVC mixing, which FinCEN defines in relevant part as "the facilitation of CVC transactions in a manner that obfuscates the source, destination, or amount involved in one or more transactions . . . ." At their core, all DLT-based systems are no different than any centralized accounting system used today. Both

systems are capable of recording debits, credits, and overall account balances of varying asset classes to ensure that fraudulent transactions do not occur on a given network. This process is known as double-entry accounting. However, unlike double-entry accounting which only involves separate retention of credits and debits, DLT-based systems augment traditional accounting practices by generating a single encrypted data structure that is comprised of both the credit and debit information of any given transaction. This is referred to as triple-entry accounting. DLT-based systems create an interlocking network of permanent accounting entries, which, for example, could unveil any transactions involving digital wallet addresses listed on the Office of Foreign Asset Control's (OFAC) Sanctioned Designated National List (SDN List). Individuals engaging in such activities rely on CVC mixers to prevent the underlying network from generating a record that tethers a specific debit to a specific credit.

The NPRM's Reporting and Recordkeeping Requirements

If adopted, the NPRM would require "covered financial institutions," a definition that is inclusive of banks, broker-dealers, and money service businesses, to collect certain information:

- The amount of any CVC transferred, in both CVC and its U.S. dollar equivalent when the transaction was initiated;
- CVC type;
- The CVC mixer used, if known;
- The CVC wallet address associated with the customer;
- Transaction hash;
- Date of transaction;
- IP addresses and time stamps associated with the covered transaction;
- Narrative;
- Customer's full name;
- Customer's date of birth;
- Address;
- Email address associated with any and all accounts from which or to which the CVC was transferred; and
- The customer's IRS Taxpayer Identification Number.

Covered financial institutions would be required to collect, maintain, and report the aforementioned information to FinCEN within 30 calendar days of initial detection.

Exempted Activities under the NPRM

The NPRM contains two notable exemptions that covered financial institutions should consider. First, excluded from the term "CVC mixing" is the usage of an internal protocol by covered financial institutions to execute non-CVC-based ancillary transactions that would otherwise contribute to the overall execution of a transaction involving CVC mixing. For example, if a customer uses a bank's services to convert illicitly obtained digital assets to fiat currency, the bank would not be required to report the fiat currency transaction under the NPRM. Second, the NPRM only requires covered financial institutions to report information that is in their possession. In other words, the NPRM does not require covered financial institutions to solicit transactional counterparties to obtain information unknown to them.

Looking Ahead

FinCEN's issuance of the NPRM is unprecedented as it marks the first time the agency has ever utilized its Section 311 authority to classify a class of international transactions as a primary money laundering concern. The fact that FinCEN has designated transactions involving CVC mixing as the relevant transaction class magnifies its concern that mass adoption of CVC mixing by illicit foreign actors has the potential to perpetuate bouts of unidentifiable criminal activity, placing the United States in a precarious situation from a national security perspective. The comment period for the NPRM ended on January 22, 2024, and as of this writing, FinCEN has not yet issued a final rule. Nevertheless, covered financial institutions that facilitate CVC transactions should assess their existing AML/CTF programs to determine whether their programs are presently capable of capturing CVC transactions with indicia of CVC mixing.

Office of Foreign Assets Control (OFAC)

Binance Holdings, Ltd. (Binance)

In a year marked by increased scrutiny and regulation of digital assets, one of the most significant developments was the settlement reached between Binance, the world's largest digital asset exchange, and OFAC. On November 21, 2023, in a landmark enforcement action, Binance was found to have processed transactions worth approximately $706 million in violation of various regulations and sanctions programs between August 2017 and October 2022. The settlement, amounting to over $968 million, is a stark reminder of the potential civil and criminal liabilities that can arise from non-compliance with existing financial services laws. We note that FinCEN also entered a consent order with Binance for failing to implement an affective AML program, inadequate filings of suspicious activity reports, and failing to register as a money services business in violation of the BSA. For these alleged violations, FinCEN imposed a civil money penalty of $3.4 billion on Binance.

OFAC's investigation revealed that Binance knowingly retained users from both the United States and sanctioned jurisdictions on its platform, with inadequate controls in place to prevent those users from trading with users in sanctioned countries and blocked persons. Despite being aware of the applicability of U.S. sanctions to trades in which Binance matched U.S. and sanctioned jurisdiction users as counterparties, Binance continued to allow such trades. This conduct was reflected in the statements of senior executives at the highest levels of the company, including the CEO and the then CCO.

In addition, Binance was found to have misrepresented its sanctions controls and its commitment to compliance to third parties in private communications, and to the public through actions such as issuing misleading terms of use and by removing references to sanctioned countries from its website while it instead continued to serve them. The encouragement for VPN usage was also evident, subtly permitting users from the U.S. and other sanctioned jurisdictions to engage in trading, despite their apparent prohibition.

As part of its settlement, Binance agreed to undertake certain compliance commitments, including retaining a monitor for five years to evaluate the effectiveness of its policies, procedures, and internal controls in relation to U.S. sanctions laws. This case serves as a potent reminder for all digital asset service providers of the importance of robust compliance systems. The Binance case also highlights the role of whistleblowers in uncovering non-compliance. Whistleblower incentive programs likely played a key role in bringing Binance's violations to light, as demonstrated by the CFTC's recent "Notice of Covered Action" allowing for the submission of award claims by individuals who provided the CFTC with original information after July 21, 2010 that led to the Binance enforcement action. This underscores the importance of companies having effective internal reporting mechanisms, and creating a culture where employees feel safe to report potential violations.

CoinList Markets LLC

Following the significant enforcement action against Binance, another noteworthy case emerged in the digital asset space involving CoinList Markets LLC (CLM), a California-based virtual currency exchange. This case, like the Binance case, highlights the critical importance of compliance with U.S. economic sanctions.

The investigation revealed that despite CLM having maintained several sanctions compliance measures, including screening new and existing customers, conducting transactional monitoring, using blockchain analytics tools to identify transactions involving high-risk jurisdictions and sanctioned wallet addresses, and implementing controls to deny access to users with IP addresses in sanctioned jurisdictions, CLM's screening procedures still failed to capture users located in Crimea. These users even provided addresses that either specified a city in "Crimea" or used the word "Crimea," but had listed their country of residence as "Russia."

As part of the $1.2 million settlement, CLM agreed to undertake certain compliance commitments, including updating its settings to automatically reject potential users who report a residential address

with a Crimean city, implementing IP geo-blocking to detect IP addresses in sanctioned jurisdictions and prevent users from accessing their accounts from those IP addresses, investing in new vendors for review and verification of identity documents and restricted party screening and tools to detect the use of VPNs that can obscure users' location, and enhancing its training program and hiring additional experienced compliance personnel.

Sinbad.io

On November 29, 2023, OFAC sanctioned digital asset mixer Sinbad.io for allegedly serving as a "key money-laundering tool" of the OFAC-designated Lazarus Group, which is a state-sponsored cyber hacking group of the Democratic People's Republic of Korea (DRPK). According to OFAC, Sinbad.io acted as a "preferred" digital asset mixer and facilitated the laundering of approximately $900 million in three heists orchestrated by the Lazarus Group during 2022 and 2023. OFAC sanctioned Sinbad.io pursuant to its authority under Executive Order 13694, as amended by Executive Order 13757, as having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat of national security, amongst other things.

Looking Ahead

These OFAC enforcement actions highlight the continued emphasis on the need for businesses engaged in virtual currencies and novel technologies to incorporate a risk-based sanctions compliance strategy into their operational framework, especially when their objective is to deliver financial services to a global customer base. This approach should be founded on and include the five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training. Postponing the development and execution of a sanctions compliance program can subject companies to a broad spectrum of potential sanctions risks, including significant financial penalties like those seen in 2023.

Consumer Financial Protection Bureau

Larger Participant Rule

On November 17, 2023, the Consumer Financial Protection Bureau (CFPB or Bureau) published its proposed rule to define a market for general-use digital consumer payment applications. Arguably, the proposed rule was the most significant DLT-related regulatory development of 2023 as, among other things, it marks the CFPB's first official attempt to bring the digital asset industry within the scope of its supervisory authority under the Consumer Financial Protection Act (CFPA). By the same token, the proposed rule also expressly addresses a key, undefined term that appears in several definitions of "consumer financial products or services" throughout the CFPA: "funds." The Bureau contends that this term "is not limited to fiat currency or legal tender, and includes digital assets that have monetary value and are readily usable for financial purposes." Although it's better than not having any definition at all, the Bureau's definition of "funds" is ambiguous and ostensibly broad in scope as it also encompasses "crypto-assets" generally. Nevertheless, the Bureau's definition aligns with the current sentiment of courts that have addressed this issue. Analyzing the EFTA and Regulation E, each of which similarly do not define the term "funds," courts have applied the ordinary meaning of that term. See *Rider v. Uphold HQ Inc.*, 657 F. Supp. 3d 491, 498 (S.D.N.Y. 2023) ("Under its ordinary meaning, the term 'cryptocurrency' means a digital form of liquid, monetary assets that constitute 'funds' under the EFTA."); *Nero v. Uphold HQ Inc.*, No. 22CV1602 (DLC), 2023 WL 5426203, at *5 (S.D.N.Y. Aug. 23, 2023) ("The definition of 'electronic fund transfer' contains no constraint that would limit the EFTA's coverage to fiat currencies . . . the statute is written broadly. Its terms, when properly construed, cover the electronic transfer of funds such as cryptocurrency.").

If the proposed rule is finalized in its current form, stakeholders operating in some, but not all, sectors of the digital asset industry will become subject to the Bureau's supervisory authority. Therefore, the question digital asset market participants should be asking themselves is "Where are the exclusions?"

Overview of the Bureau's Larger Participant Rulemaking Authority

The CFPA mainly limits the Bureau's application of its supervisory and enforcement powers to a "covered person," a term that is defined as "any person that engages in offering or providing a consumer financial product or service . . . and any affiliate of a person . . . if such affiliate acts as a service provider to [the covered person]." With respect to nondepository covered persons (hereinafter, nonbank covered persons), the applicable class of persons identified by the proposed rule, § 1024 of the CFPA generally defines these persons as anyone who "offers or provides origination, brokerage, or servicing of loans secured by real estate for use by consumers primarily for personal, family, or household purposes, or loan modification or foreclosure relief services in connection with such loans . . . ." Nevertheless, this same section contains a discretionary rulemaking pathway for the Bureau to extend its supervisory powers to certain nonbank covered persons that are "larger participant[s] of a market for other consumer financial products or services . . . ." Herein lies the Bureau's Larger Participant Rulemaking Authority.

Since 2012, the Bureau has leveraged its Larger Participant Rulemaking Authority to subject a few very important consumer-facing markets to its supervisory powers: (1) consumer reporting market; (2) consumer debt collection market; (3) student loan servicing market; (4) international money transfer market; and (5) indirect auto finance market.

Through its supervisory authority, the Bureau periodically examines applicable entities to assess their compliance with federal consumer financial law, review their compliance management systems, and to detect risks to consumers and markets for consumer financial products and services.

Elements of the Proposed Rule

Market Defined. The proposed rule applies to nonbank covered persons who are larger participants in a market for general-use digital consumer payment applications. The proposed rule defines this market as providing a covered payment functionality through a digital application for consumers' general use in making consumer payment transactions. Larger participant, covered payment functionality, and consumer payment transactions are the operative terms of the proposed rule.

Larger Participant Defined. A nonbank covered person will be a larger participant in the market for general-use digital consumer payment applications if: (1) it facilitates an annual covered consumer payment transaction volume of at least 5 million transactions; and (2) it is not a small business concern based on applicable SBA size standards. If a nonbank covered person is deemed a larger participant, it will remain a larger participant until two years from the first day of the tax year in which the person last met the larger-participant test. As to the 5 million transactions threshold, the Bureau will measure this by assessing the annual volume of both consumer-to-consumer or consumer-to-business transactions facilitated by all general use-digital consumer payment applications provided by the nonbank covered person and its affiliated companies in the preceding year.

Consumer Payment Transaction Defined. This term refers to the: (1) transfer of funds; (2) by or on behalf of a consumer; (3) physically located in a state; (4) to another person; (5) primarily for personal, family, or household purposes. According to the Bureau, the first element of this definition requires sending a payment and does not focus on the receipt of a payment. Further, the fourth element of this definition requires that the transfer of funds be made to another person besides the consumer. Potential transferees may include another consumer, a business, or some other type of entity.

Covered Payment Functionality Defined. This term incorporates two additional defined terms: (1) funds transfer functionality; and (2) wallet functionality. A nonbank covered person will be subject to the proposed rule whether it engages in activities that implicate only one, or both, of these functionalities. Notably, the proposed rule clarifies that both functionalities are consumer financial products or services under the CFPA.

The term funds transfer functionality refers to a nonbank covered person's: (1) receipt of funds for the purpose of transmitting them; or (2) its acceptance and transmission of payment

instructions received from a consumer. In the digital asset industry, digital asset exchanges frequently perform both functionalities by either maintaining a consumer's deposit of digital assets on its platform or facilitating the transmission of a consumer's digital assets from its platform to another digital wallet existing outside of its platform. Here, it would be imperative for the digital asset exchange to have procedures in place to contemporaneously determine whether the transferee of any given transaction is a person distinct from the transferor-consumer. But, as noted above, in the event a consumer utilizes a digital asset exchange's platform to send digital assets to a digital wallet owned by the same consumer, the proposed rule would not apply because the transaction would not be a consumer payment transaction.

The term wallet functionality refers to a product or service that: (1) stores account or payment credentials, including in encrypted or tokenized forms; and (2) transmits, routes, or otherwise processes stored account or payment credentials to facilitate a consumer payment transaction. The Bureau's usage of digital asset industry buzzwords like "tokenization" may lead some to believe that digital asset wallets like MetaMask and Trust Wallet would constitute a product subjected to the proposed rule. Here however, tokenization refers to the replacement of a consumer's credit or debit card number with encrypted token credentials that facilitate the secure transfer of payment data to a merchant. As the Bureau noted, the "first prong would be satisfied by storing an encrypted version of a payment account number or a token that is specifically derived from or otherwise associated with a consumer's payment account number." It's like paying for a DoorDash order through Apple Pay. Apple Pay is a service that stores payment credentials derived from the card numbers of a consumer's active debit or credit accounts. By contrast, a digital asset wallet stores a private key, in the form of an alphanumeric code, that is used to approve a wide variety of transactions, not just those that are payment-related.

So long as digital asset wallets cannot store a customer's bank, debit, or credit account credentials, companies that offer digital asset wallets likely will not be subject to the Bureau's supervisory authority under the proposed rule. But a digital asset financial services company that stores a consumer's bank account credentials on its platform is likely subject to the proposed rule.

Applicable Sector and Key Exclusions

Any digital asset financial services company that facilitates the transmission or exchange of digital assets on behalf of consumers is likely subject to the proposed rule. Additionally, any digital financial services company that stores a consumer's bank account, debit card, or credit card credentials on its platform is likely subject to the Proposed Rule. There are no exceptions to the funds transfer functionality and wallet functionality prongs of the consumer payment functionality definition.

On the other hand, the consumer payment transaction definition excludes several types of transactions from the Bureau's supervisory authority: (1) the exchange of one digital asset to another type of digital asset; (2) the exchange of one fiat currency to another type of fiat currency; (3) the purchase of a digital asset using fiat currency; (4) the sale of a digital asset in which the seller receives fiat currency in return; and (5) any transfer of funds excluded from the definition of "electronic fund transfer" under Regulation E of the EFTA.

Looking Ahead

The Bureau's current stance is that the CFPA's undefined term "funds" includes digital assets. Therefore, if finalized, the proposed rule likely applies to digital asset financial services companies. But like any regulation, the proposed rule is loaded with viable escape routes. Processing less than 5 million consumer digital asset transactions annually, facilitating commercial digital asset transactions, and processing digital asset-to-digital asset exchanges are just a few of the options available. Nevertheless, digital asset transaction monitoring with this level of granularity may require a comprehensive detection system to ensure that certain transactions do not fall within the scope of the consumer payment transaction definition. We anticipate that the courts will continue to adjudicate EFTA-related digital asset lawsuits throughout 2024. As a result, whether the Bureau's interpretation of "funds" holds water will be an important issue to monitor. During the

interim however, digital asset financial services companies should evaluate whether the compliance management costs associated with ensuring exclusion from the proposed rule outweigh the high costs of being periodically examined by the Bureau's supervisory staff.

State Regulatory Action

New York Department of Financial Services

Guidance on Custodial Structures for Consumer Protection in the Event of Insolvency

On January 23, 2023, the New York Department of Financial Services released a guidance document directed to BitLicensees (entities licensed under 23 NYCRR Part 200), as well as entities chartered as limited purpose trust companies under the New York Banking Law, who provide digital asset custody services (virtual currency entity custodians or VCE custodians). The purpose of the guidance is to ensure that VCE custodians provide a high level of customer protection with respect to asset custody. The guidance focuses on four principles related to consumer protection: (1) segregation of and separate accounting for customer virtual currency; (2) a VCE Custodian's limited interest in and use of customer virtual currency; (3) sub-custody agreements; and (4) customer disclosures.

Segregation of and Separate Accounting for Customer Virtual Currency. The guidance reiterates that the NYDFS expects VCE custodians to separately account for and segregate customer virtual currency from their corporate assets and the corporate assets of their affiliated entities. This segregation requirement applies to a VCE custodian's on-chain assets and its internal ledger accounts.

To comply with this segregation requirement, VCE custodians must adopt one of two practices: (1) maintain customer virtual currency in separate on-chain wallets and internal ledger accounts for each customer under that customer's name (separate segregation) or (2) maintain one or more omnibus on-chain wallets and internal ledger accounts that contain only virtual currency of customers held under the VCE custodian's name as agent or trustee for the benefit of those customers (omnibus segregation). Under the omnibus segregation method, a VCE custodian must ensure it has documented policies and procedures in place to maintain a clear internal audit trail that reconciles customer transactions and identifies the customer's present beneficial interest in real-time.

VCE Custodian's Limited Interest in and Use of Customer Virtual Currency. The guidance prohibits VCE custodians from establishing a debtor-creditor relationship with customers, and the NYFDS expects that VCE custodians will treat customer virtual currency in its possession or control as belonging solely to customers. As an example of a prohibited activity, the guidance specifies that a VCE custodian should not use customer virtual currency to secure or guarantee an obligation of the VCE custodian, or to extend credit to any other person.

Sub-Custody Arrangements. The guidance permits a VCE custodian to enter an arrangement with a third party to custody customer virtual currency of behalf of the VCE custodian. However, because this arrangement would constitute a "material change" to the VCE custodian's business under 23 NYCRR § 200.10 of the BitLicense Framework, the VCE custodian would be required to obtain approval from the NYDFS before entering this type of arrangement. In a request for approval, a VCE custodian will have to provide, at minimum, the following to the NYDFS: (1) applicable risk assessment performed by the VCE custodian; (2) the proposed service agreement(s) between the VCE custodian and the applicable third party; and (3) the VCE custodian's updated policies and procedures reflecting the processes and controls to be implemented around the proposed arrangement.

Customer Disclosure. Before entering an initial transaction with a resident of New York, 23 NYCRR § 200.19 requires a BitLicensee to disclose in clear, conspicuous, and legible writing in the English language and in any other predominant language spoken by the customers of the BitLicensee, all material risks associated with its products, services, activities, and virtual currency generally, and obtain acknowledgement from its customers that they have received the disclosures.

The guidance highlights several disclosures the NYDFS expects VCE custodians to issue, each of which are not currently enumerated in the BitLicense Framework:

1. A custodial relationship exists between the VCE custodian and the customer, not a debtor-creditor relationship;
2. The customer's virtual currency is segregated from the virtual currency of the VCE custodian through either the separate segregation or omnibus segregation methods;
3. The customer's property interest in any virtual currency under the care of the VCE custodian will remain with the customer at all times;
4. The VCE custodian will not use the customer's virtual currency to secure or guarantee one of its obligations, or to extend credit to another person; and
5. The terms and material risks of any sub-custody arrangement the VCE custodian enters.

Looking Ahead

Bankruptcy filings by digital asset financial services companies were rife in 2023. For a consumer, the crucial issue in these proceedings was whether s/he possessed a contractual right of title to any digital assets transferred to a digital asset financial services company, or whether upon the transfer, any right of title that a consumer may have possessed became vested with the digital asset financial services company (and its bankruptcy estate by extension). To prevent these consumer-harming contractual arrangements from arising in the future, the guidance effectively writes new disclosure requirements into the BitLicense Framework and requires a VCE custodian to reiterate to its customers that they retain an equitable and beneficial interest in any customer virtual currency under its care.

During 2024, we anticipate that state legislatures that have not already finalized a digital asset legal framework will follow in the NYDFS' footsteps and prioritize consumer protection from unfair, deceptive and/or abusive acts and practices above all else.

California Department of Financial Protection and Innovation

Digital Financial Assets Law

On October 13, 2023, California enacted the Digital Financial Assets Law (DFAL), which becomes effective July 1, 2025. California followed in the footsteps of New York and Louisiana, which adopted comprehensive digital asset regulatory regimes in 2015 and 2023 respectively.

The DFAL equips the California Department of Financial Protection and Innovation (DFPI) with supervisory and enforcement powers to ensure that any entity that engages in "digital financial asset business activity" obtains a license from the DFPI before engaging in such activity with residents of California. Interestingly, the bill allows the DFPI commissioner to issue "conditional licenses" to licensure applicants who have either obtained the elusive New York Department of Financial Services (NYDFS) "BitLicense" or have obtained a "limited purpose trust charter" from the NYDFS.

Unlike the NYDFS' BitLicense Framework, the DFAL defines the term "stablecoin" and outlines the process by which a licensee may permissibly exchange, transfer, or store a stablecoin on behalf of residents of California. For digital asset financial services companies that primarily engage in the business of facilitating stablecoin transactions, it is important to note that the DFAL sets forth two pathways to authorized usage: (1) the "reserve-backed" pathway and (2) the DFPI approval pathway.

Under the reserve-backed pathway, a licensee may exchange, transfer, or store a certain stablecoin if the issuer of the stablecoin is either: (a) an applicant; (b) a licensee under the DFAL; or (c) a bank, trust company, or national association. Alongside this requirement, the issuer of the stablecoin must also always maintain eligible securities in an amount that is not less than the amount of outstanding stablecoins issued or sold by the issuer (i.e., a 1:1 reserve ratio must be maintained). If the issuer of the stablecoin satisfies both requirements, the DFAL permits licensees to exchange, transfer, or store the issuer's stablecoin, and DFPI approval is not necessary.

Under the DFPI approval pathway, a licensee may exchange, transfer, or store a certain stablecoin—even those that are not backed by eligible securities—if the DFPI commissioner determines that the stablecoin does not compromise the interests of residents who may use the stablecoin as a payment for goods and services or as a store of value. To make this determination, the DFPI commissioner will assess specified factors, including but not limited to the following:

1. Any legally enforceable rights provided by the issuer of the stablecoin to holders of the stablecoin, including, but not limited to, rights to redeem the stablecoin for legal tender or bank or credit union credit.
2. The amount, nature, and quality of assets owned or held by the issuer of the stablecoin that may be used to fund any redemption requests from residents.
3. Any representations made by the issuer of the stablecoin related to the potential uses of the stablecoin.

Looking Ahead

By virtue of the 1:1 reserve ratio required under the reserve-backed pathway, a licensee would not be authorized to exchange, transfer, or store an algorithmic stablecoin under this pathway. However, the DFPI approval pathway provides an interesting avenue for popular decentralized stablecoins like DAI to obtain regulatory approval and (potentially) much needed legitimization.

Federal Legislation

National Defense Authorization Act (NDAA)

During December 2023, the exclusion of digital asset-related provisions from the final National Defense Authorization Act (NDAA) released by the U.S. Congress was a disappointing development. Many had hoped that the NDAA, which authorizes appropriations for defense-related activities, would include important provisions related to digital assets. Notably, the package excluded an amendment from Senators Cynthia Lummis (R-WY), Kirsten Gillibrand (D-NY), Roger Marshall (R-KS), and Elizabeth Warren (D-MA). This amendment would have required regulators to set up examination standards for financial institutions engaged in digital asset activities and required the Treasury Department to provide recommendations to Congress on digital asset mixers. The amendment was crafted from provisions taken from the 2023 Lummis-Gillibrand Responsible Financial Innovation Act and the Digital Asset Anti-Money Laundering Act, introduced by Warren and Marshall in 2023.

The proposed amendment specifically called for the Secretary of the Treasury to establish examination standards for digital assets, which would help examiners better assess risk and ensure compliance with money laundering and sanctions laws. Additionally, it required the Treasury Department to conduct a study on "combating anonymous crypto asset transactions," including the use of digital asset mixers that are sometimes used to obfuscate funds.

Another excluded provision would have created an independent working group to combat terrorism and illicit financing. This bill, known as the Financial Technology Protection Act, was introduced in April 2023 by Sen. Ted Budd (R-NC) and Gillibrand. The working group would have been composed of senior representatives from various agencies, including the Department of the Treasury, Department of Justice, U.S. Secret Service, Financial Crimes Enforcement Network, Federal Bureau of Investigation, Department of State, Drug Enforcement Administration, Internal Revenue Service, Department of Homeland Security, Office of Foreign Assets Control, and Central Intelligence Agency. The group would also have included five representatives appointed by the Under Secretary for Terrorism and Financial Intelligence that represent financial technology companies, financial institutions, or organizations engaged in research, and blockchain intelligence companies.

The omission of these digital asset and blockchain provisions was met with disappointment. Lummis expressed her dissatisfaction at the exclusion of her illicit finance provision from the NDAA, emphasizing the need for Congress to "pass meaningful crypto asset legislation to provide robust consumer

protections and create a well-regulated and safe crypto asset market in the United States." As we look ahead, the absence of these provisions in the final NDAA serves as a reminder of the ongoing regulatory uncertainty in the digital asset space.

Digital Asset Anti-Money Laundering Act of 2023

On July 27, 2023, Warren, a vocal skeptic of the digital asset industry, introduced a bill in the Senate known as the Digital Asset Anti-Money Laundering Act of 2023. This legislation would extend Bank Secrecy Act (BSA) responsibilities, including Know-Your-Customer requirements, to digital asset wallet providers, miners, validators, and other network participants involved in validating, securing, or facilitating digital asset transactions.

The bill also addressed the issue of "unhosted" digital wallets, which allow individuals to bypass AML and sanctions checks. It would direct the Financial Crimes Enforcement Network (FinCEN) to finalize and implement its December 2020 proposed rule requiring banks and money service businesses (MSBs) to verify customer and counterparty identities, keep records, and file reports on certain transactions involving unhosted wallets or wallets hosted in non-BSA compliant jurisdictions. In addition, the bill proposes to strengthen enforcement of BSA compliance. It also would direct the Treasury to establish an AML/CFT examination and review process for MSBs and other digital asset entities with BSA obligations and instructs the SEC and CFTC to establish AML/CFT compliance examination and review processes for the entities they regulate.

The bill also would extend BSA rules regarding reporting of foreign bank accounts to include digital assets. This would require U.S. persons engaged in a transaction with a value greater than $10,000 in digital assets through one or more offshore accounts to file a Report of Foreign Bank and Financial Accounts (FBAR) with the Internal Revenue Service (IRS). To mitigate the illicit finance risks of digital asset automated teller machines (ATM), the bill would direct FinCEN to ensure that digital asset ATM owners and administrators regularly submit and update the physical addresses of the kiosks they own or operate and verify customer and counterparty identity.

The introduction of the Digital Asset Anti-Money Laundering Act of 2023 came at a crucial time. With the increasing use of digital assets for illicit activities such as money laundering, ransomware attacks, and terrorist financing, this legislation aims to close regulatory loopholes and bring the digital asset ecosystem into greater compliance with AML/CFT frameworks. As of this writing, the bill remained in committee.

Financial Innovation and Technology for the 21st Century Act

On July 20, 2023, U.S. Reps. French Hill (R – AR), chairman of the Subcommittee on Digital Assets, Financial Technology and Inclusion, Glenn Thompson (R – PA), chairman of the House Committee on Agriculture, and Dusty Johnson (R-SD), chairman of the Subcommittee on Commodity Markets, Digital Assets, and Rural Development, introduced H.R. 4763, the Financial Innovation and Technology for the 21st Century Act (FIT Act). The FIT Act is aimed at bridging regulatory gaps and establishing a functional framework for digital asset regulation in the United States. The FIT Act is unique in its approach, as it would integrate digital assets into existing legal frameworks and standards, rather than creating a completely new regulatory regime, a method seen in other global digital asset-focused legislative proposals, such as the European Union's Markets in Crypto Assets Regulation (MiCA).

The FIT Act covers a range of issues, from creating new categories of registrants, such as digital commodity exchanges, brokers, and dealers, to providing a mechanism for an issuer of a digital asset to petition for its digital asset to be recognized as a commodity, subject to certain conditions. It also would clarify the roles of the CFTC and the SEC in the regulation of digital assets. It proposes that the CFTC should have explicit authority over spot market digital asset commodities, while the SEC should oversee digital assets offered as part of an investment contract, or securities. Interestingly, the discussion draft suggests that even though payment stablecoins would not be classified as digital commodities under the Commodity Exchange Act (CEA), they would still fall under the CFTC's jurisdiction when transacted on a CFTC-registered entity.

Nevertheless, the draft failed to address some key areas. For example, the draft does not provide specific provisions or guidelines for the burgeoning sectors of DeFi or NFTs, except for further joint study by the CFTC and the SEC. The draft also does not touch upon ESG issues, such as the energy consumption associated with digital asset mining, the climate impact of these activities, or the need for diversity in the governance of digital asset entities. The draft also grants the SEC significant discretion in determining whether a network is decentralized, a provision that has raised concerns about potential bottlenecks in approvals.

Lummis-Gillibrand Responsible Financial Innovation Act

On July 12, 2023, Lummis and reintroduced the Responsible Financial Innovation Act (RFIA), which is one of Congress's recent attempts to bring digital assets within the fold of federal law. A crucial aspect of the RFIA is the diverging regulatory authority it attributes to the SEC) and the CFTC. Under the RFIA, the CFTC would have exclusive regulatory authority over any agreement, contract, or transaction involving a sale of a digital asset in or affecting interstate commerce, including payment stablecoins. However, the CFTC's regulatory authority would not be unfettered. The agency's regulatory authority under the RFIA only extends to commercially fungible digital assets, a category of assets that does not include NFTs.

On the other hand, the RFIA would authorize the SEC to solely regulate "ancillary assets," which the bill defines as intangible, fungible assets 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. Although the RFIA seemingly paints the CFTC as the de facto federal regulator of the digital asset industry, the RFIA does provide the SEC with much-needed firepower. It implicitly validates the SEC's usage of the Howey Test as a viable means for initiating enforcement actions against digital asset financial services companies.

With respect to consumer protection, the RFIA would require digital asset financial services companies to: (1) maintain proof of reserves; (2) provide plain language agreements to consumers; (3) devise and implement basic consumer protection standards related to digital assets; and (4) segregate digital assets belonging to consumers from any omnibus accounts maintained by the digital asset company.

The RFIA is expansive in scope and attempts to construct the ground floor for consumer protection in the digital asset industry, while simultaneously resolving the regulatory split between the SEC and the CFTC. But private stablecoin issuers should beware. To protect the existing status quo in which banks are primarily responsible for facilitating the transfer of central bank money in the form of demand deposits, the RFIA only permits depository institutions (as defined in § 19(b)(1) of the Federal Reserve Act) to issue payment stablecoins.

State Legislation

Louisiana: Virtual Currency License Regulation

On June 13, 2023, Louisiana enacted SB 185, amending provisions relating to a legal framework intended to regulate the digital asset industry and its participants. The previously adopted act sets the stage for Louisiana to follow in New York's footsteps, requiring entities to obtain a "Virtual Currency Business Activity License," a license necessary to engage in "virtual currency business activities" in Louisiana. Unlike California, Louisiana chose to explicitly exclude from the definition of "virtual currency business activity" the practice of digital asset mining (i.e., securing or validating transactions that occur on a blockchain), minting of NFTs, and blockchain activities not involving the exchange, holding, sale, storing, or transferring of digital assets. As such, companies that engage in these activities would not be required to obtain a Virtual Currency Business Activity License before providing services to residents of Louisiana.

In the event one of these exclusions does not apply, a company seeking to enter the Louisiana market while its application is pending with the Commissioner of the Office of Financial Institutions

may request a conditional Virtual Currency Business Activity License. Many states have approved possession of the NYDFS' BitLicense as sufficient for approval of a conditional license. However, under the Louisiana bill, the commissioner's authority to issue a conditional license appears to be completely discretionary as the bill does not enumerate any grounds for conditional approval.

New York: The Crypto Regulation, Protection, Transparency and Oversight (CRPTO) Act

On May 5, 2023, New York Attorney General Letitia James a proposed a legislative framework governing digital assets, the Crypto Regulation, Protection, Transparency, and Oversight Act (CRPTO Act). James asserted that the legislation will be the "strongest and most comprehensive set of regulations on cryptocurrency in the nation."

The CRPTO Act contains interesting provisions. For example, it would prohibit a digital asset issuer from offering consumers "any note or debt instrument" that "is payable on demand or otherwise has the features of a demand deposit as defined in [Regulation D (Reserve Requirements of Depository Institutions)]." Therefore, in New York, digital asset issuers would be barred from offering interest-bearing digital asset deposit accounts to their customers. The CRPTO Act would effectively discontinue the "Earn Account" business model that many digital asset financial services companies began to implement throughout 2023, one of which we discussed here.

The CRPTO Act contains an important theme embedded in various state-level legislation proposed and enacted during 2023: the continued push to incorporate the error resolution provisions of Regulation E, the implementing regulation of the EFTA. Under the CRPTO Act, if a customer provides notice within two business days of learning of an unauthorized digital asset transfer, the consumer's liability will not exceed the lesser of $50 or the amount of the unauthorized digital asset transfers that occur before the consumer provided notice. This provision is indistinguishable from the §1005.6 of Regulation E, which contains the same notice period and $50 limitation on consumer liability.

Nevada: Digital Financial Asset Business Activity Law

On March 22, 2023, the Nevada Senate introduced SB 360, or the Digital Financial Asset Business Activity Law. Surprisingly, although Nevada's proposed law predates California's Digital Financial Assets Law, the laws share striking similarities. Nevada's definition of the term "digital financial asset business activity"—the operative term of the law—matches California's definition of that term verbatim. Under Nevada's proposed law, the Division of Financial Institutions of the Department of Business and Industry would have the authority to issue conditional licenses to entities who have already obtained a BitLicense from the NYDFS'. Nevertheless, Nevada's proposed bill contains an important provision that is not present in California's: the bill directly references the EFTA and explains that the EFTA preempts its provisions to the extent those provisions conflict with the provisions of the EFTA.

As we have previously discussed, states are making a concerted effort to endorse the EFTA and Regulation E as the central legal framework that will incrementally integrate digital financial asset business activities into the traditional financial system.

Wyoming: Stable Token Act

On March 17, 2023, Wyoming enacted the Stable Token Act, creating a commission, akin to the Federal Reserve, to develop a state-issued stablecoin backed by the dollar. As the issuer of stablecoins, the commission will choose which financial institutions will be entrusted with managing the "Wyoming Stable Tokens." An integral role of the commission will be to invest funds received for issuing Wyoming Stable Tokens and any earnings from those investments. According to the law, any revenue generated from the commission's issuance of Wyoming Stable Tokens will be exclusively invested in U.S. treasury bills.

New Hampshire: Decentralized Autonomous Organizations

In a bill sponsored by House of Representative Members Keith Ammon, Lex Berezhny, and Joe H. Alexander on January 5, 2023, New Hampshire hopes to place decentralized autonomous

organizations (DAOs) in the ranks of corporations, limited partnerships, and limited liability companies, establishing the digital management structure as a legal entity within the state.

Legislators did not propose a ton of DAO-related legislation during 2023, but DAO liability is an issue that courts continue to grapple with. On this point, the New Hampshire bill expressly asserts that the "debts, obligations, and liabilities of a New Hampshire DAO, whether arising in contract, tort, or otherwise, shall be solely the debts, obligations, and liabilities of the New Hampshire DAO." If passed, this bill would bar a member of a New Hampshire DAO from enforcing a judgment against another individual member of the New Hampshire DAO —including the DAO's founders. This limitation on personal liability would likely subdue a member's desire to initiate a lawsuit against another member, thereby preventing intra-DAO litigation like the class-action lawsuit filed against the bZx DAO, which we discussed here.

Utah: Decentralized Autonomous Organizations Act

On March 1, 2023, the Utah Legislature passed HB 357, or the Decentralized Autonomous Organization Act (DAO Act), which establishes a framework for a DAO to become a legal entity that is separate and distinct from the DAO's members. Unlike existing DAO legislation enacted by Wyoming (W.S. §17 31 101 through §17 31 116) and Tennessee (Tenn. Code Ann. §48-250-101 through 48-250-115), each of which opted to amend their respective Limited Liability Company Acts to encompass DAOs as a type of limited liability company, the DAO Act takes decentralization a step further by creating an entirely new form of corporate structure: a limited liability decentralized autonomous organization (LLD). To solve the DAO liability issue discussed supra, the DAO Act specifies that a developer, member, participant, or legal representative of a LLD may not be imputed to have fiduciary duties toward each other or third parties solely on the account of their role, unless such parties expressly assume a fiduciary role. In essence, this explicit prohibition on implied fiduciary status of LLD members will decrease the available legal grounds for establishing that LLD members owe each other a duty of care under a negligence-based legal theory.

The DAO Act signifies Utah's desire to become the Delaware of DAOs, as evidenced by its decision to prohibit LLDs from including the term "limited liability company" in their corporate names. The DAO Act became effective on January 1, 2024.

Federal Enforcement Actions

Federal Trade Commission (FTC)

During 2023, the FTC began to initiate enforcement actions against digital asset-related entities (and their executives) for failing to ensure the accuracy of marketing statements made to consumers. Liability under the FTC Act is all-encompassing—an executive may become liable if the executive participated directly in any deceptive practices performed by the company or had the authority to control, or knowledge of, the deceptive practices. Historically, the FTC has limited its pursuit of individual liability to executives of small companies. But, as seen in the FTC's recent filings naming three senior executives of a company as individual defendants, the FTC seems determined to utilize the full extent of its authoritative powers to impose liability on corporate executives in instances in which they may have simply "had the authority to control" allegedly deceptive practices. Stakeholders within the digital asset industry would be wise to monitor the FTC's actions throughout 2024 and ruminate on the massive monetary penalties imposed by the FTC in consent orders it entered with two digital asset-related companies during 2023.

On July 17, 2023, the FTC entered a consent order with a defunct digital asset financial services company (Company #1) that initially caught the FTC's attention by offering consumers interest-bearing digital asset demand deposit accounts (akin to traditional bank accounts) that purportedly yielded up to 17% APY (Earn account). The FTC's allegations against Company #1 concerned the Earn account and its associated marketing. For example, the FTC alleged that Company #1 misled consumers into believing they could withdraw, at any time, digital assets deposited into Earn accounts maintained on Company #1's platform. On the evening of June

11, 2022, Company #1 prohibited consumers from withdrawing digital assets from Earn accounts. The legality of Company #1's decision to pause withdrawals became a major point of contention during its Chapter 11 bankruptcy proceedings, which we discussed in detail here. Notably, various statements made by the ex-CEO of Company #1 served as the foundation of the FTC's enforcement action. Among other things, the FTC alleged that the ex-CEO, during various live "Ask Me Anything" sessions, asserted that "[Company #1] had a $750 million insurance policy for [digital assets deposited in Earn accounts]" and Company #1 was "the only one in the world" with such a policy. This statement, alongside other statements made by the ex-CEO, were blatantly false.

Not only did the ex-CEO's ill-advised statements provide the FTC with the necessary firepower to substantiate its case against Company #1, but those statements also acted as the jurisdictional hook that enabled the FTC to hold the ex-CEO jointly and severally liable for a whopping $4.7 billion judgment. It is one thing to attempt to distinguish your business from your competitors by zealously championing (within defined parameters) the services your business provides. It is another thing entirely to tell your customers that your business will be perpetually solvent. The latter will bring you within the crosshairs of the FTC, or worse, the Department of Justice (DOJ). On July 13, 2023, the DOJ charged the ex-CEO of Company #1 with securities fraud, commodities fraud, and wire fraud. His trial is set to begin September 2024.

Company #1 is not in complete disarray, however. On January 31, 2024, it announced its successful emergence from bankruptcy, completing its Chapter 11 reorganization plan. The plan includes distributing over $3 billion to its creditors and the creation of a new Bitcoin mining company, dubbed Ionic Digital, Inc, which will be owned by Company #1's creditors.

On October 12, 2023, the FTC entered a consent order with a defunct digital asset financial services company (Company #2) for allegedly misleading its customers that digital assets deposited onto Company #2's platform were protected by insurance offered by the FDIC. Like Company #1, Company #2 declared bankruptcy and offered its customers Earn accounts. However, unlike Company #1, Company #2 provided its customers with debit cards that could be used to make real-world transactions with either a digital asset or fiat currency. In other words, by using Company #2's debit card, a consumer could purchase a coffee from Starbucks using Bitcoin or U.S. dollars. The issuer of Company #2's debit card and custodian of the fiat currency cash balances of Company #2's customers was an insured depository institution as defined by the FDI Act. To make this service more marketable, Company #2 eventually began to promote a new layer of protection for consumers' fiat currency cash balances:

> "Through our strategic relationships with our banking partners, all customers' USD held with [Company #2] is now FDIC insured. That means in the rare event your USD funds are compromised due to the company or our banking partner's failure, you are guaranteed a full reimbursement (up to $250,000)."

Although Company #2 likely intended this advertisement to be informative and reassuring to its customers, the FTC concluded that the statement was facially misleading. To earn yield, Company #2's customers deposited USD Coin (USDC), a popular stablecoin pegged to the U.S. dollar, into their Earn accounts. From the FTC's perspective, Company #2's FDIC-related advertisement was misleading because a consumer could interpret Company #2's statement to encompass all USD-related funds held by the consumer—even stablecoins. Moreover, as the FTC specified, although an insured depository institution was responsible for managing the fiat currency cash balances of Company #2's customers, FDIC insurance would only protect up to $250,000 of a consumer's cash balance in the event of the insured depository institution's dissolution, not Company #2's. Because Company #2 was not an insured depository institution under the FDI Act, it technically could not offer FDIC insurance to its customers. The FTC's deception theory was largely based on this mechanistic impossibility.

Under the consent order, the FTC imposed a $1.65 million judgment against Company #2 and its subsidiaries. Interestingly, although the FTC named the ex-CEO of Company #2 as an individual defendant, the FTC did not seek to hold him jointly

and severally liable for the judgment. In comparison to the ample evidence of misleading statements made by the ex-CEO of Company #1, the FTC had considerably less evidence of the ex-CEO of Company #2 issuing verbal statements to the public about Company #2's provision of FDIC insurance. The lack of affirmative statements may have mitigated the FTC's otherwise strong desire to hold the ex-CEO of Company #2 personally liable for the judgment entered against Company #2.

Looking Ahead

The foregoing consent orders are cautionary tales. Due to concerns of fraud, the FTC amplified its interest in the digital asset industry. Considering the framework of the FTC's enforcement authority under the FTC Act, we anticipate that the agency will remain focused on the marketing practices of digital asset financial services companies and any statements made by their executives. Therefore, a bank that is considering partnering with a digital asset financial services company should ensure the partnership agreement authorizes it to analyze any marketing materials bearing its name before the digital asset financial services company publishes the materials to the public.

Conclusion

In alignment with Bitcoin's four-year market cycles, we expect the digital asset industry's market capitalization to continue to proliferate throughout 2024. Toward the end of 2023, the market shook off the rust of the "Crypto Winter" still lingering from 2022 and is now undoubtedly bullish. Still, while bull markets foster asset appreciation, November 2021 (when Bitcoin reached its previous all-time high of approximately $69,000) taught us that this market condition also triggers large-scale consumer euphoria that can lead to asset bubbles. Once these bubbles burst, consumers are generally left holding the proverbial "bag" with no recourse.

Understanding that a lack of prudential regulation, at minimum, contributed to the monetary injuries that consumers incurred during the aftermath of Bitcoin's sharp rise during November 2021, we expect that Congress will again try to enact a digital asset regulatory framework to ensure that consumers have access to clear and conspicuous disclosures in this cycle's upcoming rally, and to ascribe specific powers to federal regulatory agencies to decrease incidents of regulation through civil enforcement actions but this may not come until election season is over. State legislatures have already taken matters into their own hands and have implicitly approved the EFTA and Regulation E as vital tools to govern the industry.

Only time will tell whether Congress too will decide to integrate the EFTA and Regulation E into any regulatory framework it proposes. Nevertheless, considering the current state legislative trend and the plaintiffs bar's adoption of the EFTA and Regulation E to commence legal actions against digital asset financial services companies, we recommend that compliance officials within these companies begin to familiarize themselves with the disclosure and error resolution requirements of Regulation E, as well as its liability framework, which Congress deliberately constructed to limit the amount of a consumer's liability in the case of an unauthorized transfer of funds. ■

AUTHORS

Ethan Ostroff
Partner
ethan.ostroff@troutman.com
757.687.7541

Addison Morgan
Associate
addison.morgan@troutman.com
470.832.5569

Trey Smith
Associate
trey.smith@troutman.com
804.697.1218

About Troutman Pepper

Troutman Pepper is a national law firm with more than 1,100 attorneys strategically located in 20+ U.S. cities. The firm's litigation, transactional, and regulatory practices advise a diverse client base, from startups to multinational enterprises. The firm provides sophisticated legal solutions to clients' most pressing business challenges, with depth across industry sectors, including energy, financial services, health sciences, insurance, and private equity, among others.

The information in this publication is not intended to serve as legal advice. For more information about cryptocurrency and other digital assets issues, or to subscribe to our insights, please contact a Troutman Pepper attorney or visit our website at troutman.com.