August 2022

Skadden

The Distributed Ledger

Blockchain, Digital Assets and Smart Contracts

Treasury and New York Enforcement Actions Reveal Continued Focus on the Cryptocurrency Industry and Regulators' Priorities

Recent actions by the New York State Department of Financial Services (NYDFS or Department) and the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) demonstrate a continued scrutiny by both regulators of activity in the cryptocurrency industry. They highlight regulators' concerns about money laundering and other suspicious transactions using cryptocurrencies, and the need for robust compliance and cybersecurity programs.

On August 1, 2022, NYDFS imposed a $30 million fine on Robinhood Crypto, LLC (RHC) for violations of the Department's anti-money laundering (AML) and cybersecurity rules. RHC's parent, Robinhood Markets Inc., publicly disclosed the investigation in securities filings a year ago, and NYDFS has been active in licensing and regulating companies involved with digital assets for a number of years. Nonetheless, the settlement and fine were significant because it is the Department's first foray into enforcement in the crypto sector.

A week later, on August 8, 2022, OFAC imposed blocking sanctions on the decentralized cryptocurrency mixing service Tornado Cash and numerous wallet addresses associated with it. The sanctions followed a similar designation by OFAC of Blender.io in May 2022, the first time OFAC sanctioned a mixer.

The action against Tornado Cash is the latest in a string of sanctions designations and enforcement actions by OFAC involving various participants in the cryptocurrency industry, including the April 2022 designations of Hydra Market, the world's largest darknet market; various wallet addresses associated with the North Korea-backed hacker syndicate Lazarus Group; and the Russian cryptocurrency mining firm BitRiver.

This article discusses the details of the RHC and Tornado Cash actions and explains their implications for cryptocurrency businesses.

RHC Consent Order

RHC is licensed by NYDFS to operate in New York State as a "virtual currency business" and money transmitter. According to the consent order from NYDFS agreed to by RHC (Order), the Department conducted an examination of RHC between January and September 2019 that uncovered serious deficiencies in RHC's compliance function across multiple areas, including its Bank Secrecy Act (BSA) and AML and cybersecurity compliance programs.

Following the examination, NYDFS commenced an enforcement investigation and found that the deficiencies resulted in violations of NYDFS's Virtual Currency Regulation (23 NYCRR Part 200), Money Transmitter Regulation (3 NYCRR Part 417), Transaction Monitoring Regulation (23 NYCRR Part 504), and Cybersecurity Regulation (23 NYCRR Part 500).[1]

BSA/AML Deficiencies

The Order states that RHC's BSA/AML compliance program improperly relied on the programs of its parent company, Robinhood Markets, Inc., and its affiliate, Robinhood Financial, LLC. NYDFS found that the parent's and the affiliate's programs were themselves staffed inadequately and failed to address all the particular risks applicable to virtual currency businesses. NYDFS also found that RHC's problems were exacerbated by the fact that its chief compliance officer lacked sufficient experience and prominence within the parent's organizational structure, according to the Order.[2]

NYDFS also found that RHC failed to transition in a timely fashion from a manual transaction monitoring system that was inadequate for RHC's size, customer profiles and transaction volumes. While the use of a manual system does not inherently violate NYDFS regulations, the Department cited an average volume of 106,000 transactions daily totaling $5.3 million, as of September 30, 2019, concluding that RHC's manual system was inadequate to support a compliant AML program.

According to the Order, the inadequacy of RHC's manual transaction monitoring processes and the staffing deficiencies led to a backlog of over 4,300 alerts. An external compliance consultant retained by RHC in December 2019, shortly before the NYDFS's examination, also highlighted RHC's lack of an automated transaction monitoring program as a weakness. Despite that finding and the growing alert backlog, RHC failed to implement an automated transaction monitoring system until April 2021.

NYDFS further found that RHC employed an extremely high and arbitrary threshold amount — $250,000 in cumulative transaction volume over a six-month period — to generate exception reports under its two crypto-specific transaction monitoring rules. The Department deemed that figure unacceptable given the transaction volume, and noted that during the approximately eight-month examination period, RHC filed only two suspicious activity reports in response to crypto-specific transaction alerts.

Cybersecurity Deficiencies

The Order also stated that RHC did not have internal support exclusively devoted to cybersecurity when the services it was relying on from its affiliate and parent were not fully compliant with the Department's Cybersecurity Regulation. Additionally, as outlined in the Order, the Cybersecurity Regulation requires that a covered entity's chief information security officer report annually to the board of directors and that the board approve the entity's cybersecurity policies at least annually. RHC did not meet either accountability requirement, NYDFS found.

While RHC has more recently devoted significant funding to develop its cybersecurity policies, the Order says, it had not done so during DFS's investigation, and RHC's cybersecurity compliance program was lacking in a number of areas. During this period, RHC had not conducted an annual risk assessment, nor had it implemented appropriately detailed policies and procedures, including data governance and classification, IT asset management, business continuity and disaster recovery planning, or incident response activities.

The Order highlights the importance of building and maintaining robust cybersecurity procedures commensurate with business size, along with maintaining strict accountability measures around reporting compliance both internally and to the Department. The Department also emphasized the importance of internal reporting measures with some teeth — particularly where a company is relying on cybersecurity infrastructure, personnel, and services from a parent or affiliate to maintain compliance.

Improper Compliance Certifications

In light of the significant issues NYDFS identified with respect to RHC's BSA/AML and cybersecurity programs, the Order states that RHC improperly certified compliance with the Department's Transaction Monitoring Regulation and Cybersecurity Regulation. Both regulations require regulated entities to certify annually their compliance with the relevant compliance obligations. According to NYDFS, companies should only make such certification if their programs are fully compliant with the applicable regulations. The Department maintains that, in light of the deficiencies set forth in the Order, RHC's 2019 certifications to the Department should not have been made and, therefore, constituted a violation of law.

[1] NYDFS also found that RHC failed to comply with certain consumer protection requirements, including not maintaining a distinct, dedicated phone number on its website for consumer complaints. NYDFS also found that RHC breached notification obligations under the terms of the Supervisory Agreement it entered into when it obtained its license to operate a virtual currency business in New York State.

[2] For example, RHC's chief compliance officer reported to RHC's director of product operations, rather than to a legal or compliance executive at the parent or affiliate.

Outside Consultant Required

The Order also states that RHC's cooperation and engagement with NYDFS, at least initially, did not meet expectations for a licensed institution. For example, the Department found that information provided was either delayed, insufficient or both. It also found that RHC failed to disclose investigations by federal and state regulators of an RHC-affiliated entity, in violation of reporting obligations under RHC's Supervisory Agreement. More generally, NYDFS found significant shortcomings in the management and oversight of RHC's compliance programs, including a failure to maintain an adequate culture of compliance.

Under the settlement, RHC is required to retain an independent consultant for 18 months to perform a comprehensive evaluation of RHC's compliance with the Department's regulations and RHC's remediation efforts with respect to the identified deficiencies and violations, with possible extensions in scope and duration at the sole discretion of the NYDFS.

Implications of the Consent Order

Given NYDFS's prominent role in the regulation of financial services and products in New York State — and the leading role it has traditionally played among state banking and financial regulators more broadly — this settlement is noteworthy.

NYDFS's action signals its priorities. The case offers a potential preview of the Department's crypto enforcement priorities going forward. NYDFS has made clear that its stringent AML and cybersecurity requirements apply to licensed virtual currency businesses as well as to traditional financial services companies under the Department's purview. The Order suggests that the Department may increase enforcement of those requirements as applied to virtual currency businesses as a tool to ensure compliance across the board.

Strict transaction monitoring and cyber security compliance is expected. The Order brings additional clarity to the Department's regulatory expectations for the digital asset ecosystem, particularly with respect to the specific regulations the NYDFS found RHC to have violated. Given the Department's emphasis that strict compliance with the Transaction Monitoring Regulation and Cybersecurity Regulation is required before a regulated entity can properly certify to such compliance with the Department, virtual currency businesses in New York State would be well advised to use the certification process as an opportunity to conduct a formal review of their BSA/AML and cybersecurity compliance programs and practices, including reviews by outside legal and compliance advisers, and then develop and begin implementing a remediation plan, if necessary, before submitting certifications to NYDFS.

The case could serve as precedent for other regulators. Finally, the action may provide a roadmap for other regulators and law enforcement authorities when establishing their own compliance expectations and best practices in the burgeoning crypto space. Companies that find themselves under examination by state or federal regulators may want to consult with external advisors during the examination process to help them resolve any deficiencies before they escalate into an enforcement action.

Tornado Cash Sanctions

On August 8, 2022, OFAC sanctioned Tornado Cash, naming it as a Specially Designated National (SDN) and added Tornado Cash along with more than 40 Ethereum and USD Coin wallet addresses associated with the service to the SDN List. OFAC called Tornado "a notorious virtual currency mixer," and accused it of facilitating the laundering of $7 billion in virtual currencies since 2019, including $455 million of the $625 million stolen by the North Korea-backed Lazarus Group during its March 2022 hack of Axie Infinity's Ronin Network.

As a result of its designation, U.S. persons are generally prohibited from using Tornado Cash or transacting with its associated wallet addresses, and any property or interests in property belonging to Tornado Cash must be blocked if they come within the U.S. or the possession or control of a U.S. person.

Tornado Cash operates on the Ethereum blockchain. Like other cryptocurrency "mixers," "tumblers" or "blenders," it allows users to send cryptocurrency to one or more wallet addresses owned by the service, where it is pooled with the assets of other users. As a result of this pooling, when a user later instructs Tornado Cash to send funds to an address, it becomes difficult, if not impossible, to trace the payment back to the coins the user initially placed into the mixing service.

OFAC's action could have wider implications for mixers and DeFi more broadly:

The Tornado Cash action raises questions for other mixers. Proponents of crypto asset mixing services often note the various legitimate reasons to seek privacy and anonymity in conducting financial transactions. But the sanctions against Tornado Cash taken together with OFAC's designation of Blender.io, a smaller mixing protocol operating on the Bitcoin blockchain, raise existential questions for other mixers. At the least, they may be concerned about how to respond to OFAC's Tornado Cash action.

The sanctions show that OFAC is willing to target DeFi platforms. Unlike mixing or tumbling services that are operated by a centralized administrator, Tornado Cash is a decentralized finance, or "DeFi," protocol with operational and governance decisions made

by a decentralized autonomous organization (DAO). OFAC's willingness to designate a DeFi protocol like Tornado Cash sends a clear message to the market that, whether or not a platform qualifies as a regulated institution or is operated by an administrator, OFAC will take action where it perceives that the platform may be used to facilitate financial crime.

This dynamic raises significant questions about the scope of the U.S. government's expectations regarding appropriate risk mitigation and, more specifically, who it sees as responsible for developing and implementing such risk mitigation measures.

Treasury may be reluctant to imply that DiFi platforms are financial institutions. OFAC's press release makes clear that OFAC's designation of Tornado Cash is based on allegations that it was used extensively to launder the proceeds of criminal activity. In October 2020, under similar circumstances, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) assessed a $60 million civil money penalty against Larry Dean Harmon, the founder and administrator of Helix and Coin Ninja LLC, two cryptocurrency mixing services. FinCEN's enforcement action cited Mr. Harmon's failure to register as a money services business and various AML compliance program deficiencies at Helix and Coin Ninja.

However, notwithstanding the significant money laundering risk highlighted by Tornado Cash's designation, OFAC's press release does not address the AML implications of the designation, and FinCEN has not, to date, announced any action against Tornado Cash or associated persons. It is possible the Treasury Department is reticent about taking action against a DeFi platform, because doing so would imply that such platforms constitute money services businesses and are subject to regulation as financial institutions — a conclusion that would have far-reaching consequences across the crypto sector.

Bloom and Dragonchain Cases Highlight Important Factors the SEC Considers in Treating Digital Tokens as Securities

In two recent enforcement actions, the U.S. Securities and Exchange Commission (SEC) has taken the position that some digital token offerings constitute securities under *SEC v. Howey*.[3] They come on the heels of a recent enforcement action alleging insider trading in crypto currencies by a Coinbase employee, where the SEC alleged that various other digital tokens constitute securities. Together these cases shed light on the factors the agency will consider in deciding whether to treat a cryptocurrency as a security, including promotional language and a differential between the offering price and the token's consumptive value.

Bloom ICO Settlement

On August 9, 2022, Bloom Protocol, LLC, a technology startup that offered and sold Bloom Tokens (BLTs) through an initial coin offering (ICO), settled claims by the SEC that Bloom offered unregistered securities.

As part of the settlement, Bloom agreed to a consent decree with findings that, between November 2017 and January 2018, the Bloom ICO raised approximately $31 million. The SEC found that BLTs constituted securities under the *Howey* test and that the ICO was not registered nor exempt from the registration requirements. The SEC thus concluded that Bloom violated sections 5(a) and 5(c) of the Securities Act of 1933.

The SEC found that BLTs constituted securities because "the structure of the platform and the marketing demonstrate that the BLT purchasers had a reasonable expectation of profit through Bloom's efforts to develop the token's uses and increase its value." The SEC cited the incongruity of the offering price and the consumptive value of BLT, noting that, although Bloom required token purchasers to agree they were buying BLT for its "utility" rather than as an investment, the platform was not fully developed at the time of the sale and Bloom expressly disclaimed any representations that BLTs "shall confer any actual and/or exercisable rights of use, functionality, features, purpose, or attributes in connection with the Bloom platform."

Moreover, Bloom's promotional materials — posted on its website, in blog posts, on social media, online videos, and other media targeting blockchain and crypto asset enthusiasts — described the purchases as an "investment" with "rounds of financing," and stated that Bloom would use funds raised from the token sale to build out its platform. According to the SEC, some investors also stated on social media that they bought BLT as an investment.

Under the settlement, Bloom agreed to cease and desist from further violations and to pay a $300,000 civil penalty. The SEC said that Bloom had voluntarily taken remedial efforts to prepare for registration.

Bloom also agreed to certain undertakings, including registering BLTs as a security; issuing a press release notifying the public about the settlement and the SEC order; notifying purchasers about potential claims; and offering rescission to purchasers. If Bloom does not abide by the undertakings, the civil penalty will be increased to approximately $31 million.

[3] 328 U.S. 293 (1946)

Dragonchain Enforcement Action

On August 16, 2022, the SEC filed an enforcement action against Dragonchain, Inc. (Dragonchain), two related entities (Dragonchain Foundation and the Dragon Company), and their founder, Joseph John Roets (together Defendants), in the U.S. District Court for the Western District of Washington alleging violations of Sections 5(a) and 5(c) of the Securities Act of 1933.

The SEC alleges that Defendants engaged in unregistered offerings of securities via a "presale" of a crypto asset known as Dragon (DRGN) in August 2017, an ICO of DRGNs between October and November 2017, and continued sales of DRGNs between 2019 and 2022.

According to the complaint, the presale and ICO raised approximately $14 million from over 5,000 investors globally, while the continued sales of DRGNs between 2019 and 2022 raised an additional $2.5 million. The SEC claims that the funds were used to develop Defendants' technology and for business expenditures, including marketing of the Defendants' services.

Notably, the complaint alleges that Dragonchain told potential investors that the value of DRGN would grow as the Dragonchain ecosystem evolved and Dragonchain retained a market maker for DRGNs. Additionally, Dragonchain is alleged to have used sales-based commissions to entice crypto influencers to market DRGNs.

The SEC is seeking permanent injunctions against all Defendants, disgorgement with prejudgment interest and civil penalties pursuant to Section 20(d).

Takeaways From Bloom and Dragonchain Cases

The Bloom and Dragonchain actions are the latest examples of the SEC's position that certain ICO-era digital token offerings constitute securities under *Howey*. Together with the Coinbase employee case, they show that the SEC is asserting jurisdiction over a range of cryptocurrency matters. See our July 26, 2022, client alert "Cryptocurrency Insider Trading Case Could Have Broader Ramifications for the Industry."

In both the Bloom enforcement order and the Dragonchain complaint, the SEC's analyses focus on the issuers' promotional activities, including language used in describing the digital asset and offering, as well as the development teams' *bona fides*, in marketing materials and the white paper. It also looked to the functionality of the protocol at the time of the offering and the price at which the tokens were offered, as compared to their supposed consumptive value at the time.

The Fed Aligns With the OCC and FDIC on Banks' Cryptocurrency Activities as Senators Question the OCC's Approach, Citing Risks

On August 10, 2022, four prominent senators wrote Acting Comptroller of the Currency Michael J. Hsu, expressing concern that guidance issued by the Office of the Comptroller of the Currency (OCC) to national banks and federal savings associations regarding cryptocurrency activities was not issued in full coordination with all stakeholders and exposed the banking system to unnecessary risk. The letter from Senators Elizabeth Warren (D-Mass.), a member of the Senate Banking Committee; Dick Durbin (D-Ill.), chairman of the Senate Judiciary Committee; Sheldon Whitehouse (D-R.I.); and Bernie Sanders (I-Vt.) cited the recent volatility of cryptocurrency markets.

Shortly thereafter, on August 16, 2022, the Board of Governors of the Federal Reserve System (Federal Reserve) issued an advisory (Fed Advisory) to the Reserve Banks and all banking organizations it supervises reiterating that supervised institutions may engage in crypto asset-related activities and outlining steps that banks must take before doing so.

The Fed Advisory brings the Federal Reserve's formal position on crypto assets into closer alignment with the OCC's and that of the Federal Deposit Insurance Corporation (FDIC), as articulated in an April 7, 2022, financial institution letter on the topic.

While the timing of the Fed Advisory is noteworthy in its own right, it is also significant for Federal Reserve-supervised institutions that may have been hesitant to enter or expand their footprint in the digital asset space. The Fed Advisory also reinforces the view that the federal banking regulators are guiding crypto asset-related activities toward regulated institutions to foster greater oversight of the sector.

The growing consensus among the federal banking regulators to institute a de facto supervisory sign-off process for digital asset activity at regulated institutions blunts to some extent the criticisms presented in the senators' letter. Still, the senators' letter opens a new front in the ongoing debate over cryptocurrency regulation and shows that consumer protection and financial stability remain key concerns for policymakers.

Senators Oppose Certain OCC Interpretive Letters

In light of recent events, the senators urged the OCC to (a) withdraw four interpretive letters it has issued concluding that national banks and federal savings associations have the governing authority to engage in certain cryptocurrency activities and (b) jointly replace them with more comprehensive and restrictive guidance in conjunction with other federal regulators, including the Federal Reserve and FDIC.

The first three letters cited by the senators (OCC Interpretive Letters 1170, 1172, and 1174), issued under the Trump administration, found that national banks and federal savings associations have the authority to (a) provide cryptocurrency custody service for customers, (b) hold deposits that serve as reserves for certain stablecoins, and (c) use independent node verification networks (INVNs) and stablecoins for payment activities, respectively. The fourth letter (OCC Interpretive Letter 1179), was issued under acting Comptroller Hsu, a Biden appointee, and largely affirmed the analysis of the first three interpretive letters.

- **OCC Interpretive Letter 1170** (July 22, 2020) confirmed the authority of national banks and federal savings associations to provide cryptocurrency custody services. The OCC determined that these services fall within "longstanding authorities to engage in safekeeping and custody activities" and that an institution may provide cryptocurrency custody services on behalf of its customers, including holding the unique cryptographic keys associated with cryptocurrency. The OCC described cryptocurrency custody services as merely "a modern form of ... traditional bank activities."
- **OCC Interpretive Letter 1172** (September 21, 2020) concluded that a national bank or federal savings association may hold stablecoin reserves as a service to bank customers. The OCC found that stablecoin issuers may place assets backing the stablecoin in a reserve account to provide assurance that the issuer has sufficient assets backing the stablecoin where there is a hosted wallet. The OCC emphasized that the letter only addresses the use of stablecoin backed on a 1:1 basis by a single fiat currency, where the bank verifies at least daily that reserve account balances are always equal to or greater than the number of the issuer's outstanding stablecoins.
- **OCC Interpretive Letter 1174** (January 4, 2021) concluded that a national bank or federal savings association may validate, store and record payments transactions by serving as a node on an INVN, and that an institution may use INVNs and related stablecoins to carry out other permissible payment activities. The OCC emphasized that the institution must conduct these activities consistent with applicable law and safe and sound banking practices.
- **OCC Interpretive Letter 1179** (November 18, 2021) clarified that the activities addressed in Interpretive Letters 1170, 1172, and 1174 are legally permissible for a national bank or federal savings association to engage in, provided the bank can demonstrate to the satisfaction of its supervisory office that it has controls in place to conduct the activity in a safe and sound manner. The OCC indicated that the institution should notify its supervisory office in writing of its intention to engage in any of these activities and should not engage in them until it receives written notification of the supervisory office's non-objection. The OCC added, however, that institutions already engaged in cryptocurrency, distributed ledger or stablecoin activities as of the date of the letter not need to obtain supervisory non-objection, although the OCC expects that a bank that has commenced such activity would have provided notice to its supervisory office.

The senators' letter does not directly challenge the OCC legal analysis underpinning the interpretive letters, which likely will be at the center of any joint regulatory process that may ensue.

In addition to their criticism of the interpretive letters, the senators also seek detailed information from the OCC, including the specific institutions that have received permission to engage in cryptocurrency-related activities and the types of activities in which the institutions are engaged.

This signals that both the OCC and OCC-regulated institutions that engage in cryptocurrency-related activities may come under additional investigative and oversight scrutiny by Congress in the months and years ahead. It suggests that legislative activity to define permissible activities and regulatory jurisdiction over them will continue to increase as the current session of Congress ends and the next session begins.

Federal Reserve Advisory

The Fed Advisory, titled "Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organizations," begins by touting the potential opportunities that crypto assets and related technologies present, while cautioning institutions regarding their inherent risks. Among the risk factors, it highlights (a) the operational risk posed by the nascent and quickly evolving technology underlying crypto assets, (b) the anti-money laundering compliance risk associated with the lack of transparency inherent to crypto assets, and (c) the broader risk to financial stability that the widespread adoption of crypto assets could create.

Notwithstanding these risks, the Fed Advisory states that Federal Reserve-supervised banks may engage in crypto asset-related activities provided they have satisfied certain preconditions:

- **Legal permissibility:** Banking organizations should first establish that the activity in which they seek to engage is legally permissible under federal and state law and assess whether any specific filings are required under relevant laws or regulations.
- **Notification:** After determining the activity is permissible, the bank should notify its lead supervisory point of contact at the Federal Reserve of the bank's intent to engage in the activity. Even if the bank is already engaged in the activity, it should notify its point of contact promptly if it has not already done so. The Fed Advisory also encourages state member banks to notify their state regulators prior to engaging in such activity.

- **Risk management:** Banking organizations should have in place an adequate risk management framework, including systems and internal controls, to monitor and manage the risks presented by crypto assets and allow the bank to conduct its crypto asset-related activities in a safe and sound manner.

While the Fed Advisory is not a general authorization to engage in crypto asset-related activities across the board, it will nonetheless provide comfort to institutions that desire to participate in the crypto space but have been uncertain as to how the agency might perceive such activities. It remains to be seen whether the Fed Advisory will be met with same kind of congressional push-back expressed in the senators' letter to Acting Comptroller Hsu.

The FTC Joins Banking Regulators and the SEC in Scrutinizing Cryptocurrency Activities

An August 9, 2022, order by the Federal Trade Commission (FTC) denying Bachi.Tech Corporation's petition to quash a civil investigative demand (CID) revealed details about the agency's investigation of that Web3 company, and marked the first time that the FTC is known to have investigated an entity in this sector. The investigation focuses on a December 2021 security breach, in which hackers withdrew digital assets valued between $150 million and $200 million from two BitMart wallets on the BitMart cryptocurrency exchange operated by Bachi.Tech.[4]

The investigation may be a harbinger of future FTC activity in this area. President Biden's March 9, 2022, Executive Order on digital assets directed the FTC to consider the extent to which privacy or consumer protection measures within its jurisdiction may be used to protect consumers of digital assets and whether additional measures may be needed. (See our March 22, 2022, client alert "Executive Order Aiming To Coordinate Digital Assets Policies May Bring Much-Needed Clarity.") In addition, an FTC Data Spotlight issued in June 2022 reported that, since the start of 2021, more than 46,000 people have reported losing over $1 billion in crypto currencies to scams.

According to the FTC's August 9, 2022, order in the Bachi.Tech case, the agency is examining BitMart's representations concerning its advertised exchange services; allegations that consumers have been denied access to their accounts; and concerns about the security of customer accounts in light of the December 2021 security breach.

The FTC is seeking to determine whether Bachi.Tech's marketing and operation of BitMart (i) constituted unfair or deceptive online practices, (ii) constituted deceptive or unfair consumer privacy and/or data security practices in violation of Section 5 of the FTC Act, or (iii) violated the Gramm-Leach-Bliley Act (GLB Act). The CID sought a variety of information relating to Bachi.Tech's operation of the BitMart cryptocurrency exchange, which the company operates with Spread Technologies LLC (Spread). The FTC issued virtually identical CIDs to Bachi.Tech and Spread on May 11, 2022, and the commission previously rejected Spread's petition to quash on July 18, 2022.

In many ways, the FTC's CID seeks the type of information the agency typically demands when it investigates a data security incident, such as:

- Bachi.Tech's knowledge of, involvement in, and ability to prevent, security breaches for currency investments traded on its BitMart platform;
- reported fraud associated with BitMart and its customer service processes;
- the adequacy of its customer service operations;
- the veracity of BitMart's representations about its services and security;
- the structure of Bachi.Tech's and BitMart's operations;
- methods used to market BitMart's services and to communicate with consumers, including the identity of third parties promoting its services; and
- consumer complaints, lawsuits, other investigations and compliance with federal law.

In addition, the FTC has sought information unique to the Web3 space, such as procedures used by Bachi.Tech to determine "whether any cryptocurrency listed or considered for listing with BitMart is regulated by the [SEC] or another federal agency, and documents reflecting the company's assessment about whether any such cryptocurrency is a security under the federal securities laws." According to the FTC, this information could "reflect more broadly on the practices and lawfulness of cryptocurrency trading on BitMart and Bachi.Tech's corporate responses to data breaches and other illegal conduct."

In response to the CIDs, Spread and Bachi.Tech filed nearly identical petitions to quash. Both companies argued that the FTC could not compel them to produce materials located abroad, that the CID seeks irrelevant information, that the FTC's requests are overbroad and that production would impose an undue burden.

[4] See BitMart's December 7, 2021, statement re its response.

Rejecting each of Bachi.Tech's challenges in turn, the FTC countered that Bachi.Tech failed to provide factual information regarding any practical or legal impediments to responding to the CID, did not request clarification from the FTC on any CID specification, did not propose to narrow any CID request and never scheduled a meet-and-confer conference with the FTC.

Key Takeaways

To date, the Web3 industry has typically not focused on the broad powers of the FTC to protect against consumer harm through its Section 5 authority, including by investigating data security breaches, and its jurisdiction to enforce the handling of data under the GLB Act. Web3 companies should have strong and documented cybersecurity practices in place, and ensure they are in compliance with the GLB Act.

Contacts

Alexander C. Drylewski
Partner / New York
212.735.2129
alexander.drylewski@skadden.com

Alessio Evangelista
Partner / Washington, D.C.
202.371.7170
alessio.evangelista@skadden.com

Eytan J. Fisch
Partner / Washington, D.C.
202.371.7314
eytan.fisch@skadden.com

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Jessie K. Liu
Partner / Washington, D.C.
202.371.7340
jessie.liu@skadden.com

Bao Nguyen
Partner / Washington, D.C.
202.371.7160
bao.nguyen@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Khalil N. Maalouf
Counsel / Washington, D.C.
202.371.7711
khalil.maalouf@skadden.com

Andrew R. Beatty
Associate / New York
212.735.3278
andrew.beatty@skadden.com

Branka Cimesa
Associate / Chicago
312.407.0671
branka.cimesa@skadden.com

Ian C. Lerman
Associate / New York
212.735.2507
ian.lerman@skadden.com

Joe Sandman
Associate / Washington, D.C.
202.371.7355
joseph.sandman@skadden.com

Greg Seidner
Associate / Washington, D.C.
202.371.7014
greg.seidner@skadden.com

Gabriel U. Mohr
Law Clerk / New York
212.735.2486
gabriel.mohr@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000

skadden.com