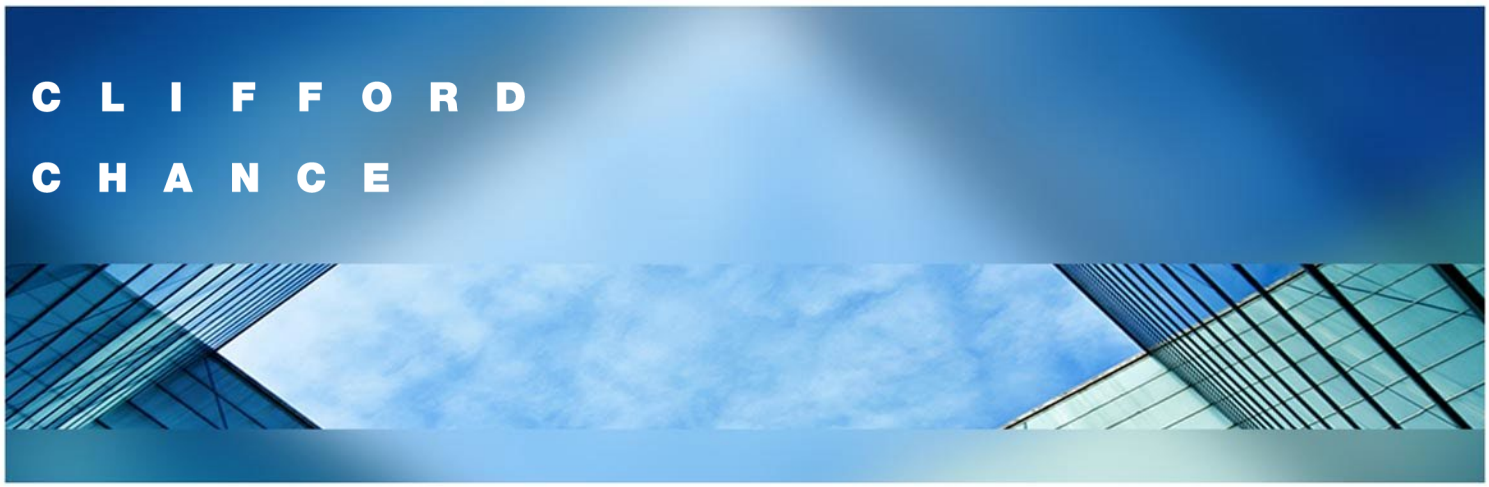

NYDFS FLEXES ENFORCEMENT MUSCLE IN CRYPTO MARKETS WITH $30 MILLION AML AND CYBERSECURITY FINE AND DRAFT CYBERSECURITY AMENDMENTS

On August 1, 2022, the New York Department of Financial Services ("NYDFS") levied a hefty $30 million penalty on Robinhood Crypto, LLC ("Robinhood Crypto"), citing what the agency identified as persistent and pervasive transaction monitoring and cybersecurity compliance failures. NYDFS also required Robinhood Crypto to retain an independent compliance consultant for 18 months. Although NYDFS has investigated other virtual currency businesses and other New York state authorities have brought significant enforcement actions, the Consent Order marks NYDFS's first cryptocurrency enforcement action containing a monetary penalty and extensive other remedies.[1]

In addition, NYDFS recently released draft amendments to its Cybersecurity Regulation.[2] NYDFS virtual currency business licensees should proactively review these amendments and ensure that their compliance programs are sufficient to ensure compliance.

OVERVIEW OF NYDFS REGULATIONS APPLICABLE TO ROBINHOOD CRYPTO

Robinhood Crypto is a wholly-owned subsidiary of Robinhood Markets, Inc. (RHM), and an affiliate of Robinhood Financial, LLC (RHF), a securities broker-dealer registered with the US Securities and Exchange Commission. Robinhood Crypto's trading platform allows RHF customers to trade certain cryptocurrencies in virtual currency markets using U.S. dollar funds carried in their securities brokerage accounts.

Robinhood Crypto is licensed by NYDFS both to engage in virtual currency business activity and to act as a money transmitter. As such, Robinhood Crypto is

[1] In 2019, NYDFS issued a cease-and-desist order to Bittrex, Inc., following the denial of its application for a virtual currency business license. In addition, a leading US cryptocurrency exchange recently disclosed that it is subject to an NYDFS investigation focused on its compliance program.

[2] 23 NYCRR Part 500 (available here).

governed by regulations—namely, New York's Virtual Currency Regulation,[3] Money Transmitter Regulation,[4] and Transaction Monitoring Regulation[5]—that require NYDFS-regulated entities to have effective, risk-based AML programs with policies and procedures aimed at preventing possible BSA/AML violations, facilitating suspicious activity reports ("SARs"), and preventing transactions prohibited by the Treasury's Office of Financial Asset Control ("OFAC"). The Transaction Monitoring Regulation also requires licensed money transmitters to document any material issues with compliance to the regulation and to certify compliance with the regulation to NYDFS annually.

In addition, under New York's Cybersecurity Regulation, NYDFS-regulated entities like Robinhood Crypto must implement a risk-based cybersecurity program that protects the entity's information systems and data. The program must include periodic risk assessments and written cybersecurity policies that address several industry-standard cybersecurity elements, including user access controls, multi-factor authentication, and incident response protocols. Entities are also required to implement business continuity and disaster recovery ("BCDR") plans and to designate a Chief Information Security Officer ("CISO"), who must certify compliance with this Cybersecurity Regulation annually.[6] In addition to similar cybersecurity requirements, the Virtual Currency Regulation also requires that virtual currency licensees test their BCDR plans annually and address a number of specific components, such as essential documents, data backup, and internal and external communications, in those plans. The Virtual Currency Regulation also requires covered entities to provide a telephone number for the receipt of customer complaints on their websites in a clear and conspicuous manner.

NYDFS conducts regular examinations of licensees, which involve a thorough analysis of internal controls and auditing, legal and regulatory compliance, management, and systems and technology to ensure compliance with all relevant regulations.

NYDFS INVESTIGATION FINDS PERSISTENT AND PERVASIVE COMPLIANCE FAILURES

According to the Consent Order, NYDFS conducted a supervisory examination of Robinhood Crypto's activities in 2019 starting from day one of Robinhood Crypto's entry into a Supervisory Agreement with NYDFS upon issuance of its virtual currency business license. The examination uncovered what the Consent Order describes as "serious deficiencies" in compliance protocols causing it to open an enforcement investigation. Upon concluding the investigation, NYDFS found that Robinhood Crypto failed to: a) maintain an effective BSA/AML program; b) comply with the Cybersecurity Regulation; c) comply with certain aspects of the Supervisory Agreement; and d) provide a telephone number on their website for consumer complaints.

NYDFS found that Robinhood Crypto's overall approach to compliance "substantially contributed to its deficiencies." In support of this allegation, NYDFS alleged that Robinhood Crypto's full reliance on its parent and affiliate for

3 23 NYCRR Part 200 (available here).
4 3 NYCRR Part 417 (available here).
5 23 NYCRR Part 504 (available here).
6 For more information on NYDFS's Cybersecurity Regulation, see our briefing here.

compliance, though not inherently improper, was problematic because the compliance program was not reasonably designed to account for the unique risks inherent in operating a virtual currency business. NYDFS also alleged that the organizational structure, under which the Chief Compliance Officer ("CCO") did not report to any legal or executive personnel or the independent audit and risk committees or Board of Directors at the parent or affiliate, led to an inability for Robinhood Crypto to obtain necessary resources and adopt new measures.

BSA/AML & Transaction Monitoring Deficiencies

In addition, NYDFS found Robinhood Crypto had insufficient staff covering BSA/AML compliance given the rapid growth the entity experienced during 2019 and 2020. The order states that its CCO relied on the affiliate entity's financial crimes team for staffing, which NYDFS alleges was unable to provide necessary coverage. NYDFS also found the CCO lacked sufficient experience to oversee a virtual currency-oriented compliance program.

The Consent Order indicates that these alleged staffing inadequacies were compounded by Robinhood Crypto's reliance on a manual transaction monitoring program, noting that the NYDFS believes it should have implemented an automated program much sooner than April 2021, given the high volume and value of transactions it was processing. According to the Consent Order, this lack of staff and automated resources caused Robinhood Crypto's parent entity to have a significant backlog of transactions needing review. Further, NYDFS alleges Robinhood Crypto had too high of a threshold for generating exception reports for cryptocurrency transactions and found the entity's process for escalating continued suspicious activity and repeat SAR filings inadequate. Because of these alleged deficiencies, NYDFS deemed Robinhood Crypto's 2019 certification with the Transaction Monitoring Regulation to be improper.

Cybersecurity Deficiencies

NYDFS also alleges that Robinhood Crypto had significant issues with its cybersecurity program. As with its AML program, Robinhood Crypto fully relied on its parent company's cybersecurity program, which NYDFS alleges did not fully address the risks, reporting lines, and operations of a virtual currency business and which was not compliant with the Cybersecurity Regulation. Among other alleged deficiencies, at the time of the supervisory exam, the cybersecurity program did not include processes for the board of directors to approve the written cybersecurity policy annually, had insufficient cybersecurity personnel to manage core cybersecurity functions, and failed to input fully satisfactory risk assessment policies and procedures. Additionally, the Consent Order states that Robinhood Crypto failed to create a BCDR Plan, and its incident response plan did not include any process for notifying regulators of a cybersecurity incident. Again, in light of these findings, NYDFS found Robinhood Crypto's 2019 certification of compliance with the Cybersecurity Regulation to be improper.

Supervisory Agreement & Website Deficiencies

NYDFS also found that Robinhood Crypto violated its Supervisory Agreement with the regulator by failing to promptly notify NYDFS about any real or potential proceedings brought against it by government regulators or agencies and by failing to inform NYDFS of subpoenas from government entities indicating it was

the target of an investigation. Finally, the Consent Order states that Robinhood Crypto failed to publicize a telephone number clearly and consciously for customer complaints on its website.

TERMS OF THE CONSENT ORDER

Under the Consent Order, Robinhood Crypto must pay a monetary penalty of $30 million to NYDFS. It must also retain an independent consultant for eighteen months, who must report to NYDFS, review the entity's current compliance programs, and assist with remedial efforts.

There is no indication as to whether NYDFS coordinated with other regulators, state or federal, but the Consent Order acknowledges that it does not bind others from taking separate action.

TAKEAWAYS & SIGNIFICANT NEW REGULATIONS ON THE HORIZON

Robinhood Crypto's Consent Order provides valuable insights into how a leading state regulator is evaluating BSA/AML and cybersecurity compliance programs and illuminates some of the compliance issues that can arise when companies experience rapid growth without compliance functions keeping pace. As NYDFS's first cryptocurrency enforcement action involving monetary penalties and ongoing independent compliance oversight, the Consent Order exemplifies the growing and continued focus among regulators worldwide on the cryptocurrency industry. It also reflects NYDFS's concern over "a level of cooperation with [NYDFS] that, at least initially, was less than what is expected of a licensee that enjoys the privilege of conducting business in the State of New York."

Compliance requirements for NYDFS-regulated entities continue to increase. On July 29, 2022, NYDFS released draft amendments to its Cybersecurity Regulation that would impose the following requirements on regulated entities, among others:

- notify the regulator within 72 hours of unauthorized access to privileged accounts or the deployment of ransomware to a material part of information systems (in addition to the current 72-hour window for reporting material cyber incidents);
- notify the regulator within 24 hours of making a ransom payment;
- submit a written description detailing why a ransom payment was necessary and a detailed description of alternatives considered and diligence performed within 30 days of the payment;
- for large entities, conduct annual independent audits of cybersecurity programs and weekly "systemic" vulnerability assessments;
- require board members to have a sufficient knowledge and expertise of cybersecurity risks, or be advised by persons with sufficient knowledge and expertise; and
- implement new requirements regarding the access, number, and use of privileged accounts.

If implemented, the amendments would also clarify the existing penalty framework to explain that one single act prohibited by the regulation constitutes a violation.

Importantly, NYDFS also seeks an aggressive timeline for the implementation of these amendments, providing for a brief comment window and proposing an effective date of 180 days after enactment for most amendments and only 30 days post-enactment for the new notification requirements.

As these developments illustrate, NYDFS licensed firms should be proactive in assessing their existing BSA/AML and cybersecurity compliance programs. This is particularly true for entities that share compliance resources and procedures with other affiliates. Finally, entities seeking licenses in New York should anticipate and plan for regulatory examinations within their first year of being licensed and should foster cooperative relationships with applicable regulatory authorities.

CONTACTS

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Steve Gatti
Partner

T +1 202 912 5095
E steve.gatti
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Devika Kornbacher
Partner

T +1 212 878 3424
E devika.kornbacher
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Jamal El-Hindi
Counsel

T +1 202 912 5167
E jamal.elhindi
@cliffordchance.com

Shannon O'Brien
Associate

T +1 212 880 5709
E shannon.obrien
@cliffordchance.com

Jesse Overall
Associate

T +1 212 878 8289
E jesse.overall
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

622171
August 2022