ALERT MEMORANDUM

U.S. Government Digital Asset Reports:

How the Industry Can Prepare for Congressional, Regulatory, and Enforcement Action in 2023

January 18, 2023

Following President Biden's March 9, 2022 Executive Order on Ensuring Responsible Development of Digital Assets, the White House announced in September 2022 the "first-ever comprehensive framework" on digital assets based on a series of reports from various federal government agencies and offices. The reports, however, are far from a "comprehensive framework." Instead, they are heavy on descriptions of risks and malfeasance of actors in the digital assets space, but light on concrete recommendations and substantive actions. This Alert Memorandum sets forth key takeaways from the reports, and describes, over six thematic areas, what industry participants can do in 2023 to prepare should some of the reports' suggestions become more concrete. It also discusses throughout whether any changes in legislation, regulation, or enforcement can be expected.

At the regulatory level, given the small number of constructive advances or plans in the reports, and the focus on risks rather than solutions, we expect significant near-term increases in enforcement actions as the primary short-term approach to developing the regulatory regime, with the potential for modest medium-term rule making.

At the federal legislative level, with the Republicans taking control of the House of Representatives, a potential stalemate on comprehensive legislation is likely, although various members of Congress have declared that either or both a stablecoin framework or a broader digital assets framework can be passed. In the meantime, the FTX bankruptcy situation lends greater weight to those who would impose more restrictive or prohibitive measures on digital assets.

Without clarity or a comprehensive framework, it is likely that industry actors will continue to seek either jurisdictions or vehicles that provide them the most flexibility for engaging in digital asset activities, potentially continuing a vicious cycle of adverse events and increasing calls for greater and earlier enforcement actions.

If you have any questions concerning this Alert Memorandum, please reach out to your regular firm contacts or to the following authors:

Derek M. Bush
+ 202 974 1526
dbush@cgsh.com

David Lopez
+1 212 225 2632
dlopez@cgsh.com

Hugh C. Conroy Jr.
+1 212 225 2828
hconroy@cgsh.com

Chase Kaniecki
+1 202 974 1792
ckaniecki@cgsh.com

Brandon Hammer
+1 212 225 2635
bhammer@cgsh.com

Samuel Levander
+1 212 225 2951
slevander@cgsh.com

Michael Sanders
+1 202 974 1894
msanders@cgsh.com

Caleb J. Robertson
+1 202 974 1924
cjrobertson@cgsh.com

William S. Dawley
+1 202 974 1771
wdawley@cgsh.com

Megan Lindgren
+1 212 225 2769
mlindgren@cgsh.com

This Alert Memorandum sets forth key takeaways from the reports and describes, over six thematic areas, what industry participants can do in 2023 to prepare should some of the reports' suggestions become more concrete. It also discusses throughout whether any changes in legislation, regulation, or enforcement can be expected.

THE REPORTS

The reports released by the United States Department of the Treasury ("**Treasury**"), Department of Justice ("**DOJ**"), Department of Commerce ("**Commerce**"), the White House Office of Science and Technology Policy ("**OSTP**"), and the Financial Stability Oversight Council ("**FSOC**"), among others, cover a wide range of topics both technical and legal, including continued emphasis on civil and criminal enforcement actions, possible areas of regulatory rulemaking, the potential for the Federal Reserve to issue a U.S. Central Bank Digital Currency ("**CBDC**"), suggestions for Congressional legislation, issues related to climate change and the United States' position as a global leader in developing digital asset-related technology. The "**Reports**" discussed in this Alert Memorandum are cataloged below:

- DOJ, *How to Strengthen International Law Enforcement Cooperation for Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets* (June 6, 2022) (the "**DOJ Report**")
- Treasury, *Fact Sheet: Framework for International Engagement on Digital Assets* (July 7, 2022) (the "**Treasury International Report**")
- Treasury, *The Future of Money and Payments* (Sept. 2022) (the "**Treasury Payments Report**")
- Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses* (Sept. 2022)
- Treasury, *Action Plan to Address Illicit Financing Risks of Digital Assets* (Sept. 2022) (the "**Treasury Illicit Finance Report**")
- DOJ, *The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets* (Sept. 6, 2022) (the "**Law Enforcement Report**")
- Commerce, *Responsible Advancement of U.S. Competitiveness in Digital Assets* (Sept. 2022) (the "**Commerce Report**")
- White House OSTP, *Technical Evaluation for a U.S. Central Bank Digital Currency System* (Sept. 2022) (the "**OSTP CBDC Report**")
- White House OSTP, *Climate and Energy Implications of Crypto-Assets in the United States* (Sept. 8, 2022) (the "**OSTP Climate Report**")
- FSOC, *Report on Digital Asset Financial Stability Risks and Regulation* (Oct. 3, 2022) (the "**FSOC Report**").

KEY TAKEAWAYS

— **Absence of concrete plans, timelines or frameworks.** The Reports identify a wide array of perceived risks associated with digital assets without providing concrete solutions or even frameworks for devising solutions. Since (and undoubtedly before) the U.S. banking regulators announced the completion of their "crypto sprint" toward the end of 2021, industry participants have expected a shift toward action and guidance—and perhaps clarity—from the federal government. Unfortunately, more than a year later, the Reports generally provide few constructive advances or plans, including for key topics such as stablecoins.

— **Continued focus on enforcement, based on existing laws, rules and frameworks**. Rather than provide clarity in relation to the numerous questions that have emerged under the attempted application of existing statutory and regulatory frameworks, the Reports repeatedly declare that industry actors are avoiding

compliance with existing rules. In light of the focus of the Reports on risks rather than solutions, and the focus on problems rather than innovative use cases, we expect significant near-term increases in enforcement actions and regulatory admonitions. Indeed, several of the Reports call for "urgent" enforcement intervention and for "aggressive" and continued enforcement action by agencies. The Reports repeatedly encourage the SEC, CFTC, CFPB, and FTC to enforce existing statutory and regulatory frameworks aggressively, implicitly assuming that existing law is sufficient for the purpose. The Reports also include multiple specific proposals aimed at strengthening DOJ and Treasury law enforcement efforts.

— **If and when legislative or regulatory action is taken, expect the U.S. federal government to centralize enforcement and other regulatory solutions at the expense of states and even international governments.** Several of the Reports highlight state statutory and regulatory frameworks as an inconsistent and ineffective patchwork. It is clear from the Reports that the federal agencies view federal legislation as necessary and likely to displace state legislation and regulation in this space. As examples:

  - The FSOC Report recommends the passage of legislation providing for rulemaking authority for federal financial regulators over spot markets for digital assets that are not securities, federal legislation creating a comprehensive prudential framework for stablecoin issuers, federal legislation providing for consolidated supervision of "crypto-asset entities" and their affiliates, and the study, at the federal level, of potential risks and conflicts associated with vertical integration of digital asset services.
  - Furthermore, noting the insufficiency of state money transmitter laws, the Treasury Payments Report calls for the establishment of a first-ever federal framework for payments regulation, including for nonbank financial institutions that are primarily regulated by state authorities.
  - A number of the Reports, and in particular the Treasury International Report and the Treasury Illicit Finance Report, call out gaps, "uneven" enforcement and opportunities for "arbitrage" in foreign country frameworks, indicating that some extraterritorial application of U.S. law or at least U.S. efforts to push foreign governments in a particular direction may be contemplated.

— **More reports, and possibly substantive recommendations, are to come.** The Reports generally constitute a "plan to make a plan" rather than a comprehensive framework for improving clarity in the digital asset space.

  - **Additional reports are planned for 2023.** The Reports note that Treasury will release reports on decentralized finance ("**DeFi**") in February 2023 and non-fungible tokens ("**NFTs**") in July 2023.
  - **More work to be done on a CBDC**. The Reports discuss the prospect of a CBDC at length, but decline to explicitly support or oppose a CBDC and generally do not express a preference for particular features of a CBDC (other than the OSTP CBDC Report indicating a preference for a two-tier approach in which financial institutions onboard and manage payments and the Federal Reserve records account balances). Interestingly, Treasury indicates that it will move forward with the creation of an inter-agency CBDC working group, notwithstanding the Federal Reserve's relatively singular role in creating a CBDC.
  - **Revival of previously-proposed rules for AML/BSA enforcement.** Treasury signals that it plans to focus on advancing previously proposed rules that: (1) clarify applicability to digital assets of the travel rule and recordkeeping rules, which require financial institutions to collect and transmit certain information about funds transfers to other financial institutions, including through an additional notice of proposed rulemaking expected in 2024 and (2) require banks and money services businesses ("**MSBs**") to submit reports to FinCEN, keep records, and verify the identity of customers with respect to digital asset transactions with "unhosted wallets," defined as wallets not hosted by a financial institution.

Based on these key takeaways from the Reports, what might industry actors need to monitor in 2023? Below we highlight six thematic areas in which industry participants may want to invest time and thought to prepare for future developments:

I. Expect continued, and likely more aggressive, monitoring and enforcement;

II. In particular, expect deeper AML, BSA, combatting the financing of terrorism ("**CFT**") and sanctions scrutiny, enforcement and potentially rulemaking;

III. Review products and services for opportunities to decrease risks to consumers and investors;

IV. Be aware of potential vulnerabilities arising from interconnections with the traditional financial system and payment rails, as well as within the digital asset industry itself;

V. Monitor the legislative and regulatory process at the federal level, even if firms are state-regulated (or a foreign company); and

VI. Prepare for the U.S. federal government to prioritize the potential of domestic and international payments systems, rather than benefits from the broader digital asset sphere.

I. Expect Continued, and Likely More Aggressive, Monitoring and Enforcement.

Many of the Reports, in particular the Treasury Reports and DOJ Reports, focus almost solely on the risks of illicit activity involving digital assets. A running theme throughout many of the Reports is the need to maintain and increase regulatory and criminal investigations and monitoring of digital asset transactions and virtual asset service providers to prevent money laundering, fraud and other illicit activities that may be facilitated more readily by digital assets than traditional financial instruments. The Reports also repeatedly highlight noncompliance of some industry participants, with a particular focus on mixers and darknet markets.

Notably, the Reports themselves are noncommittal on some of the more nuanced questions about digital assets, particularly how they should be classified, who should be regulating them, and under what circumstances. Instead, the Treasury reports call for a collaborative, interagency approach to monitoring, investigating, and regulating digital assets, with a priority in the near-term on enforcement under current regulatory frameworks. A variety of law enforcement and regulatory agencies could be involved in these activities, including the DOJ, SEC, CFTC, CFPB, FTC, and Treasury, among others. The Reports call on these agencies to proactively share information and work together to prevent illicit activity involving digital assets.

The DOJ announced the formation of a 150-person-strong network of prosecutors (the DAC Network) tasked with becoming experts on digital assets and with the prosecution of digital asset-related criminal activity. The DAC Network will be led by the National Cryptocurrency Enforcement Team and will include prosecutors from various U.S. Attorneys' Offices and DOJ departments. The DAC network will undoubtedly be under pressure to develop high-profile and groundbreaking cases to justify the considerable allocation of resources. Likewise, the SEC has considerably increased its investment in enforcement, doubling the size of the Division of Enforcement's Crypto Assets and Cyber Unit in May 2022.

Firms that operate in the digital asset space and want to maintain a good reputation with law enforcement should ensure they have the functional ability to respond quickly, completely, and efficiently to requests from law enforcement for information. In particular, firms should make sure that they are appropriately tracking and storing transaction data and their own internal communications in case they become the subject of document requests from the government. Firms should also be sure to advise their employees that their work-related communications, including on smartphone apps such as Telegram, WhatsApp, or Signal, may be subject to subpoena from law enforcement or regulatory authorities. Market participants should also consider whether they have adequate policies regarding the use by employees of confidential information belonging to the firm, as well

as employee trading in digital assets that are involved in that firm's business.

Regulatory enforcement may intensify in other areas as well, as FSOC identified compliance with, and enforcement of, the existing regulatory framework as a key step in addressing financial stability risks.[1] Additionally, the bankruptcy of FTX will increase pressure on agencies and law enforcement to bring enforcement actions using currently-available tools.[2] Firms should continue to work in good faith to understand and develop policies related to federal and state securities laws, to consider the permissibility of new digital asset derivatives products, and to ensure that statements regarding the availability of federal deposit insurance, or regarding the extent to which firms or products are regulated, are not false or misleading.

II. Expect deeper AML, BSA, CFT and Sanctions scrutiny, enforcement and potentially rulemaking.

Many of the Reports highlight concerns related to AML, BSA, CFT, and sanctions risks of digital asset transactions. In particular, the Treasury Illicit Finance Report sets forth actions that Treasury expects to take to mitigate those risks. Many of these actions are simply continuing current work, but some of Treasury's plans are new, and industry actors should consider what impact they could have on their operations.

— Primary Risks and Vulnerabilities

Treasury acknowledges that the use of digital assets significantly lags behind more traditional methods of money laundering and terrorist financing in terms of use and adoption but highlights ransomware,[3] drug trafficking, fraud, sanctions evasion, terrorist financing,[4] and unfriendly government actors as key risks. Those involved in such activities exploit vulnerabilities cited by Treasury, including: (1) the lack of involvement of regulated, compliant virtual asset service providers, whether because of (a) disintermediation (*e.g.*, self-hosted wallets), (b) lack of regulation, or (c) noncompliance and (2) anonymity-enhancing technologies, which can include assets, such as "privacy coins," or services, such as mixers or tumblers, that may help to hide the movement or origin of funds.

— DeFi, NFTs, and P2P under the microscope

Treasury appears concerned that decentralized finance ("**DeFi**"), non-fungible tokens ("**NFTs**"), and peer-to-peer digital asset transactions ("**P2P**") are vulnerable for use in illicit finance because of a lack of BSA/AML regulation or lack of compliance by related actors who already have BSA/AML compliance obligations.[5] Treasury appears set to take concrete steps with respect to DeFi, NFTs, and P2P, including:

- Treasury plans to publish a risk assessment by February 2023 on the money laundering and terrorist financing risks related to DeFi;
- Treasury plans to publish a risk assessment by July 2023 on money laundering and terrorist financing risks related to NFTs;

[1] FSOC Report, at 5.

[2] *See, e.g.*, Treasury, Statement by Secretary of the Treasury Janet L. Yellen on Recent Crypto Market Developments (Nov. 16, 2022) ("Where existing regulations apply, they must be enforced rigorously so that the same protections and principles apply to crypto assets and services"). Note that the SEC's complaints against Sam Bankman-Fried, Caroline Ellis, and Gary Wang allege defrauding of equity investors in FTX, rather than relying on new theories regarding securities transactions with customers. The SEC stated that "investigations as to other securities law violations and into other entities and persons relating to the alleged misconduct are ongoing." *See* SEC Press Release 2022-219 (Dec. 13, 2022) and SEC Press Release 2022-234 (Dec. 21, 2022). In contrast, the CFTC's complaints allege fraud "in connection with the sale of digital commodities." *See* CFTC Press Release 8638-22 (Dec. 13, 2022).

[3] For further discussion of ransomware developments, *see* Cleary Gottlieb, OFAC Ramps up Targeting of Ransomware-linked Actors and FinCEN Updates Ransomware Advisory, OFAC Updates Ransomware Advisory and Sanctions Virtual Currency Exchange and Ransomware and Sanctions Compliance: Considerations for Responses to Attacks.

[4] For further discussion of issues related to terrorist financing concerns, *see* Cleary Gottlieb, Cryptocurrency and Other New Forms of Financial Technology: Potential Terrorist Financing Concerns and Liability.

[5] In particular, Treasury notes that P2P service providers and DeFi protocols could constitute virtual asset service providers and have BSA/AML obligations as MSBs.

- Treasury plans to finalize FinCEN's previously proposed "unhosted wallet" rule, although it has recently pushed the expected finalization date until early 2024;
- Treasury issued a Federal Register request for input on, among other things, the illicit finance risks of NFTs, DeFi, and P2P; and
- Although DOJ specifically called for the application of the BSA/AML framework to NFT networks, Treasury has not yet adopted that goal as an action item.

— Updating BSA regulations, including finalizing FinCEN's "unhosted wallet" rule

Treasury indicates that it will continue to update BSA regulations with respect to digital asset activities. In particular:

- Treasury will focus on proposed rules that would: (1) clarify that the travel rule and recordkeeping rules[6] (collectively, the "**Travel Rule**") apply to digital asset transactions (the "**Travel Rule Update**"),[7] and (2) require banks and MSBs to submit reports to FinCEN, keep records and verify the identity of customers with respect to digital asset transactions with "unhosted wallets" and "hosted wallets" in certain designated jurisdictions (the "**Unhosted Wallet Rule**").[8]
- According to Treasury's semiannual agenda of August 8, 2022, Treasury planned to issue (1) a second notice of proposed rulemaking with respect to the Travel Rule Update in December 2022 and (2) a final Unhosted Wallet Rule in March 2023.[9] However, those expected releases have been pushed back in both cases to February 2024 in the recently-released Fall 2022 Unified Agenda of Federal Regulatory and Deregulatory Actions.[10] Furthermore, FinCEN has a number of other priorities and is experiencing delays with respect to other rulemakings, so those timeframes may be further extended. Likewise, the Unhosted Wallet Rule sparked significant backlash when it was initially proposed, and it is possible that such opposition could have an effect on a final rule, if any is implemented.

The **Travel Rule** requires financial institutions to collect and retain information related to funds transfers and transmittals of funds in amounts of $3,000 or more and transmit that information to other financial institutions participating in the transfer or transmittal. Although FinCEN takes the position that the Travel Rule currently applies to digital asset transactions,[11] some commenters and observers have suggested that the Travel Rule does not apply to those transactions because digital assets are not "money" as defined by the Travel Rule.[12] These parties argue that the underlying obligations apply only to funds transfers, which involve an instruction to pay a "fixed or determinable amount of money," and digital assets do not qualify as "money" under the rules.[13]

Additionally, compliance with the Travel Rule with respect to transactions in digital assets faces a number of technical challenges, and although industry groups are working collaboratively towards solutions, much is left to be done. FinCEN has acknowledged these

[6] 31 C.F.R. §§ 1020.410(a), 1020.410(f), 1010.410(e).
[7] 85 Fed. Reg. 68005, 68010 (Oct. 27, 2020).
[8] 85 Fed. Reg. 83840 (Dec. 23, 2020).
[9] 87 Fed. Reg. 48324 (Aug. 8, 2022).
[10] *See* Fall 2022 Unified Agenda of Regulatory and Deregulatory Actions.

[11] *See, e.g.*, FinCEN, Prepared Remarks of FinCEN Director Kenneth A. Blanco at the Consensus Blockchain Conference (May 13, 2020) (stating that the United States has consistently applied the travel rule to digital currency transmittals).
[12] 85 Fed. Reg. 68005, 68011 (Oct. 27, 2020).
[13] In particular, the preamble to the adopting release of the recordkeeping rule states that all terms not specifically defined in the regulation will have the meaning given to them in Article 4A of the Uniform Commercial Code, which provides that "money" is defined as "a medium of exchange currently authorized or adopted by a domestic or foreign government." *Id.* at 68010. El Salvador has adopted Bitcoin as legal tender.

challenges,[14] and the Reports also recognize the difficulty in complying with the Travel Rule.[15] As it stands, although FinCEN has claimed to cite financial institutions for violations of the Travel Rule,[16] to our knowledge, no public enforcement action has been brought on that basis.

Finalizing the Travel Rule Update may lead to enforcement of the Travel Rule with respect to digital asset transactions through regulatory or even criminal actions. In fact, the DOJ in its Law Enforcement Report stated that "[o]nce FinCEN issues the final rule, the [DOJ] proposes to support FinCEN in enforcing the rule and encouraging its implementation throughout the digital assets industry."[17]

The **Unhosted Wallet Rule** would require banks and MSBs to submit reports to FinCEN, keep records, and verify the identity of customers with respect to transactions in digital currency with "unhosted wallets," defined as wallets not hosted by a financial institution subject to the BSA or a foreign financial institution, or "hosted wallets" in certain designated jurisdictions.[18] In particular, in certain circumstances, banks and MSBs may be required to collect the name and address of each counterparty (i.e., holder of an "unhosted wallet") and include that information in a report submitted to FinCEN. These changes could significantly disrupt the current practices of, and pose compliance burdens on, banks and MSBs involved in digital asset transactions.

- Treasury will continue to consider whether any gaps exist in the BSA/AML framework that should be addressed, which could include continued consideration of lowering the $3,000 threshold for the Travel Rule, despite the fact that the October 2020 proposal[19] to lower that threshold to $250 for cross-border transactions was withdrawn.[20]
- Treasury may expand FinCEN's 314(a) program[21] to include more virtual asset service providers. This program enables Treasury to reach out to financial institutions to locate accounts and transactions identified by law enforcement agencies.
- Shortly after release of the Reports, Treasury issued a Federal Register request for input on certain matters "relevant to Treasury's ongoing efforts to assess the illicit finance risks associated with digital assets as well as the ongoing efforts to mitigate the risks."[22] The request specifically asked for input on, among other things, the risks of NFTs, DeFi, and P2P.

— BSA/AML/sanctions compliance programs

Virtual asset service providers subject to BSA/AML and sanctions requirements[23] or expectations should

[14] *Id.* at 68011 ("FinCEN is aware that the [convertible virtual currency] industry is working on developing systems and processes to achieve full compliance with the Travel Rule as applied to virtual currency transactions.").
[15] *See*, *e.g.*, Treasury Illicit Finance Report, at 14 (discussing the support for emerging technologies to support the development of Travel Rule compliance solutions).
[16] *See* FinCEN, Prepared Remarks of FinCEN Director Kenneth A. Blanco at Chainalysis Blockchain Symposium (Nov. 15, 2019) ("FinCEN, through our delegated examiners at the Internal Revenue Service (IRS), has been conducting examinations that include compliance with the [] Travel Rule since 2014. In fact, to date it is the most commonly cited violation by the IRS against MSBs engaged in [convertible virtual currency] money transmission.").
[17] DOJ Report, at 43.
[18] Initially, the jurisdictions would be those designated by FinCEN as jurisdictions of primary money laundering concern.
[19] 85 Fed. Reg. 68005, 68007 (Oct. 27, 2020).
[20] 87 Fed. Reg. 5278 (Jan. 31, 2022).
[21] 31 C.F.R. § 1010.520.
[22] 87 Fed. Reg. 57556 (Sep. 20, 2022).
[23] As noted in our discussion of OFAC guidance provided to the digital asset industry (*see* Cleary Gottlieb, OFAC Issues Sanctions Guidance to Virtual Currency Industry), jurisdiction with respect to U.S. sanctions is broad. U.S. sanctions laws apply to all U.S. citizens and lawful permanent residents wherever located, all individuals and entities located within the United States and all entities organized under the laws of the United States or any jurisdiction of the United States, including foreign branches

implement effective compliance programs, including experienced compliance personnel and effective screening and monitoring technology.[24] Effective compliance programs will be crucial in avoiding regulatory scrutiny, as well as preventing or mitigating enforcement actions and private litigation.[25]

— Continuing use of Treasury sanctions and designation powers

Treasury expects to continue to use Office of Foreign Assets Control ("**OFAC**") sanctions and FinCEN special measures designations to "cut [actors] off from the international financial system."[26] Negative reactions to OFAC's designations related to Tornado Cash do not appear to have lessened Treasury's willingness to use its sanctions designation power and other powerful tools at its disposal to punish activities that may otherwise be outside of the reach of direct sanctions prohibitions (*e.g.*, that are conducted outside of the United States by non-U.S. persons and do not involve a U.S. nexus, such as dollar transactions that clear through the U.S. financial system). Even the Commerce Report calls for a sufficient regulatory framework backed by diligent enforcement as a means to increase innovation and U.S. leadership in this space.

III. Review products and services for opportunities to decrease risks to consumers and investors.

Rather than focusing on providing more guidance or clarity to the industry on various open questions (the answers to which would likely enhance compliance), the Reports focus on protection of the end users of digital assets, whether they are consumers, investors, or businesses, from noncompliant actors. Concerns about the risks of fraud, theft, and market manipulation drive much of the discussion in the Reports about the need for comprehensive regulation and aggressive enforcement. The Reports also discuss the need for adequate disclosures to consumers and additional transparency about the risks of digital assets.

Firms should consider how to proactively address concerns about risks to consumers, investors, and businesses. In particular, firms should evaluate how they describe their business practices and the risks associated with their digital asset-related products and services in regulatory filings, company reports, and marketing. Furthermore, firms should review existing disclosures, terms and conditions, and agreements with customers, in order to ensure that the transactions and obligations are described correctly, and any representations regarding regulation of the firm or protection afforded to the customer are accurate. In particular, digital asset platforms seeking to offer pass-through Federal Deposit Insurance Corporation ("**FDIC**") insurance should consider their statements in light of the FDIC's final rule and recent proposed rule regarding deposit insurance advertising.[27] Having appropriate measures in place early may lead to better outcomes with regulatory and law enforcement agencies who later pursue investigations.

IV. Be aware of potential vulnerabilities arising from interconnections with the traditional financial system and payment rails, as well as within the digital asset industry itself.

of those entities. In addition, certain activities by non-U.S. persons that involve a U.S. nexus, such as U.S. persons or goods or services exported from the United States, may be subject to sanctions restrictions.

[24] The Treasury Illicit Finance Report makes clear that Treasury view adoption and use of blockchain analytics and similar technological solutions as a "best practice." This was also previously expressed in OFAC's guidance to the digital asset industry.

[25] For further discussion of sanctions compliance, *see* Cleary Gottlieb, OFAC Issues Sanctions Guidance to Virtual Currency Industry. For further discussion of issues related to terrorist financing concerns, *see* Cleary Gottlieb, Cryptocurrency and Other New Forms of Financial Technology: Potential Terrorist Financing Concerns and Liability. Note also that states are aggressively enforcing federal and state laws related to AML and sanctions compliance programs. *See*, *e.g.*, NY Department of Financial Services, In the Matter of Coinbase, Inc. (Jan. 4, 2023).

[26] Treasury Illicit Finance Report, at 14.

[27] *See* FDIC, False Advertising, Misrepresentation of Insured Status, and Misuse of the FDIC's Name or Logo, 87 Fed. Reg. 33415 (June 2, 2022); FDIC, FDIC Official Sign and Advertising Requirements, False Advertising, Misrepresentation of Insured Status, and Misuse of the FDIC's Name or Logo, 87 Fed. Reg. 78017 (Dec. 21, 2022).

The FSOC Report identifies a number of interconnections with the traditional financial system, spanning stablecoins and payments, products and services offered to digital asset companies by banking organizations, publicly offered investment products, private investments, on-ramps for consumers and retail investors (*e.g.*, credit card rewards denominated in digital assets), insurance policies held by digital asset firms, municipal tax payments, and mortgage collateralization and securitization. While acknowledging that a number of these interconnections are the result of innovation to improve platforms and offerings, thereby increasing convenience and choice for customers, FSOC expressed concern over how shocks in digital asset markets could lead to knock-on effects in the traditional financial system and broader economy. In addition, federal banking regulators have continued to warn banks about their connections and potential concentrations with virtual asset service providers.[28]

Therefore, it is key that industry participants become aware of, and foster compliance when participating in, touchpoints between the digital assets industry and the traditional financial system. These touchpoints form a vector for regulatory and enforcement actions under existing statutory and regulatory frameworks.

Nevertheless, the FSOC Report requests greater authority for regulators under new legislation or rulemaking. In particular, the FSOC Report warns of potential systemic crises should the scale and scope of the digital asset industry continue to grow and should these intersections with the traditional financial system become more material and widespread. The FSOC Report suggests that financial stability vulnerabilities arising from the combination of growth and interconnections be addressed through legislation or regulations related to:

— Stablecoin issuers' reserve assets;

— Scope of permissible activities and prudential requirements for banking organizations,[29] as well as greater oversight of the affiliations and activities of nonbank stablecoin issuers;

— Prudential requirements for SEC- and CFTC-regulated entities;

— State charter and license frameworks;

— Regulatory and examination authority over third-party service providers;

— State insurance law and regulations;

— Registration or reporting requirements for private fund advisors (noting that private funds and certain types of investors may be difficult to oversee); and

— Jurisdiction of, and enforcement actions by, the SEC and CFTC.

The FSOC Report also identifies a number of interconnections within the digital asset industry, and across digital asset platforms, investors, and other counterparties, that could lead to substantial distress if one link were to fail. FSOC uses as case studies recent financial distress at hedge fund Three Arrows Capital and the collapse of the TerraUSD stablecoin, indicating that FSOC has been studying how such situations arise and will watch for signs of future adverse events among firms engaged in digital asset activity.

The FSOC Report warns of a number of regulatory implications for digital asset firms:

— FSOC reiterated the SEC's long-standing position that a digital asset platform may need to register with the SEC as an exchange, broker-dealer, investment company, or clearing agency, or otherwise operate under or obtain an appropriate exemption, depending on its functions. Furthermore, FSOC stated that certain digital asset platforms are likely currently listing securities in

[28] *See* Federal Reserve, Office of the Comptroller of the Currency ("**OCC**") and FDIC, Joint Statement on Crypto-Asset Risks to Banking Organizations (Jan. 3, 2023). *See, also*, OCC, Semiannual Risk Perspective 20-21 (Dec. 8, 2022); Mishra, Knight, Crypto Bank Silvergate Shares Plunge 46% After $8.1B Withdrawal in Q4 Prompts 200 Job Cuts, CoinDesk (Jan. 5, 2023).

[29] *See, e.g.*, Financial Stability Board, Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative Document (Oct. 11, 2022); Basel Committee on Bank Supervision, Prudential treatment of cryptoasset exposures (Dec. 2022), for implementation by January 2025.

violation of exchange, broker-dealer, or other registration requirements, as SEC Chairman Gary Gensler has often warned.

— FSOC takes the position that current regulation of digital asset platforms through MSB laws is inadequate to address systemic risk (even though there are federal laws with respect to MSBs) as: (i) MSB regulation is designed for AML and consumer protection purposes and not comprehensive risk mitigation or market integrity goals, (ii) state-level MSB laws provide for only limited loss absorbing buffers and vary widely in strength and application of capital requirements, and (iii) state-level regulators may consider a platform's non-money transmission activity but do not limit such activity as strictly as bank charters do.[30]

— FSOC recognizes that state charter frameworks offer some protections (*e.g.*, New York, Wyoming, Louisiana, and Nebraska have enacted certain prudential standards) but notes that state regulators may not have sufficient or comprehensive visibility into activities of affiliates or subsidiaries,[31] thus implying that a regulatory framework more similar to the Bank Holding Company Act may be appropriate.

— Firms involved in the commodities derivatives market as trading organizations, clearing organizations, or intermediaries may be subject to certain registration and other requirements. FSOC states that central clearing may limit risks of interconnectedness by reducing the likelihood that a shock of a single counterparty's default will ripple throughout the futures markets. In the swaps market, required review or approval by the CFTC for clearing organizations to clear certain swaps may limit availability of digital asset swaps and further reduce risk.[32]

— FSOC noted that it may be difficult to assess the capital and liquidity buffers held by large digital asset platforms due to lack of information, possibly signaling an area of future regulatory attention.[33]

Pending further legislative or regulatory developments, firms can take steps to prepare for possible enhanced oversight and position themselves with respect to financial stability goals. Firms, including stablecoin issuers, could adopt or improve governance structures, risk management, financial reporting, auditing and internal control standards, and capital and liquidity guidelines. All firms should consider enhanced third-party vendor and service agreement diligence and risk management. Custody providers should consider the commercial law and operational implications of whether customer funds are considered property of the bankruptcy estate in the event of insolvency, which could stem rapid withdrawals. Firms could also implement new or increase existing counterparty exposure limits to help avoid excessive exposures.

V. Monitor the legislative and regulatory process at the U.S. federal level, even if you are state-regulated or a foreign company.

Firms should closely monitor the legislative landscape in 2023, as the Reports signaled interest in enacting targeted federal legislation with respect to digital assets.

Furthermore, Treasury called for the establishment of a federal framework for payments regulation, including for "nonbank companies that are involved in the issuance, custody, or transfer of money or money-like assets,"[34] which could encompass fintechs offering digital asset services, in addition to capturing current payment providers that may not be federally regulated. In the meantime, Treasury plans to convene state supervisors responsible for virtual asset service providers to promote standardization and coordination of licensing and anti-money laundering obligations, as well as supervision.

Additionally, DOJ expresses support for legislation that would: (1) include digital asset service providers in anti-tip-off statutes, (2) amend the law for operation of an unlicensed money transmission business to

[30] FSOC Report, at 98-99.
[31] FSOC Report, at 99.
[32] FSOC Report, at 98.
[33] FSOC Report, at 36-37.
[34] Treasury Payments Report, at 47.

increase penalties and capture more digital asset-related activity, (3) increase the statute of limitations period for all digital asset-related crime to 10 years, (4) expand the civil and criminal forfeiture power with respect to digital assets, (5) increase the sentencing guidelines for anti-money laundering crimes under the BSA, (6) subject NFT platforms to the U.S. AML regulatory framework, and (7) amend the venue provisions of federal statutes to permit prosecution in any district where the victim of a digital assets-related offense or other cybercrime is found. However, the White House states only that the "President will evaluate whether to call upon Congress to" pass legislation to take such steps.[35]

To address regulatory gaps it identified in its Report, FSOC recommends federal legislation: (1) providing for rulemaking authority for federal financial regulators over spot markets for digital assets that are not securities (but without interfering with or weakening current regulatory authorities), (2) creating a comprehensive prudential framework for stablecoin issuers, and (3) providing for consolidated supervision of "crypto-asset entities." FSOC also calls for the study of the conflicts and risks related to vertical integration of digital asset markets and activities, particularly those providing direct retail access, which could prompt additional federal legislative developments, such as regulation of affiliations.[36]

In addition, the White House expresses support in the OSTP Climate Report for exploring executive actions and legislation that would "limit or eliminate the use of high energy intensity consensus mechanisms for crypto-asset mining" (and, in particular, proof-of-work mechanisms).[37]

The bankruptcy of FTX will provide fuel to regulators, law enforcement and others who seek to enact legislation providing for stricter oversight of digital assets and industry players.[38]

VI. Prepare for the U.S. federal government to focus on the potential of domestic and international payments systems, rather than benefits from the broader digital asset sphere.

In contrast to the enforcement focus and cautionary tone of other reports, the Treasury Payments Report describes non-cash payments—using both fiat currency and digital assets—as the way of the future. Themes of the Report include developing systems for faster and cheaper consumer payments, maintaining stability and liquidity among financial institutions, and expanding financial market access to the unbanked and underbanked.

> The Treasury Payments Report allows for the possibility that a U.S. CBDC, instant payment systems, and stablecoins could exist simultaneously and could be interoperable, but indicates that such benefits would depend on design choices, which intermediaries have access and applicable regulatory frameworks.

— Instant Payment Systems

Instant payment systems process smaller interbank transfers (that would not typically be sent by wire transfer) such that funds are instantly available to recipients, unlike, for example, potentially multi-day settlement of FedACH transactions. These payments typically use bank deposit money but ultimately settle through the central bank payment rails. The Treasury Payments Report speaks favorably of instant payment systems, citing them as having the potential to lower transaction costs while providing greater stability and

[35] The White House, FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets (Sept. 16, 2022).
[36] *See* FSOC Report, at 112-119.
[37] OSTP Climate Report, at 7.
[38] *See*, *e.g.*, CFTC, Testimony of Chairman Rostin Behnam Before the U.S. Senate Committee on Agriculture, Nutrition, and Forestry (Dec. 1, 2022) ("I strongly believe that we need to move quickly on a thoughtful regulatory approach to establish guardrails in these fast-growing markets of evolving risk, or they will remain an unsafe venture for customers and could present a growing risk to the broader financial system"); Treasury, Statement by Secretary of the Treasury Janet L. Yellen on Recent Crypto Market Developments (Nov. 16, 2022) ("The federal government, including Congress, also needs to move quickly to fill the regulatory gaps the Biden Administration has identified").

reliability than stablecoins. However, the administration does not view the adoption of instant payment systems as a substitute for potential issuance of a CBDC. A senior administration official stated on record that one may choose to use a CBDC "for a number of other reasons" unrelated solely to instant settlement.[39]

The Treasury Payments Report notes that insured depository institutions are currently eligible to participate in The Clearing House's instant payment system (Real Time Payments) and highlights as a promising development that the FedNow Service will be available to U.S. depository institutions and U.S. branches of foreign banks as early as 2023. Treasury states that FedNow is expected to enhance speed and efficiency, competition, and inclusion in payment systems. Still, Treasury expects frictions that may limit the benefits of instant payment systems, including slow adaptation by consumers, businesses, and financial institutions of habits and procedures and that access to instant payment systems is generally limited only to depository institutions.[40] Whether access may potentially be extended to other nonbanks remains a key open question.

— Stablecoins

The Treasury Payments Report defines stablecoins as "digital assets issued by private entities that aim to maintain a stable value relative to a national currency or other reference assets, often utilizing distributed ledger technology, such as blockchain."[41] Treasury notes that stablecoins are primarily used today to facilitate trading, lending or borrowing of other digital assets, and questions whether they may in fact become a widespread means of payment, including for more efficient cross-border transactions. The Treasury Payments Report generally expresses greater skepticism of stablecoins compared to CBDC and instant payments. It notes that CBDC could crowd out "potentially risky forms of private money, such as money issued by non-bank intermediaries" (*i.e.*, weaker stablecoins), notwithstanding previous statements by Chairman Powell that CBDC and stablecoins could coexist.[42] Citing the President's Working Group Report on Stablecoins and articles about Terra and Tether,[43] the Treasury Payments Report notes that some stablecoins lack reliable means to maintain a stable value and may be vulnerable to runs, especially in the absence of quality design or adequate regulatory oversight (including of issuers, wallet providers and exchanges). The Treasury Payments Report also describes certain challenges for stablecoins related to distributed ledger technology ("**DLT**"), including network congestion, high fees for permissionless blockchains, and limited functionality of permissioned blockchains.[44]

The FSOC Report echoes these concerns and identifies stablecoin issuers' asset holdings as a key interconnection between the traditional financial system and developments in stablecoin markets.[45] FSOC argues that, if a stablecoin run leads to a fire sale of any traditional assets backing a stablecoin, traditional financial markets could experience dislocations and the financial institution holding the assets could face pressure, especially where stablecoin reserves are opaque and/or illiquid. Firms involved in stablecoin arrangements should assess the quality and composition of stablecoin reserves and the adequacy of their public statements such as monthly asset attestations.

Treasury also signaled that it has heightened concerns about widely-adopted stablecoins with respect to anti-money laundering ("**AML**") matters. As a result, firms that currently engage in or intend to engage in stablecoin arrangements should plan for increased regulatory scrutiny, particularly of their governance practices and AML and sanctions compliance.

— U.S. CBDC

[39] The White House, Background Press Call by Senior Administration Officials on the First-Ever Comprehensive Framework for Responsible Development of Digital Assets (Sept. 15, 2022).
[40] Treasury, Remarks by Under Secretary for Domestic Finance Nellie Liang at the Brookings Institution (Sept. 23, 2022).
[41] Treasury Payments Report, at 16.
[42] Treasury Payments Report, at 20.
[43] *See* President's Working Group on Financial Markets, FDIC and OCC, *Report on Stablecoins* (Nov. 2021).
[44] Treasury Payments Report, at 18.
[45] FSOC Report, at 15.

Many of the Reports discuss the potential for a U.S. CBDC. In particular, the Treasury Payments Report and OSTP CBDC Report discuss in detail the policy objectives, technical design choices, and resources for a potential U.S. CBDC. Both reports decline to take a position on whether a CBDC would be in the best interest of the United States or advocate for any particular model. However, the OSTP CBDC Report does explicitly assume that some form of permissioned system would be more appropriate since a trusted central entity is involved (namely, the Federal Reserve), without assuming use of a DLT system.

— The Treasury Payments Report describes a two-tier approach for a CBDC where banks (and possibly nonbank financial intermediaries) onboard and manage payments, while the Federal Reserve records account balances, as "more feasible" than a single-tier approach with the Federal Reserve alone. This is the closest the Report comes to advocating for a specific design choice, and is largely based on general concerns about the U.S. government's access to financial data. However, any intermediaries would need to implement appropriate AML and sanctions programs and could be subject to institution holding limits on wholesale CBDC to support financial stability in times of stress.

— Both traditional and nonbank market participants across the payments and digital asset spaces may consider their future offerings, and seek opportunities or face competition based on design choices and policy considerations, including that a CBDC could:

  - Be based on either a centralized payment system or DLT; if DLT is used, then the CBDC would most likely be based on a permissioned blockchain to speed transactions and reduce energy consumption; regardless, CBDC would include some element of centralization given the Federal Reserve's involvement;
  - Be settled 24/7 (or at least have longer operating hours than Fedwire), including by intermediaries for wholesale CBDC;
  - Lower the cost of payments below that of instant payment systems, depending on competitive dynamics including the range of institutions with access;
  - Be held by consumers in digital wallets with payment verification services conducted by intermediaries;
  - Enable transaction programmability or support tokenization, including for digital assets; and
  - Be connected to cross-border payments systems and/or foreign CBDCs.

In terms of process, the Executive Order calls for DOJ to determine whether legislative changes would be necessary to issue a CBDC, but senior administration officials stated they would not "get ahead of [themselves] while the Fed studies the issue."[46] Additionally, although the Reports call for creation of an inter-agency CBDC working group, led by Treasury rather than the Federal Reserve, as well as further research and development on a potential CBDC, officials acknowledge that, even if authorized, implementation would likely take years.

…

CLEARY GOTTLIEB

[46] The White House, Background Press Call by Senior Administration Officials on the First-Ever Comprehensive Framework for Responsible Development of Digital Assets (Sept. 15, 2022).