New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
ALM.
AUGUST 17, 2022

Familiar Themes in DFS's First Enforcement Action Against Virtual Currency Company

By Karen R. King and Alexander M. Levine

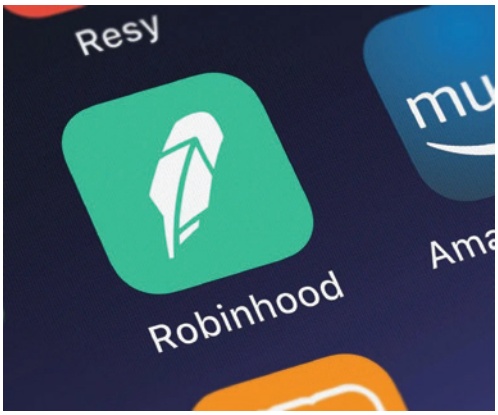
On Aug. 2, 2022, the New York State Department of Financial Services (DFS) announced a consent order with Robinhood Crypto (RHC), the virtual currency trading platform of mobile trading app provider Robinhood Markets, finding that RHC failed to maintain proper anti-money laundering (AML) and cybersecurity compliance programs. RHC agreed to a $30 million fine and an 18-month review by an independent compliance consultant who will report to DFS. Through this enforcement action, DFS has made clear its expectation that virtual currency companies, like traditional financial institutions, must invest in compliance programs to ensure they are commensurate with the risks and volume of their business, particularly for financial crimes compliance and cybersecurity.

KAREN R. KING *is a partner and* ALEXANDER M. LEVINE *is an associate at Morvillo Abramowitz Grand Iason & Anello.*

The RHC order is the first major cryptocurrency-related enforcement action by DFS. It is consistent with increased attention by DFS on the industry in the last year. Among other things, DFS issued more virtual currency-related licenses in the first half of 2022 than it did in all of 2021, it announced plans to triple its virtual currency team, and it was the first financial regulator in the country to issue guidance on stablecoins.

The principal terms of the RHC consent order were negotiated in the summer of 2021 and first disclosed in Robinhood's S-1 filing dated July 1, 2021, in which it estimated at least a $15 million fine. That estimate was increased a few weeks later to $30 million in Robinhood's initial public offering.

Unlike other regulators, DFS typically provides factual details in its consent orders, giving the industry insight into the key issues leading to the enforcement action. Supervised entities have long been encouraged to study past consent orders for guidance and lessons learned. The RHC consent order follows



(Photo: Shutterstock.com)

in that tradition. Notably, the key findings and themes are similar to the content of historical DFS consent orders: (1) failure to maintain a culture of compliance, including insufficient staffing and resources, and lack of stature for the compliance function; (2) failure to build an effective AML program, particularly with respect to transaction monitoring; and (3) lack of cooperation and transparency with regulators. In addition, the RHC order is the latest in a string of actions focused on compliance with the Cybersecurity Regulation and improper certifications under Part 500.

Lack of Culture of Compliance

The central finding in the consent order is that RHC failed

to develop an appropriate culture of compliance and its compliance department lacked stature within the organization. DFS found that RHC played no meaningful role in compliance efforts at the entity level and was instead dependent on its parent and affiliated entities. For example, RHC's CCO had no direct support staff and was reliant on the parent entity's team, which itself was inadequately staffed, particularly as RHC's business grew. DFS also found that the "lack of prominence for RHC compliance within" its parent's organizational structure "exacerbated" its compliance problems. It noted that the CCO reported to the director of product operations, rather than to a legal or compliance executive at the parent organization, and did not participate in any formal reporting to the board of directors or audit or risk committees.

These themes echo findings that appear in several past consent orders against traditional financial institutions. Earlier this year, DFS's consent order against the National Bank of Pakistan found that the New York branch failed to staff compliance units adequately and promote a culture of compliance, and that lack of supervision allowed "problems to persist year after year." Similarly, in its 2020 consent order against Goldman Sachs, DFS noted that one subsidiary "substantially relied" on its parent's due diligence and review of the Malaysian bond transactions at the heart of the 1MDB, exposing the entity to "undue financial and reputational risk." In a 2016 consent order against Mega International Commercial Bank of Taiwan, DFS criticized the compliance structure at the New York branch because compliance and operational functions were comingled and there was inadequate reporting of the compliance environment to the home office. In the same year, DFS found that Agricultural Bank of China did not give the New York branch CCO sufficient independence and impeded her from carrying out important compliance responsibilities. In 2017, DFS found that the compliance department of NongHyup Bank's New York branch lacked sufficient resources, was understaffed, and at one point led by a chief compliance officer who did not have an adequate understanding of BSA/AML concepts.

> The Robinhood Crypto order is the first major cryptocurrency-related enforcement action by DFS. It is consistent with increased attention by DFS on the industry in the last year.

Failure To Build an Effective AML Program

Another major issue identified in the RHC consent order was failure to establish an effective AML program in violation of the Virtual Currency Regulation. Among other things, RHC lacked risk-based policies and procedures and had no automated transaction monitoring system until April 2021. In October 2020, RHC had a backlog of more than 4,300 suspicious transaction alerts. Moreover, RHC had been told by an outside consultant that its manual transaction review process had "minimal value" and should be expeditiously upgraded to an automated system, but RHC did not remediate the issue promptly. Finally, DFS found that RHC "did not have sufficient BSA/AML staff with the appropriate level of skills to support its BSA/AML compliance program" and that RHC's CCO "lacked commensurate experience to oversee a compliance program such as RHC's, particularly as it grew." Based in large part on these failures, DFS concluded that RHC's Part 504 Certification attesting to compliance with the Transaction Monitoring Regulation for the calendar year 2019 was improper.

Most DFS enforcement actions against traditional financial institutions include findings about deficiencies in AML compliance programs, particularly with respect to transaction monitoring systems. Most similar to RHC is a 2020 consent order against the Industrial Bank of Korea in which DFS identified serious delays in the New York branch's implementation of an automated transaction

monitoring system. The continued reliance on manual review of suspicious activity at the branch led to substantial backlogs and a failure to detect patterns of inappropriate transactions. Similarly, in its 2017 consent order against NongHyup Bank, DFS found that the New York branch failed to establish an effective transaction monitoring protocol and did not review all suspicious activity alerts promptly.

Lack of Cooperation and Transparency With Regulators

DFS also faulted RHC for not cooperating fully with its investigation, providing information that was "either delayed, insufficient, or both" and, in several instances, failing to disclose investigations by federal and state regulators of an RHC-affiliated entity. According to the consent order, RHC was initially resistant to DFS's examination, claiming incorrectly that DFS did not have the authority to examine the policies or practices of RHC's parent or affiliated entities.

DFS's demand for cooperation from regulated entities is a common refrain in its enforcement actions. DFS has gone out of its way to praise some financial institutions for their level of cooperation, including the National Bank of Pakistan, Société Générale, NongHyup Bank, Industrial Bank of Korea, and Mashreq Bank. In contrast, it specifically noted that RHC's cooperation "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." Similar language appeared in DFS's consent order against Bank Hapoalim, which was criticized for not immediately cooperating with the investigation and narrowly construing a subpoena from DFS.

Deficiencies in RHC's Cybersecurity Program

As with its AML program, RHC relied on its parent entity's information systems and did not have any employees dedicated to cybersecurity, despite its "tremendous growth." Although DFS took no issue with RHC relying on its parent entity's policies and procedures, it found that those policies did not adequately address RHC's operations and risk, and were also not themselves in full compliance with DFS's Cybersecurity Regulation. DFS was also critical of RHC's failure to devote more resources to its cybersecurity program or develop its risk assessment policies earlier. For example, a year after receiving its license, RHC still did not have a business continuity and disaster recovery plan. Moreover, once implemented, the plan was not sufficiently detailed. Based on these failures, DFS concluded that RHC's Part 500 Certification attesting to compliance with the Cybersecurity Regulation for the calendar year 2019 was improper.

DFS's finding of a violation of the Cybersecurity Regulation, and improper certification of compliance, is a continuation of DFS's recent actions on this issue. In 2020, DFS brought its first Cybersecurity Regulation enforcement action against First American Insurance Company, which was charged with false certification under Part 500, among other violations. In 2021, DFS entered consent orders with three more companies based on improper certification.

* * *

The RHC action underscores DFS's expectation that virtual currency companies will invest in their compliance programs as they grow and maintain effective AML and cybersecurity programs that keep up with the risk profile of the business. Regulated businesses in the nascent industry are forewarned to learn from the experiences of other financial institutions, and to ensure that risk-based compliance programs and transparent regulatory engagement are priorities that run in tandem with business growth.