

August 9, 2022

NY DFS Announces First Crypto Enforcement Action Against Robinhood Crypto for AML and Cybersecurity Compliance Deficiencies

On August 2, 2022, the New York Department of Financial Services (“DFS”) announced a \$30 million consent order (the “Order”) against Robinhood Crypto, LLC (“Robinhood Crypto”), a wholly owned subsidiary of Robinhood Markets Incorporated (“RHM”), which offers cryptocurrency trading.¹ This marks DFS’s first enforcement action against a crypto company. When announcing the consent order, Superintendent Adrienne Harris said that DFS would continue to take action when virtual currency companies licensed by DFS violate DFS’s anti-money laundering and cybersecurity regulations.²

DFS found, among other things, that Robinhood Crypto (i) failed to maintain a compliant anti-money laundering (“AML”) program as required by New York’s Virtual Current Regulation and as part of Robinhood Crypto’s registration with DFS as a money transmitter; (ii) violated DFS’s Part 504 regulation by failing to maintain an appropriate transaction monitoring system and submitting an “improper” certification of compliance; and (iii) violated DFS’s Part 500 regulation by failing to maintain a compliant cybersecurity program and submitting an “improper” certification of compliance.³

In addition to the monetary penalty, Robinhood Crypto is required to maintain an independent consultant for an 18-month term that will report to DFS and conduct a comprehensive review of Robinhood Crypto’s compliance programs.⁴ DFS launched its investigation into Robinhood Crypto following a finding of “serious deficiencies” during a safety and soundness examination that began in 2020.⁵

Key takeaways from the Order are:

- **Crypto Companies Should Ensure That Their Compliance Programs Are Proportionate to Their Size and Scope.** DFS found that Robinhood Crypto lacked adequate staff or resources throughout 2019 and 2020, during which it used a manual transactions monitoring program and its transaction volume across the enterprise increased by more than 500 percent.⁶ DFS stated that the use of the manual transaction monitoring system was not a per se violation, but that Robinhood Crypto should have transitioned to an automated system because it averaged 106,000 daily transactions for a total of \$5.3 million per day.⁷ DFS pointed specifically to a “substantial backlog” in process alerts, including those used for evaluating potentially suspicious transactions to determine whether a suspicious activity report (“SAR”) should be filed.⁸ Additionally, DFS found that Robinhood Crypto “employed an extremely high and arbitrary threshold amount”—specifically, a cumulative transaction volume of \$250,000 over a six-month period—to generate exception reports; as a result of that threshold amount, Robinhood Crypto only filed two SARs during the time period for the 2019 examination.⁹ As such, DFS found that Robinhood Crypto did not devote sufficient funding or resources to grow the compliance program as the user base increased.

- **DFS Also Focuses on Compliance Leadership and Culture of Compliance.** DFS found that Robinhood Crypto’s leadership—specifically, its Chief Compliance Officer (“CCO”)—lacked “commensurate experience to oversee a compliance program such as [Robinhood Crypto’s], particularly as it grew” and was “insufficiently involved in the oversight of the launch and implementation of [Robinhood Crypto’s] automated software program. . . that was designed to enhance [Robinhood Crypto’s] compliance program.”¹⁰ DFS found that the overall culture of compliance and oversight of compliance was lacking, which DFS stated was evidenced through its reliance on the compliance programs of RHM and Robinhood Financial, LLC (“RHF”), a broker-dealer subsidiary of RHM.¹¹ As described in more detail below, DFS found that the organizational structure of RHM resulted in Robinhood Crypto playing “no meaningful role in compliance efforts at the entity level, resulting in a lack of an ability to influence staffing and resources, or to timely and adequately adopt measures that would assure compliance with [DFS’] Regulations.”¹²
- **Companies Should Be Cautious When Relying on Parent or Group-Wide Compliance Systems.** DFS took issue with the fact that Robinhood Crypto substantially relied on the compliance programs of its parent and affiliate, while noting that such reliance is not inherently problematic.¹³ According to the consent order, Robinhood Crypto relied on RHM and RHF for its AML compliance, its fraud detection, and its cybersecurity program despite the fact that the compliance programs at RHM and RHF were also “not compliant with New York State regulations” and did not “address all the particular risks applicable to licensed virtual currency business.”¹⁴ Further, DFS noted that Robinhood Crypto’s CCO reported to Robinhood Crypto’s Director of Product Operations instead of RHM and RHF’s Board of Directors, independent auditors, or risk committees, or anyone who oversaw the compliance programs at RHM and RHF—which DFS suggested would be more appropriate in this context since Robinhood Crypto was relying on the compliance programs of RHM and RHF.¹⁵
- **This Was DFS’s First Citation of a Violation of Part 504.** To our knowledge, this was DFS’s first citation of a violation of its Part 504 AML/sanctions regulation in a public enforcement action.¹⁶ In addition to finding that Robinhood Crypto’s transaction monitoring system did not satisfy one of the substantive requirements of Part 504, DFS also found that the company’s certification of compliance with Part 504 for calendar year 2019 was “improper” because it was filed despite the deficiencies in its transaction monitoring and, as noted by DFS, acknowledgement by RHF’s Head of Anti-Money Laundering that Robinhood Crypto was not in compliance with Part 504.¹⁷ This perhaps indicates DFS’s greater willingness to cite Part 504 violations in the future. All DFS-regulated companies subject to Part 504 should consider reviewing and, where needed, bolstering their internal procedures for complying with Part 504, including its certification requirement.

In the context of the fragmentation and uncertainty at the federal level with respect to crypto regulation, the DFS has emphasized that, for years, it has provided a rigorous framework of licensing and regulation over crypto companies of various kinds. With this first consent order, it appears that DFS is signaling that enforcement will be an important, and perhaps growing, feature of this framework. Crypto companies should consider taking this opportunity to evaluate and, where needed, enhance their financial crimes and cybersecurity compliance programs.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content.

Jonathan H. Ashtor
+1-212-373-3823
jashtor@paulweiss.com

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Jessica S. Carey
+1-212-373-3566
jcarey@paulweiss.com

David Fein
+44-20-7367-1608
dfein@paulweiss.com

Michael E. Gertzman
+1-212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Brad S. Karp
+1-212-373-3316
bkarp@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Jacobus J. Schutte
+1-212-373-3152
jschutte@paulweiss.com

Associate Carly Lagrotteria contributed to this Client Alert.

¹ N.Y. Dep’t of Fin. Services, *In the Matter of Robinhood Crypto, LLC* (Aug. 2, 2022), available [here](#) (hereinafter, the “DFS Order”); N.Y. Dep’t of Fin. Services, *DFS Superintendent Harris Announces \$300 Million Penalty on Robinhood Crypto for Significant Anti-Money Laundering, Cybersecurity & Consumer Protection Violations* (Aug. 2, 2022), available [here](#) (hereinafter, the “DFS Press Release”).

² N.Y. Dep’t of Fin. Services, *DFS Superintendent Harris Announces \$300 Million Penalty on Robinhood Crypto for Significant Anti-Money Laundering, Cybersecurity & Consumer Protection Violations* (Aug. 2, 2022), available [here](#).

³ DFS Order, *supra* note 1.

⁴ *Id.*

⁵ *Id.*

⁶ *Id.* at ¶ 38.

⁷ *Id.* at ¶ 41.

⁸ DFS Order, *supra* note 1, at ¶ 37.

⁹ *Id.* at ¶ 45.

¹⁰ *Id.* at ¶ 36.

¹¹ DFS Press Release, *supra* note 1.

¹² DFS Order, *supra* note 1, at ¶ 31.

¹³ *Id.* at ¶ 6

¹⁴ *Id.*

¹⁵ *Id.* at ¶ 31.

¹⁶ In DFS’s Industrial Bank of Korea consent order, the DFS noted that IBK’s Part 504 certification was inappropriate, but Part 504 was not among the legal violations cited by the order. See Paul, Weiss, *Industrial Bank of Korea Reaches \$86 Million AML Resolution with DOJ, NY Attorney General, and NY DFS* (Apr. 24, 2020), available [here](#). By contrast, DFS has cited violation of the Part 500 cybersecurity rule, including inappropriate certifications of compliance with that rule, in several prior enforcement actions. See Paul, Weiss, *New York DFS Files First Enforcement Action Alleging Violations of Cybersecurity Regulation* (July 30, 2020), available [here](#).

¹⁷ DFS Order, *supra* note 1, at ¶ 48.