NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
ONE STATE STREET
NEW YORK, NEW YORK 10004

----------x

In the Matter of :

ROBINHOOD CRYPTO, LLC :

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and Robinhood Crypto, LLC ("RHC") agree to resolve the matters described herein without further proceedings.

WHEREAS, RHC is a trading platform that allows customers to trade cryptocurrencies in virtual currency markets using U.S. dollars;

WHEREAS, RHC is licensed by the Department to engage in virtual currency business activity in New York State; RHC is also licensed by the Department as a money transmitter;

WHEREAS**,** federal and New York laws and regulations require businesses such as RHC to, among other things, maintain effective controls for the purpose of guarding against money laundering and certain other illicit activities;

WHEREAS, New York laws and regulations further require businesses to implement and maintain robust compliance programs in connection with their cybersecurity and virtual currency business activity programs;

WHEREAS, in 2020 the Department conducted a safety and soundness examination of RHC covering the period of January 24, 2019, through September 30, 2019 (the "Examination") and found serious deficiencies in RHC's compliance function across multiple areas;

WHEREAS, following the 2019 Examination, the Department began an enforcement investigation into the various compliance failures identified by the Examination, including whether RHC's compliance programs adequately comply with applicable federal and New York State laws and regulations related to anti-money laundering, cybersecurity, and virtual currency (the "Enforcement Investigation");

WHEREAS, the Enforcement Investigation found compliance deficiencies, a lack of adherence to regulatory requirements, and a failure on the part of RHC's management to adequately develop and maintain an appropriate culture of compliance at RHC;

WHEREAS, the Enforcement Investigation specifically found violations of Part 200 of the Regulations of the Superintendent of Financial Services (the "Virtual Currency Regulation"), Part 417 of the Superintendent's Regulations (the "Money Transmitter Regulation"), Part 500 of the Regulations of the Superintendent of Financial Services (the "Cybersecurity Regulation"), and Part 504 of the Superintendent's Regulations (the "Transaction Monitoring Regulation"); and

WHEREAS, the Enforcement Investigation also found that RHC has breached certain notification obligations under the terms of the Supervisory Agreement it entered into with the Department in connection with obtaining its virtual currency license;

NOW THEREFORE, to resolve this matter without further proceedings, pursuant to the Superintendent's authority under Sections 39 and 44 of the New York Banking Law and Section 408 of the New York Financial Services Law, the Department finds as follows:

THE DEPARTMENT'S FINDINGS

Introduction

1. The Department is the primary financial services regulator in the State of New York, and it licenses and oversees various financial services businesses, including licensed virtual currency businesses and licensed money transmitters such as RHC.

2. The head of the Department, the Superintendent of Financial Services (the "Superintendent"), is responsible for ensuring the safety, soundness, and prudent conduct of the providers of financial services in New York State and to enforce the various laws and regulations that are applicable to financial services licensees, including the New York Banking Law, the New York Financial Services Law, and the various regulations that have been promulgated under those statutes.

3. The Superintendent has the authority to conduct investigations and to bring enforcement proceedings, levy monetary penalties, and order injunctive relief against parties who have violated relevant laws and regulations.

4. RHC is a wholly owned subsidiary of Robinhood Markets, Inc. ("RHM"). RHM is a financial services company with businesses that, among other activities, allow United States-

based individual retail customers to trade stocks and options on a commission-free basis through its broker-dealer subsidiary, Robinhood Financial, LLC ("RHF").

5. RHC's trading platform allows RHF customers to trade certain cryptocurrencies in virtual currency markets using U.S. dollar funds custodied in customers' brokerage accounts. RHC holds customers' cryptocurrency and routes customers' transactions to market-making trading venues.

6. Throughout the time period relevant to this Consent Order, RHC relied on an "enterprise wide" system of compliance, specifically relying upon RHM and RHF for its Bank Secrecy Act and Anti Money Laundering ("BSA/AML") compliance, its fraud detection, and its cybersecurity program.

7. RHC is licensed by the Department to engage in virtual currency business activity in New York State; RHC is also licensed by the Department as a money transmitter.

Legal Framework

BSA/AML Program and Transaction Monitoring Requirements

8. Various provisions of both federal and New York State law require financial institutions such as RHC to maintain an effective anti-money laundering program and to devise and implement systems reasonably designed to identify and report suspicious activity and block transactions prohibited by law.

9. The Virtual Currency Regulation, for example, requires that a DFS-regulated virtual currency entity establish an effective AML program and that their policies and procedures be based on a risk assessment to provide assurance that the compliance program is commensurate with the risk profile of the licensee. 23 NYCRR § 200.15 (b), (d).

10. DFS regulations similarly require licensed money transmitters to establish, implement, and maintain an effective AML compliance program that, among other things, includes: (i) internal policies, procedures, and controls reasonably designed to guard against money laundering; (ii) a designated individual or individuals to coordinate and monitor day-to-day compliance with the BSA, New York Banking Law, and relevant regulations; (iii) an employee training program; (iv) independent program testing; (v) customer identification verification; and (vi) accurate, complete and timely reports of suspicious activity or "SARs." 3 NYCRR § 417.2.

11. Moreover, in light of the importance of transaction monitoring to the BSA/AML compliance function, the Transaction Monitoring Regulation requires certain DFS-regulated entities, including money transmitters such as RHC, to maintain transaction monitoring and sanctions screening programs that are reasonably designed, based upon the risk assessment of the entity, to ensure the monitoring of the entity's transactions for potential BSA/AML violations and suspicious activity reporting and to interdict transactions that are prohibited by the U.S. Treasury Department's Office of Financial Asset Control ("OFAC"). 23 NYCRR § 504.3(a) & (b).

12. Where a licensed entity has identified areas that require material improvement in its compliance with the Transaction Monitoring Regulation, the entity must document those areas, as well as any remedial efforts, planned and underway, to address such areas. 23 NYCRR § 504.3(d).

13. To help assure compliance, the Transaction Monitoring Regulation requires that licensed money transmitters adopt, and submit to the Superintendent annually, a board resolution

or senior officer(s) compliance finding that confirms, to the best of their knowledge, that the transaction monitoring and filtering program complies with Section 504.3. 23 NYCRR § 504.4.

Cybersecurity Program Requirements

14. To support the Superintendent's critical obligation to protect private and personally sensitive data, particularly data relating to consumers, DFS requires, through its Cybersecurity Regulation, all DFS-regulated entities ("Covered Entities" or, in the singular, "Covered Entity"), including licensed virtual currency businesses and money remitters like RHC, to establish and maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of its Information Systems, as well as any Nonpublic Information ("NPI") contained therein. 23 NYCRR § 500.02(b) and 23 NYCRR § 200.16.

15. The Cybersecurity Regulation requires that all Covered Entities conduct a periodic risk assessment of their Information Systems sufficient to inform the design of the entities' cybersecurity program and update such risk assessment as necessary to address changes to the Covered Entities' Information Systems, NPI, or business operations. 23 NYCRR § 500.09(a).

16. Further, a Covered Entity's cybersecurity risk assessment must be carried out pursuant to written policies and procedures that include: (1) criteria for evaluating and categorizing identified cybersecurity risks or threats; (2) criteria for the assessment of the "confidentiality, integrity, security and availability of the Covered Entity's Information Systems and [NPI]"; and (3) requirements describing how identified risks will be addressed. 23 NYCRR § 500.09(b).

17. As part of its cybersecurity program, each Covered Entity must establish and maintain written cybersecurity policies, approved by a Senior Officer or board of directors,

setting forth the policies and procedures that protect the entity's Information Systems. Pursuant to these regulations, a Covered Entity's cybersecurity policy must address the following areas:

- information security;
- data governance and classification;
- asset inventory and device management;
- access controls and identity management;
- business continuity and disaster recovery planning and resources;
- capacity and performance planning;
- systems operations and availability concerns;
- systems and network security;
- systems and network monitoring;
- systems and application development and quality assurance;
- physical security and environmental controls;
- customer data privacy;
- vendor and Third Party Service Provider management;
- risk assessment;
- monitoring and implementing changes to core protocols not directly controlled by the entity; and
- incident response.

23 NYCRR § 500.03 and 23 NYCRR § 200.16(b).

18. Covered Entities must also establish and maintain a written business continuity and disaster recovery ("BCDR") plan "reasonably designed to ensure the availability and functionality of the licensee's services in the event of an emergency or other disruption to licensee's normal business activities." 23 NYCRR § 200.17. The BCDR plan must meet several requirements, including: (i) the condition that the plan be independently tested at least annually (§ 200.17[e]); (ii) that it address essential documents, data, facilities, infrastructure, personnel, and competencies (§ 200.17[a][1]), internal and external communications (§ 200.17[a][3]), data back-up (§ 200.17[a][5]), and third-party dependencies (§ 200.17[a][6]); and (iii) that it establish requirements for training and testing (§ 200.17[c] & [d]).

19. Moreover, Covered Entities must formally designate a qualified individual as Chief Information Security Officer ("CISO"). 23 NYCRR § 500.04 and 23 NYCRR § 200.16(c).

The CISO is responsible for overseeing, implementing, and enforcing the company's cybersecurity program. If the designated individual is employed by an affiliate of the company, the Department's licensee must retain responsibility for compliance with the Cybersecurity Regulation.

20. The Department's regulations require, among other things, that the CISO report in writing, at least annually, to a board of directors or an equivalent governing body on the Covered Entity's cybersecurity program, any and all material risks, and steps for remediation to the extent inadequacies in the cybersecurity program are identified. 23 NYCRR § 500.04(b) and 23 NYCRR § 200.16(d).

21. Moreover, absent continuous monitoring or other systems designed to detect vulnerabilities on an ongoing basis, virtual currency licensees must conduct: (a) annual penetration testing of the entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and (b) bi-annual vulnerability assessments, also based on the entity's Risk Assessment. Under 23 NYCRR § 200.16(e)(1), vulnerability assessments are required at least quarterly.

22. Further, the Cybersecurity Regulation requires written procedures, guidelines, and standards designed to ensure the use of secure development practices for in-house developed applications and procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee within the context of its technology environment. 23 NYCRR § 500.08(a).

23. Similar to the certification obligations found in the Transaction Monitoring Regulation, to ensure compliance with the above-described obligations, Section 500.17(b) of the Cybersecurity Regulation requires that Covered Entities annually submit to the Superintendent a

written statement certifying that the licensee is in compliance with the requirements of the Cybersecurity Regulation. To the extent that an entity has identified areas that require material improvement, it is required to document all such areas, as well as any planned and underway remedial efforts designed to address them. This certification must be submitted annually and covers the licensee's compliance for the prior calendar year.

Obligation to Receive Consumer Complaints

24. The Virtual Currency Regulation imposes certain consumer protection requirements on each Covered Entity. One such requirement is that each licensee must provide, in a clear and conspicuous manner, on its website(s), a telephone number for the receipt of customer complaints. 23 NYCRR § 200.20(b)(1).

The Supervisory Agreement

25. In connection with the issuance of RHC's virtual currency business license, RHC and the Department entered into a Supervisory Agreement dated January 24, 2019 (the "Supervisory Agreement"). The Supervisory Agreement sets forth certain obligations upon RHC that exist in addition to those obligations set forth in the relevant laws and regulations, including with respect to specific capital requirements, protection of consumer assets, certain prohibitions on conduct, notice requirements, and a confirmation that RHC is subject to the Department's transaction monitoring and BSA/AML compliance requirements.

26. Among other requirements, under the terms of the Supervisory Agreement RHC is obligated to "promptly notify DFS of any actual or material potential action, proceeding, or similar process that has been or may be instituted against RHC or any affiliated entity by any regulatory body or governmental agency."

27. The Supervisory Agreement also obligates RHC to "promptly notify DFS of the receipt by RHC, or any affiliated entity, of any subpoena from any regulatory body or governmental agency in which RHC, or any affiliated entity, is the target of an investigation."

28. Pursuant to Section 44 of the Banking Law, violations of the Supervisory Agreement constitute a violation of the Banking Law, subjecting RHC to civil monetary penalties.

RHC's Compliance Deficiencies

29. Through the Examination and Enforcement Investigation, the Department has found that RHC failed to fully meet its legal obligations in two broad areas: (a) to maintain an effective BSA/AML program, including an adequate transaction monitoring system, commensurate with its growth; and (b) to fully comply with the Department's Cybersecurity Regulations. In addition, RHC failed to comply in certain respects with the terms of the Supervisory Agreement and to maintain on its website a telephone number for the receipt of customer complaints.

30. Although these deficiencies will be discussed in turn more fully below, it is worth beginning with the Department's observation that RHC's overall approach to its compliance obligations substantially contributed to such deficiencies. Starting on May 23, 2019, when RHC commenced operations of its regulated business activity in New York and at least throughout 2020 (the time period relevant to this Consent Order), RHC was not fully compliant with New York State regulations, and failed to address some of the particular risks associated with operating a cryptocurrency trading platform. RHC was reliant on its parent and affiliates for substantial aspects of its compliance program. Although such reliance is not inherently violative of DFS requirements, in this case, such reliance proved to be a weakness because the programs

of the parent (RHM) and affiliate (RHF) were not compliant with New York State regulations, and they failed to address all the particular risks applicable to licensed virtual currency businesses.

31. These problems were exacerbated by a lack of prominence for RHC compliance within RHM's organizational structure. Despite RHC's reliance on its parent and affiliate for its compliance program, RHC's Chief Compliance Officer ("CCO") reported to RHC's Director of Product Operations, rather than reporting directly to a legal or compliance executive at the parent or affiliate. The CCO also did not participate in any formal reporting to the Board of Directors or independent audit or risk committees at the parent or affiliate. Thus, RHC played 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 full compliance with the Department's Regulations.

32. RHC's compliance approach manifested not only in substantive failures, but also contributed to a level of cooperation with the Department 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. For example, information provided by RHC was either delayed, insufficient, or both. In several instances, RHC failed to disclose investigations by federal and state regulators of an RHC affiliated entity, in violation of reporting obligations governed by RHC's Supervisory Agreement with the Department.

33. RHC also initially claimed during the Examination, erroneously, that the Department did not have authority to examine policies or practices of RHC's parent and affiliates. RHC further claimed that any weaknesses in its programs were overstated because

RHC relied on more robust programs of its parent and affiliate, when in reality such programs were not compliant with various aspects of the Department's laws and regulations.

Deficiencies in RHC's BSA/AML and Transaction Monitoring Programs

34. These weaknesses in RHC's approach to compliance led to issues across RHC's BSA/AML and Transaction Monitoring programs.

35. The Department's investigation found that RHC did not have sufficient BSA/AML staff with the appropriate level of skills to support its BSA/AML compliance program, particularly given the size and pace of RHC's growth. RHC's CCO had no direct support staff within RHC but instead relied exclusively on the RHF Financial Crimes team for management of RHC's BSA/AML program. RHF, in turn, was itself inadequately staffed to provide adequate compliance support for RHC.

36. During the relevant period, RHC's CCO, who lacked commensurate experience to oversee a compliance program such as RHC's, particularly as it grew, was insufficiently involved in the oversight of the launch and implementation of RHC's automated software program, which was designed to enhance RHC's compliance program by providing fraud prevention and anti-money laundering software to RHC. As detailed below, the AML software program was necessary to ensure that RHC's transaction monitoring was consistent with federal and New York laws and regulations.

37. Among other things, throughout 2020, RHM had a substantial backlog in processing alerts, *i.e.*, in evaluating potentially suspicious transactions in order to determine whether a SAR should be filed. As of October 26, 2020, there existed a backlog of 4,378 alerts.

38. The lack of adequate staff or resources for RHC's BSA/AML compliance program was compounded by RHC's reliance throughout 2019 and 2020 on a manual system for

its transaction monitoring program, during which time alert volume across the enterprise increased by more than 500%.

39. Transaction monitoring is a cornerstone of an effective BSA/AML program. It must be conducted thoughtfully, efficiently, and in a manner commensurate with institutions' business profiles.

40. Whereas, nearly all institutions the size of RHC conduct at least some degree of automated transaction monitoring, RHC did not have any automated AML transaction monitoring and case management system in place at the time of the 2019 Examination, and did not have a fully automated AML system in place for many months after.

41. Though a manual system is not inherently a violation of DFS's Transaction Monitoring Regulation, RHC did not timely transition its manual system to an automated transaction monitoring system, which was unacceptable for a program that, as of September 30, 2019, averaged 106,000 transactions daily, totaling $5.3 million. Given this level of business and increase in alert volume at the enterprise level, a manual system was not adequate to support a compliant AML program, particularly in light of the staffing inadequacies. It is not surprising, therefore, that AML staff simply could not keep up with the transaction alerts, resulting in the significant backlog.

42. In sum, RHC's manual transaction monitoring process was inadequate for its size, customer profiles, and transaction volumes.

43. RHC independently engaged an outside consultant (the "Consultant") — in December 2019 to review RHC's compliance with BSA/AML requirements. Notably, the Consultant also identified RHC's lack of an automated AML management software program as a weakness. The Consultant cited the manual process as having "minimal value currently." The

Consultant recommended that RHC move expeditiously on RHC's plans to implement the automated AML Software Program.

44. Despite these noted concerns and the growing SARs backlog, the launch of the AML software program was not implemented until April 2021.

45. RHC's BSA/AML program was also materially deficient in other ways. For its two crypto-specific transaction monitoring rules, examiners found that RHC employed an extremely high and arbitrary threshold amount to generate exception reports. That threshold amount was $250,000, in cumulative transaction volume over a six-month period. Such a high threshold amount was unacceptable given the volume of transactions processed through RHC. As a result, during the time period for the 2019 Examination, only two SARs were filed in response to RHC's crypto-specific transaction monitoring alerts.

46. Additionally, escalation processes for continuing suspicious activity and repeat SAR filings were inadequate.

47. In sum, during the relevant period, RHC's BSA/AML and Transaction Monitoring programs were insufficient to be fully compliant with Department regulations.

48. Notwithstanding all of these deficiencies, including acknowledgment by RHF's Head of AML that RHC was not in compliance with the Transaction Monitoring Regulation, on May 31, 2020, RHC's CCO filed a Certification of Compliance with DFS, attesting to compliance with the Transaction Monitoring Regulation for calendar year 2019.

49. In light of the foregoing, RHC's filing of a Certification of Compliance attesting to compliance with the Transaction Monitoring Regulation for calendar year 2019 was improper.

Deficiencies in RHC's Cybersecurity Program

50. RHC also had deficiencies in its cybersecurity compliance program.

51. As with the AML program, RHC, which exclusively uses and relies on RHM's information systems, had no in-house staff exclusively devoted to its cybersecurity program, but instead adopted and relied wholly on the cybersecurity program of RHM. Although technology support services (staffing, information technology support, computer equipment, and information/professional services) were being provided to RHC by RHM under a 2018 Administrative Service Agreement, this Agreement was not promptly updated after the Department's virtual currency business license was issued to reflect the increased reliance on security personnel required to comply with New York State regulatory requirements.

52. Though RHC was within its right, under the Cybersecurity Regulation, to rely on RHM's (or another affiliate's) policies and procedures, in this case these policies and procedures did not fully address RHC's operations, risks, and reporting lines. Moreover, these policies and procedures were not in full compliance with the requirements of the Cybersecurity Regulation.

53. Enterprise-wide procedures and standards did not promote adequate accountability for RHC's cybersecurity program, including requirements for the CISO to report in writing *at least annually* to RHC's Board, as required by Section 200.16(d) of the Virtual Currency Regulation and Section 500.04(b) of the Cybersecurity Regulation. There were also insufficient procedures in place for RHC's Board (or an equivalent governing body) to approve the written cybersecurity policy at least annually.

54. As it experienced tremendous growth, RHC did not employ sufficient cybersecurity personnel to manage its cybersecurity risks and to perform the core cybersecurity functions specified in the Cybersecurity Regulation.

55. Notwithstanding that RHC has since devoted additional resources to its cybersecurity program, it did not do so during the Examination Period. As of the date of the 2019

Examination, RHC had not established sufficiently detailed policies or procedures to guide data governance and classification, IT asset management, business continuity and disaster recovery planning, systems operations and availability concerns, system and network monitoring, systems and application development, configuration and change management, physical security and environmental control, vulnerability and patch management, risk assessment, and incident response activities.

56. Furthermore, at the time of the 2019 exam, RHC had not conducted a risk assessment compliant with the Cybersecurity Regulation and the policies and procedures that RHC had in place to address cybersecurity and information security did not fully satisfy the requirements of Section 500.09(b) for risk assessment policies and procedures.

57. Moreover, written procedures, guidelines, and standards designed to promote secure development and testing of in-house and externally developed applications did not fully meet the requirements of Section 500.08 of the Cybersecurity Regulation.

58. A set of written cybersecurity policies and procedures unique to RHC was adopted by RHC's Board of Managers in November 2020, while the Department's investigation was underway.

59. By 2020, a year after the Department's licensure of RHC, RHC (and its parent and affiliate RHM and RHF) did not have a written Business Continuity and Disaster Recovery Plan ("BCDR Plan"), and the Incident Response Plan did not include a process for notifying regulators and law enforcement in the event of a cybersecurity incident.

60. Even after RHC created a BCDR Plan in November 2020 in response to the Department's concerns, the BCDR Plan failed to provide an adequate level of detail with regard to critical systems and services, internal and external communications, data back-up and third-

party dependencies, and requirements for training and testing, as mandated by the Virtual Currency Regulation.

61. Notwithstanding these gaps in RHC's compliance with the Cybersecurity Regulation, on May 31, 2020, RHC filed a Certification of Compliance, attesting to compliance with the Cybersecurity Regulation for the calendar year 2019.

62. In light of the foregoing, RHC's filing of a Certification of Compliance attesting to compliance with the Cybersecurity Regulation for the calendar year 2019 was improper.

Violations of Virtual Currency Regulation: Consumer Complaints

63. At the time of the 2019 exam, RHC did not provide a telephone number for the receipt of customer complaints on its website, in violation of 23 NYCRR 200.20(b)(1).

64. As of the date of this filing, there remains no conspicuous telephone number on RHC's website.

Violations of Law and Regulations

65. RHC failed to maintain an effective and compliant BSA/AML program, in violation of 3 NYCRR § 200.15 and 3 NYCRR § 417.2.

66. RHC failed to comply with its obligations to maintain an effective transaction monitoring program, in violation of 23 NYCRR § 504.3.

67. Because RHC's transaction monitoring program did not meet all the requirements of the Transaction Monitoring Regulation, the Certification of Compliance attesting to compliance for the calendar year 2019 was improper, in violation of 23 NYCRR § 504.4.

68. RHC failed to maintain a compliant cybersecurity program in violation of 3 NYCRR § 200.16 and 23 NYCRR § 500.

69. Because RHC's cybersecurity program did not meet all the requirements of the Cybersecurity Regulation, the Certification of Compliance attesting to compliance for the calendar year 2019 was improper, in violation of 23 NYCRR § 500.17(b).

70. RHC failed to comply with the Supervisory Agreement by failing to promptly notify the Department of (a) actual or material potential actions, proceedings, or similar process that were or may have been instituted against RHC or any affiliated entity by any regulatory body or governmental agency; and (b) of the receipt by RHC, or any affiliated entity, of any subpoena from any regulatory body or governmental agency in which RHC, or any affiliated entity, was the target of the investigation. Such failure constitutes a violation of Section 44(1)(a) of the New York Banking Law.

NOW THEREFORE**,** to resolve this matter without further proceedings, the Department and RHC stipulate and agree to the following terms and conditions:

SETTLEMENT PROVISIONS

Monetary Penalty

71. No later than ten (10) days after the Effective Date (as defined below) of this Consent Order, RHC shall pay a civil monetary penalty pursuant to Financial Services Law § 408 and Banking Law §§ 39 and 44 to the Department in the amount of [thirty million U.S. Dollars ($30,000,000.00)]. The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

72. RHC shall not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

73. RHC shall neither seek nor accept, directly or indirectly, reimbursement or indemnification with respect to payment of the penalty amount, including but not limited to, payment made pursuant to any insurance policy.

Independent Consultant

74. During the course of the Enforcement Investigation, RHC retained a third-party consultant to assist RHC in improving its compliance performance with regard to the issues discussed above. The Department has agreed to permit that third-party consultant to stay on as the Independent Consultant appointed pursuant to the terms of this Consent Order (the "Independent Consultant").

75. Within thirty (30) days of the Effective Date of this Consent Order (as defined below), RHC shall enter into a new engagement with the Independent Consultant in a form acceptable to the Department. That engagement shall be explicit that the Independent Consultant will report to DFS and will commence a comprehensive review of RHC's current compliance programs with respect to Part 200 of the Regulations of the Superintendent of Financial Services (the "Virtual Currency Regulation"), Part 417 of the Superintendent's Regulations (the "Money Transmitter Regulation"), Part 500 of the Regulations of the Superintendent of Financial Services (the "Cybersecurity Regulation"), and Part 504 of the Superintendent's Regulations (the "Transaction Monitoring Regulation"). The Independent Consultant will review, report on, and assist RHC regarding its efforts to remedy these deficiencies in RHC's compliance programs with regard to the following:

a) A review of and reporting on the thoroughness and comprehensiveness of RHC's current BSA/AML and transaction monitoring programs, including programs designed to address the failures set forth in this Consent Order;

b) A review of and reporting on the organizational structure, management oversight, and reporting lines that are relevant to BSA/AML and transaction monitoring

compliance, and an assessment of the staffing of such tasks including the duties, responsibilities, authority, and competence of officers or employees responsible for RHC's compliance with laws and regulations pertaining to BSA/AML and transaction monitoring;

c) A review of and reporting on the propriety, reasonableness, and adequacy of any proposed, planned, or recently-instituted changes to RHC's BSA/AML and transaction monitoring;

d) Assistance with the implementation of any corrective measures necessary to address identified weaknesses or deficiencies in RHC's BSA/AML and transaction monitoring compliance programs;

e) A review and reporting on RHC's current compliance with Part 200 of the Regulations of the Superintendent of Financial Services (the "Virtual Currency Regulation"), Part 417 of the Superintendent's Regulations (the "Money Transmitter Regulation"), Part 500 of the Regulations of the Superintendent of Financial Services (the "Cybersecurity Regulation"), and Part 504 of the Superintendent's Regulations (the "Transaction Monitoring Regulation"), including a review of and reporting on the organizational structure, management oversight, and reporting lines, and an assessment of the staffing of such tasks including the duties, responsibilities, authority, and competence of officers or employees that are relevant to compliance with these regulations;

f) A review of and reporting on the propriety, reasonableness, and adequacy of any proposed, planned, or recently-instituted changes to RHC's Virtual Currency Regulation, Cybersecurity Regulation, Money Transmitter Regulation and Transaction Monitoring Regulation compliance programs; and

g) Assistance with the implementation of any corrective measures necessary to address identified weaknesses or deficiencies in RHC's compliance with the Virtual Currency Regulation, the Cybersecurity Regulation, the Money Transmitter Regulation and the Transaction Monitoring Regulation.

76. The specific work to be performed by the Independent Consultant will be determined based on discussions with DFS and may be updated, in DFS's sole exercise of its regulatory discretion, after consultation with RHC and the Independent Consultant, as the engagement progresses and additional information is obtained.

77. After the Independent Consultant has been engaged for six (6) months, should the Department determine that the Independent Consultant is failing to achieve the tasks set forth herein, to act with sufficient independence from RHC, or to coordinate adequately with DFS —

or for any other reason in DFS's sole regulatory discretion — the Department may require RHC to replace the Independent Consultant with a consultant of the Department's choosing. In that case, RHC will enter into an engagement with the newly selected consultant within thirty (30) days of notification of the Department's selection, and the newly selected consultant will assume all of the responsibilities of the Independent Consultant set forth herein.

78. The term of the Independent Consultant's engagement shall be eighteen (18) months from the effective Date of this Consent Order (as defined below). RHC reconfirms its commitment to cooperate fully with the Independent Consultant (including any replacement(s) selected pursuant to the preceding paragraph). Such cooperation does not include providing the Independent Consultant with materials protected by attorney-client or work product privilege. RHC acknowledges that, although no extension of the consultancy is currently contemplated, the Department may, in its sole regulatory discretion, extend the scope of duration of the consultancy to address fully the Company's particular failures described herein.

Full and Complete Cooperation

79. RHC commits and agrees that it will fully cooperate with the Department regarding all terms of this Consent Order. RHC further agrees that it will fully cooperate with the Independent Consultant and will support the work of each by, among other things, providing each full and complete access to all relevant controlled personnel, consultants, and third-party service providers, files, reports, or records relevant to the products RHC offers to New York residents, whether located in New York, or any other location sought, consistent with applicable law.

Waiver of Rights

80. The parties understand and agree that no provision of this Consent Order is subject to review in any court, tribunal, or agency outside of the Department.

Parties Bound by the Consent Order

81. This Consent Order is binding on the Department and RHC, as well as any successors and assigns. This Consent Order does not bind any federal or other state agency or any law enforcement authority.

82. No further action will be taken by the Department against RHC for the conduct set forth in this Consent Order, including the deficiencies identified by the 2019 Examination, provided that RHC fully complies with the terms of the Consent Order.

83. Notwithstanding any other provision in this Consent Order, however, the Department may undertake additional action against RHC for transactions or conduct that was outside the scope of the 2019 Examination and/or which was not disclosed in the presentations or written materials submitted to the Department by RHC in connection with this matter.

Breach of Consent Order

84. In the event that the Department believes RHC to be in material breach of the Consent Order, the Department will provide written notice to RHC of the breach. Within ten (10) business days of receiving such notice, or on a later date if so determined in the Department's sole discretion, RHC must appear before the Department to demonstrate that no material breach has occurred or, to the extent pertinent, that the breach is not material or has been cured.

85. RHC understands and agrees that its failure to make the required showing within the designated time period set forth in Paragraph 73 shall be presumptive evidence of RHC's breach. Upon a finding that a breach of this Consent Order has occurred, the Department has all

the remedies available to it under the New York State Banking Law, Financial Services Law, or any other applicable laws, and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Notices

86. All notices or communications regarding this Consent Order shall be sent to:

For the Department:

Laura E. Meehan
Senior Assistant Deputy Superintendent for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

Matthew Quinones
Assistant Deputy Superintendent for
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

For RHC:

Andrew J. Ceresney
Debevoise & Plimpton LLP
919 Third Avenue
New York, New York 10022

Eric R. Dinallo
Debevoise & Plimpton LLP
919 Third Avenue
New York, New York 10022

Miscellaneous

87. This Consent Order and any dispute thereunder shall be governed by the laws of the State of New York without regard to any conflicts of laws principles.

88. This Consent Order may not be altered, modified, or changed unless in writing and signed by the parties hereto.

89. This Consent Order constitutes the entire agreement between the Department and RHC and supersedes any prior communication, understanding, or agreement, whether written or oral, concerning the subject matter of this Consent Order.

90. Each provision of this Consent Order shall remain effective and enforceable against RHC, its successors, and assigns, until stayed, modified, suspended, or terminated by the Department.

91. In the event that one or more provisions contained in this Consent Order shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect any other provision of this Consent Order.

92. No promise, assurance, representation, warranty or understanding other than those contained in this Consent Order has been made to induce any party to agree to the provisions of this Consent Order.

93. Nothing in this Consent Order shall be construed to prevent any consumer from pursuing any right or remedy at law.

94. Except with regard to the enforcement of this Consent Order, RHC's consent to the provisions of this Consent Order does not bar, estop, waive, or otherwise prevent RHC from raising any defenses to any action taken by any federal or state agency or department, or any private action against RHC.

95. This Consent Order may be executed in one or more counterparts, and shall become effective when such counterparts have been signed by each of the parties hereto and the

Consent Order is So Ordered by the Superintendent of Financial Services or her designee (the "Effective Date").

[*remainder of this page intentionally left blank*]

IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed on the dates set forth below.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: /s/ Laura Meehan
LAURA MEEHAN
Senior Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement

August 1, 2022

By: /s/ Kevin R. Puvalowski
KEVIN R. PUVALOWSKI Acting
Executive Deputy Superintendent
Consumer Protection and Financial Enforcement

August 1, 2022

ROBINHOOD CRYPTO, LLC

By: /s/ James Nguyen
JAMES NGUYEN
General Counsel and Chief Compliance Officer

July 14, 2022

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Adrienne A. Harris
ADRIENNE A. HARRIS
Superintendent of Financial Services

August 1, 2022