

**COMMONWEALTH OF MASSACHUSETTS  
OFFICE OF THE SECRETARY OF THE COMMONWEALTH  
SECURITIES DIVISION  
ONE ASHBURTON PLACE, ROOM 1701  
BOSTON, MASSACHUSETTS 02108**

_____	)	
IN THE MATTER OF:	)	
	)	
ROBINHOOD FINANCIAL LLC,	)	Docket Nos.
	)	E-2020-0047
RESPONDENT.	)	E-2022-0006
_____	)	

**CONSENT ORDER**

**I. PRELIMINARY STATEMENT**

This Consent Order (the “Order”) is entered into by the Massachusetts Securities Division and respondent Robinhood Financial LLC (“Robinhood” or “Respondent”) with respect to (1) the administrative proceeding (E-2020-0047) commenced through an amended administrative complaint filed by the Enforcement Section of the Massachusetts Securities Division (the “Enforcement Section” and the “Division,” respectively) against Robinhood on October 21, 2021 (the “Complaint”), alleging Robinhood violated the Massachusetts Uniform Securities Act, M.G.L. c. 110A (the “Act”) and the corresponding regulations promulgated thereunder at 950 Mass. Code Regs. 10.00 – 14.413 (the “Regulations”) by marketing itself to Massachusetts residents, in part, by deploying certain in-app features and other promotional campaigns and failed to maintain the infrastructure and procedures necessary to meet the demands of its customer base and (2) the investigation commenced by the Division concerning Robinhood’s cybersecurity controls at the time of a November 3, 2021 data breach which resulted in an unauthorized third-

party obtaining names, emails, or phone numbers for approximately 117,000 Massachusetts consumers (the “Investigation”).

On January 17, 2024, Respondent submitted an Offer of Settlement (the “Offer”) to the Division. Respondent neither admits nor denies the factual allegations set forth in Section VI(A), admits the factual allegations set forth in Section VI(B), neither admits nor denies the Violations of Law set forth in Section VII, and consents to the entry of this Order by the Division, consistent with the language of the terms of the Offer, settling the claims brought in the Complaint (E-2020-0047) and the Investigation (E-2022-0006) with prejudice. This Order is necessary and appropriate in the public interest for the protection of investors and is consistent with the purposes fairly intended by the policies and provisions of the Act.

## **II. JURISDICTION AND AUTHORITY**

1. The Division has jurisdiction over matters relating to securities pursuant to the Act.

2. The Offer was made and this Order entered in accordance with the Act and with Section 10.10 of the Regulations.

3. The acts and practices constituting violations occurred while Robinhood was registered as a broker-dealer in Massachusetts.

## **III. RELEVANT TIME PERIOD**

4. Except as otherwise expressly stated, the conduct described herein occurred during the approximate time period of December 1, 2017, through the present (the “Relevant Time Period”).

#### **IV. RESPONDENT**

5. Robinhood Financial LLC (“Robinhood”) is a Delaware limited liability company with a principal place of business located at 500 Colonial Center Parkway, Suite 100, Lake Mary, Florida.

6. Robinhood has a Financial Industry Regulatory Authority Central Registration Depository number of 165998.

7. Robinhood has been registered as a broker-dealer in Massachusetts since January 7, 2014.

#### **V. OTHER INVOLVED AND RELATED PARTIES**

8. Robinhood Markets, Inc. (“Robinhood Markets”) is a Delaware corporation with a principal place of business at 85 Willow Road, Menlo Park, California 94025.

9. Robinhood Markets is the sole owner of Robinhood.

10. As of October 8, 2021, Robinhood Crypto, LLC (“Robinhood Crypto”) is a wholly-owned subsidiary of Robinhood Markets.

11. Robinhood Agent is a natural person.

12. During the Relevant Time Period, Robinhood Agent was employed by Robinhood Markets and was registered as a broker-dealer agent of Robinhood in Massachusetts.

13. As of November 3, 2021, Robinhood granted Robinhood Agent access to internal information regarding customers of Robinhood (“Robinhood’s Internal Information”).

14. Robinhood Supervisor is a natural person.

15. Robinhood Supervisor supervised Robinhood Agent at the time of an unauthorized third-party gaining access to Robinhood’s internal systems on November 3, 2021 (the “Data Breach”).

16. During the Relevant Time Period, Robinhood Supervisor was employed by Robinhood Markets and was registered as a broker-dealer agent of Robinhood in Massachusetts.

17. Robinhood Director is a natural person.

18. During the Relevant Time Period, Robinhood Director was employed by Robinhood.

19. Robinhood Director was a senior employee in Robinhood Markets’ Security and Privacy team, responsible, in part, for training employees concerning securities awareness including training relative to reporting social engineering attacks.

## VI. STATEMENT OF FACTS

### A. **Robinhood Did Not Provide the Infrastructure and Supervision Necessary to Protect Customers in Massachusetts.**

20. Robinhood is a broker-dealer that offers commission-free trading for stocks, ETFs, and options.

21. Robinhood’s stated mission is to “democratize finance for all.”

22. Robinhood’s advertising attracted younger individuals, many of whom had limited or no investment experience.

23. For portions of the Relevant Time Period, the median Robinhood customer’s age was approximately 31 years old. About half of Robinhood’s customers

were first time investors, and the median customer account size at Robinhood was approximately \$240.

24. Robinhood approved approximately 71,744 Massachusetts residents for options trading during a portion of the Relevant Time Period, approximately two-thirds of whom self-identified as having limited or no prior investment experience.

25. Since its founding in 2013, Robinhood experienced exponential growth.

26. Robinhood customer accounts increased in number from approximately one million in 2016 to approximately six million in October 2018, an increase of 500% over that time period.

27. As of the end of 2019, Robinhood had approximately ten million customer accounts. By May 2020, only five months later, that number had grown by 30% to approximately thirteen million accounts.

28. As of the week prior to the filing of the Division's first complaint, Robinhood had approximately 486,598 Massachusetts customer accounts with an approximate total value of \$1,671,435,739.

**a. Robinhood developed an application that included digital engagement practices to engage with its customer base.**

29. Robinhood developed and made available for downloading an application for use on mobile devices which allowed its customers to access their accounts (the "Application").

30. Robinhood uses the Application as the primary means of engaging with its customer base.

31. Prior to the Complaint, Robinhood developed digital engagement features and prompts, but did not implement procedures reasonably designed to supervise these features and prompts in a manner necessary to protect customers in Massachusetts, including the supervision of:

- i. A “First List” that includes stocks “chosen based on their popularity on Robinhood’s platform.” This list was provided on the home screen of the Application and it was one of the first items that a new customer may see;
- ii. A section titled “Popular Lists” that all customers could search to browse potential investments. The Popular Lists section included lists compiled from customer trading activity, such as the “100 Most Popular” list;
- iii. Push notifications sent to certain customers regarding specific changes in the value of stocks held in their accounts;
- iv. A one-time push notification sent to certain customers after funding an account that stated: “Top Movers: Choosing stocks is hard. [flexing bicep emoji] Get started by checking which stock prices are changing the most.” Upon clicking on the push notification, the application redirected customers to a “Top Movers” list;
- v. A one-time push notification sent to some customers after funding an account that stated: “Popular Stocks: Can’t decide which stocks to buy? [thinking emoji] Check out the most popular stocks on Robinhood.” Upon clicking on the push notification, the application redirected customers to the 100 Most Popular list;

- vi. Digital confetti raining down from the top of the screen after a customer's first trade;
- vii. An offer of free stock rewards for new customers, highlighting the possibility to receive stocks such as "Microsoft, Visa, or Apple" despite a low probability of receiving shares of those companies. Robinhood required customers to mimic the motion of "scratching off" a lottery ticket in order to reveal the free stock and promised existing customers the ability to earn up to \$500 per year in additional free stock rewards by recommending Robinhood's Application to others; and
- viii. The ability for customers to improve their position on an early access waitlist by "tapping" a digital representation of a debit card displayed in the Application up to 1,000 times per day. Robinhood displayed a message to customers who "tapped" on the card 1,000 times in a day that they were "out of taps today! Come back tomorrow if you're feeling tappy."

32. Following the Division's Complaint, Robinhood ceased many of its digital engagement practices and prompts. For example:

- i. Robinhood ceased use of the digital confetti feature on its Application as of March 31, 2021;
- ii. Robinhood ceased use of the digital "scratch-off" ticket to reveal free stock rewards as of April 5, 2021;
- iii. Robinhood ceased use of the waitlist tapping feature for its cash management product; and

iv. Robinhood ceased use of certain push notifications, including the notifications discussed above with links to the Top Movers list and 100 Most Popular list as of January 2022.

**b. Some inexperienced investors executed trades frequently on Robinhood's platform.**

33. As described in the Complaint, over 200 Robinhood customers with no self-reported investment experience averaged at least 5 trades per day on Robinhood's trading platform.

34. At least 25 of these customers with no self-reported investment experience made at least 15 trades per day.

35. At least 10 of these customers averaged 25 trades per day during the time period in which they were actively trading.

36. Some of these customers averaged 58 to 92 trades per day.

37. The aforementioned 25 customers combined to make 125,790 trades during the Relevant Time Period outlined in the Complaint.

**c. Robinhood did not adequately review and approve options trading in customer accounts.**

38. Robinhood uses an automated process, approved by a registered principal, in order to approve customers for options trading.

39. Accounts approved for options trading are subject to review through a manual and limited spot-checking process.

40. Until September 2020, in order to gain approval for level 2 options trading—the lowest level of options trading that Robinhood offered—Robinhood required customers to have margin accounts and both: (1) more than four filled orders, investment



experience greater than none, or options trading experience greater than none, and (2) a medium or high-risk tolerance.

41. Robinhood failed to exercise appropriate due diligence in approving options trading in accounts. The failures include: (i) approving accounts with inconsistent information including for customers who were younger than 21 years old who nevertheless claimed to have more than three years' experience trading options; (ii) approving accounts for customers with a low risk tolerance; and (iii) approving options account applications for customers who had previously been rejected, often only minutes earlier, without additional diligence.

42. Robinhood failed to adequately supervise the approval process through which Massachusetts customer accounts were approved to engage in options trading.

**d. Robinhood's trading platform experienced several outages and disruptions.**

43. Robinhood experienced several outages or disruptions on its trading platform from January 1, 2020, through November 30, 2020. These disruptions impacted the ability of Robinhood customers to access their accounts and purchase and sell securities.

44. Certain of the most impactful Robinhood outages occurred in March 2020. On March 2, 2020, the Dow Jones Industrial Average had what was then its largest one-day gain in history, a gain of 1,290 points.

45. During this record-setting day, and on part of the following day, Robinhood experienced an outage that prevented customers from making trades in their accounts.

46. On March 9, 2020, amid a stock market plunge, Robinhood experienced another outage on its trading platform that prevented customers from making trades in their accounts for a portion of the day.

47. The technology infrastructure of Robinhood's trading platform was not sufficient to support the rapidly increasing trading volume.

48. Robinhood's outages and disruptions impacted the ability of Massachusetts customers to access and make trades on Robinhood's platform, resulting in certain Massachusetts customers suffering losses.

**B. Robinhood Failed to Maintain and Enforce Reasonable Cybersecurity Policies and Procedures.**

49. On November 3, 2021, an unauthorized and non-Robinhood affiliated user or users (the "Unauthorized Third Party") accessed certain customer information stored on internal Robinhood systems ("Robinhood Internal Systems").

50. The Unauthorized Third Party gained access to certain Robinhood Internal Systems through a social engineering attack.

51. Specifically, the Unauthorized Third Party used tactics known as vishing and caller ID spoofing by placing a series of telephone calls to Robinhood Agent's personal telephone (the "Unauthorized Access Calls") and purporting to be a Robinhood human resources employee. The Unauthorized Access Calls appeared to come from an internal Robinhood phone number. The Unauthorized Third Party provided information to Robinhood Agent demonstrating internal knowledge of Robinhood and its other employees, including the name of Robinhood Agent's Robinhood Supervisor and the non-public name of a Robinhood data system.

52. The Unauthorized Third Party placed the first Unauthorized Access Call to Robinhood Agent at approximately 6:07 p.m.

53. The first Unauthorized Access Call lasted for approximately 1 hour and 32 minutes.

54. The Unauthorized Third Party directed Robinhood Agent—in service of a supposed Robinhood-authorized investigation—to download, install, and run a third-party remote access software, AnyDesk, on Robinhood Agent’s Robinhood-issued laptop (the “Robinhood Device”).

55. At approximately 6:31 p.m., Robinhood Agent downloaded and installed AnyDesk on the Robinhood Device.

56. The Unauthorized Third Party placed an additional Unauthorized Access Call to Robinhood Agent at approximately 7:44 p.m.

57. During a significant portion of the Unauthorized Access Calls, the Unauthorized Third Party was remotely connected via AnyDesk to the Robinhood Device, which enabled access to certain Robinhood Internal Systems.

58. The Unauthorized Third Party’s remote connection using AnyDesk lasted approximately 4 hours, during which time the Unauthorized Third Party obtained access to certain of the Robinhood Internal Systems accessible by Robinhood agent.

59. At approximately 11:33 p.m., Robinhood Agent rebooted the Robinhood Device, thereby ending the AnyDesk connection.

60. The Unauthorized Third Party placed additional Unauthorized Access Calls to Robinhood Agent at 11:49 p.m. and 11:55 p.m.

61. During a portion of the Data Breach, Robinhood Agent left the Robinhood Device unattended while the Unauthorized Third Party was able to access certain Robinhood Internal Systems.

**a. The Unauthorized Third Party obtained information related to 117,000 Massachusetts consumers.**

62. After gaining access to certain of Robinhood's Internal Systems through the use of AnyDesk installed on the Robinhood Device, the Unauthorized Third Party obtained a bulk file containing names, email addresses, and/or telephone numbers for at least 117,763 individuals who had previously given Robinhood a Massachusetts address (the "Massachusetts Individuals"). The names, email addresses, or telephone numbers did not appear together and were not associated with each other such that, for instance, a name does not appear alongside a telephone number.

63. The Massachusetts Individuals may have been current or former Robinhood customers, as well as Massachusetts individuals who never became customers of Robinhood but nonetheless provided their name, email address, or telephone number information to Robinhood in the process of seeking approval to open an account.

64. The Unauthorized Third Party also obtained non-public personal identifying information for three of the Massachusetts Individuals. For these three additional individuals, the Unauthorized Third Party obtained e-mail addresses, names, telephone numbers, dates of birth, and city, state, and zip code on file at Robinhood.

65. During the Data Breach, the Unauthorized Third Party gained access to Robinhood Internal Systems displaying nonpublic personal information for about eight other Robinhood customers, including Robinhood account numbers and trading

information, which the Unauthorized Third Party may have seen. None of these Robinhood customers were Massachusetts residents.

66. The Robinhood Internal Systems accessed by the Unauthorized Third Party also contained information concerning additional individuals with a Massachusetts address but whose information was not downloaded.

67. The Robinhood Agent rebooted the Robinhood Device at 11:33 p.m., which terminated the Unauthorized Third Party's access to the Robinhood Internal Systems via AnyDesk.

**b. Robinhood's internal controls concerning the Data Breach.**

68. At the time of the Data Breach, while Robinhood Agent had completed certain trainings, including the onboarding security training "Partnering With Security," the 2021 Annual Privacy training, and the customer service Social Engineering training, Robinhood Agent had not yet completed the 2021 Annual Security Training, which included topics specifically designed to protect against social engineering tactics, including phishing and caller ID spoofing. That 2021 training was released on November 1, 2021, and completion was required by November 12, 2021, nine days after the Data Breach. The 2021 Annual Security Training included guidance concerning the precursors and indicators of social engineering.

69. Robinhood did not ensure that Robinhood Agent started an additional training entitled, "*Detective Robinhood and the Case of the Social Engineers v.1*," until November 16, 2021, and Robinhood Agent did not enroll in the course until November 9, 2021.

70. Following the Unauthorized Access Calls, Robinhood Agent made numerous attempts to report the Data Breach to Robinhood.

71. Robinhood Agent was unable to locate a Robinhood telephone number to report the Data Breach.

72. Robinhood Agent, unable to recall how to report a security incident, called a general Robinhood contact number at 11:13 p.m. and twice at 11:20 p.m., but was unable to reach any Robinhood employee.

73. A relative of Robinhood Agent, after becoming aware of the Data Breach, searched publicly-available information in an attempt to identify a Robinhood telephone number that Robinhood Agent could use to report the Data Breach.

74. This same relative even downloaded the Robinhood application in an unsuccessful effort to identify a telephone number for Robinhood Agent to call and report the issue.

75. Robinhood Agent contacted Robinhood's "ethics hotline," and reached an automated messaging service for ethics reporting managed by a third-party. Robinhood Agent did not leave a message. At 11:36 p.m., Robinhood Agent requested a call from Robinhood Supervisor by sending a direct message through a separate Robinhood Slack channel, stating that Robinhood Agent required emergency assistance.

76. Robinhood Agent also sent a Slack message requesting help from Robinhood's IT-Help Department at 11:52 p.m., approximately 19 minutes after rebooting the Robinhood Device at 11:33 p.m.

77. In response to this message, Robinhood Agent received an automated response from an internal bot named "Halp."

78. In another communication at 12:16 a.m., Robinhood Agent stated via Slack to Robinhood's IT-Help Department ("IT") that there was an emergency and that Robinhood Agent needed immediate help.

79. At 12:32 a.m., Robinhood Agent once again requested help from a Robinhood customer service manager by sending a direct message through a separate Robinhood Slack channel, again stating that an emergency situation existed.

80. Beginning at 12:37 a.m., Robinhood Agent conducted searches of Robinhood's internal Wikipedia-like system known as Confluence.

81. At 12:52 a.m. Robinhood Agent submitted a service ticket for a "Potential Computer Compromised" to Robinhood Security personnel.

82. At 12:55 a.m., Robinhood Agent received a call back from a Robinhood technical program manager.

83. At 12:49 a.m., nearly one hour after Robinhood Agent first sent a message to IT asking for someone to contact them, IT responded to Robinhood Agent's message. Robinhood Market's Security Incident Response Plan, as used by Robinhood, stated that reporting a security incident, such as the Data Breach, "should be easy for any individual to report" and identified ways Robinhood's security team may receive reports of a potential security incident.

84. Despite that training directive, according to testimony from Robinhood Agent, Robinhood Agent was unable to quickly identify the appropriate telephone hotline or contact information to report a data breach.

**c. Robinhood was on notice of the cybersecurity vulnerabilities used by the Unauthorized Third Party.**

85. Prior to the Data Breach, key industry guidance noted an increase in occurrences of social engineering attacks, including Verizon's widely-publicized 2020 and 2021 Annual Data Breach Investigations Reports.

86. Similarly, as early as 2018 FINRA issued direct guidance concerning cybersecurity practices, and noted that broker-dealer firms such as Robinhood must have in place processes to facilitate the secure notification of cybersecurity attacks by employees.

87. Robinhood's executives likewise were affirmatively on notice of the need to protect against the type of cybersecurity threats exposed by the Data Breach given that Robinhood Director briefed Robinhood executives on cybersecurity issues resulting from social engineering attacks prior to the Data Breach.

88. Prior to the Data Breach, Robinhood was aware that vishing, phishing, and caller ID spoofing were known cybersecurity threats, in addition to being aware of the security vulnerabilities created by remote access software such as AnyDesk.

89. Despite being on notice, Robinhood failed to reasonably implement its supervisory procedures to protect against the download of third-party software.

90. AnyDesk in particular was, or should have been, a known security risk at the time of the Data Breach.

91. On July 21, 2017, the Verizon Cyber Intelligence Center issued a public notice highlighting AnyDesk as a security vulnerability.



92. Furthermore, the U.S. Cybersecurity & Infrastructure Security Agency (“CISA”) published a bulletin on or about June 8, 2020, which identified AnyDesk as a “high” vulnerability program, and issued additional guidance in January and October 2021.

93. Despite such warnings, at the time of the Data Breach, Robinhood controls against downloading third party software, such as this version of AnyDesk, did not include a block of downloads of all such unapproved software.

94. While Robinhood’s policies and procedures required approval from Robinhood’s engineering team prior to remote access software being downloaded on devices with access to Robinhood Internal Systems, Robinhood failed to have adequate technical controls in place to stop an employee from downloading and using all unapproved software.

95. In this instance, Robinhood failed to prevent AnyDesk from being downloaded, installed, and run on the Robinhood Device.

96. Well-established cybersecurity and data privacy industry standards include placing restrictions on authorized users’ ability to download and install certain third-party software—including remote access software.

97. Robinhood failed to reasonably address the risk posed by malicious use of AnyDesk or take reasonable action to prevent its download and use on a Robinhood device.

98. In August 2022, Robinhood Crypto, an affiliate of Robinhood and subsidiary of Robinhood Markets, entered into a negotiated settlement concerning cybersecurity and virtual currency regulations which occurred between 2019 and 2020 with the New York State Department of Financial Services.

99. More recently, Robinhood settled class action claims in *Mehta v. Robinhood Financial LLC, et. al.*, No. 21-cv-01013 (N.D. Cal. 2021) whereby class plaintiffs alleged Robinhood maintained inadequate cybersecurity controls that notably did not concern the particular cybersecurity deficiencies at issue in the Division’s investigation into the Data Breach.

**d. Robinhood agents failed to reasonably address the Data Breach.**

100. On November 6, 2021, Robinhood Agent, upon the encouragement of Robinhood Agent’s family and *after notifying and first communicating with Robinhood Director*, sent the following e-mail to Robinhood Director:

Hi [Robinhood Director],

Please find attached my resume [sic] for your reference. If you have any questions, please let me know[,] and I look forward to hearing from you!

Kind Regards,

[Robinhood Agent]

101. The e-mail that Robinhood Agent sent to Robinhood Director included an attached PDF entitled, “Resume [sic].”

102. The PDF attachment to Robinhood Agent’s e-mail to Robinhood Director was not a résumé; rather, it was Robinhood Agent’s “event log” for November 3, 2021 (the “Event Log”).

103. The Event Log contained Robinhood Agent’s contemporaneous recollection of the events of the Data Breach—including Robinhood Agent’s own account of the difficulties Robinhood Agent experienced in reporting the incident and lack of response from Robinhood even after expressing that the situation was an emergency.

**e. The Data Breach impacted Massachusetts consumers.**

104. On November 8, 2021, Robinhood publicly announced the Data Breach.

105. On November 8, 2021, Robinhood began contacting Massachusetts Individuals via e-mail (the “November 8<sup>th</sup> Notice”). In the November 8<sup>th</sup> Notice, Robinhood stated that as a consequence of the Data Breach affected individuals may now be targeted by phishing scams and recommended that the Massachusetts residents take further action of their own accord to mitigate the harm caused by the Data Breach.

106. Since the November 8<sup>th</sup> Notice, Massachusetts residents contacted the Division to register complaints regarding the Data Breach.

## **VII. VIOLATIONS OF LAW**

### **Count I – Violations of Mass. Gen. Laws ch. 110A, § 204(a)(2)(G)**

107. Section 204(a)(2)(G) of the Act provides in pertinent part:

The secretary may by order impose an administrative fine or censure or deny, suspend, or revoke any registration or take any other appropriate action if he finds (1) that the order is in the public interest and (2) that the applicant or registrant or, in the case of a broker-dealer or investment adviser, any partner, officer, or director, any person occupying a similar status or performing similar functions, or any person directly or indirectly controlling the broker-dealer or investment adviser:–

....

(G) has engaged in any unethical or dishonest conduct or practices in the securities, commodities or insurance business[.]

The Regulations further provide:

Each broker-dealer shall observe high standards of commercial honor and just and equitable principles of trade in the conduct of its business.

950 Mass. Code Regs. 12.204.

108. The conduct of Respondent, as described in Section VI(A) above, constitutes violations of Mass. Gen. Laws c. 110A, § 204(a)(2)(G).

**Count II – Violations of Mass. Gen. Laws ch. 110A, § 204(a)(2)(J)**

109. Section 204(a)(2)(J) of the Act provides:

The secretary may by order impose an administrative fine or censure or deny, suspend, or revoke any registration or take any other appropriate action if he finds ... (2) that the applicant or registrant or, in the case of a broker-dealer or investment adviser, any partner, officer, or director, any person occupying a similar status or performing similar functions, or any person directly or indirectly controlling the broker-dealer or investment adviser:

(J) has failed reasonably to supervise agents, investment adviser representatives or other employees to assure compliance with this chapter[.]

Mass. Gen. Laws c. 110A, § 204(a)(2)(J).

110. The conduct of Respondent, as described in Section VI(A) and VI(B) above, constitutes violations of Mass. Gen. Laws c. 110A, § 204(a)(2)(J).

**VIII. ORDER**

**IT IS HEREBY ORDERED:**

A. Robinhood shall permanently cease and desist from violations of the Act and Regulations in Massachusetts;

B. Robinhood is censured by the Division;

- C. For Massachusetts customers, Robinhood shall:
- a. Add disclosures to lists on its platform that are based on Robinhood data, such as those identified in Paragraph 31 of this Order, indicating that the list is based on Robinhood data and not directly related to overall market data;
  - b. Remove all emojis from the life-cycle of a transaction;
  - c. Permanently cease the future use of any waitlist tapping feature similar to that as described in Paragraph 31 of this Order;
  - d. Permanently cease the future use of confetti as described in Paragraph 31 of this Order or other celebratory imagery directly tied to frequency of trading;
  - e. Permanently cease the future use of generalized push notifications highlighting specific lists similar to that as described in Paragraph 31 of this Order; and
  - f. Permanently cease features that mimic games of chance similar to that as described in Paragraph 31(vii) of this Order.

D. Within thirty (30) days of the entry of this Order, Robinhood shall engage an independent compliance consultant who is not unacceptable to the Division (“Independent Compliance Consultant”) to:

- a. Attest that the previous changes recommended in the 2021 FINRA Third-Party Consultant Report have been implemented and they, or their substantial equivalent, are still properly functioning; and

- b. Attest the following regarding the Application's customer-facing features:
  - i. That the Application's pre-populated list disclosures are displayed to customers;
  - ii. Attest that emojis have been removed from customer communications related to the life-cycle of a transaction;
  - iii. Attest that there are no more waitlist features allowing certain customers to advance over others by tapping;
  - iv. Attest that there are no more generalized push notifications highlighting specific lists as described in Paragraph 31(iv) & (v) of this Order;
  
- c. Review, report, and make recommendations concerning the following:
  - i. The sufficiency of disclosures, the accuracy of educational materials, and reasonable policies and procedures for ensuring the use of lists, interfaces, and digital engagement practices with Massachusetts customers who self-identify as having limited to no prior trading experience comply with state and federal securities laws;
  - ii. The sufficiency of disclosures and the accuracy of educational materials to Massachusetts customers who self-identity as having limited to no prior trading experience concerning IPO access;

- iii. With respect to employee access:
    - a) The sufficiency of user access controls;
    - b) The sufficiency of controls on user ability to download third-party software;
    - c) The sufficiency of controls on user ability to access and download bulk-files;
  - iv. The sufficiency of the process for employees to report data breaches and other similar events; and
  - v. The reliance by Robinhood on cybersecurity policies and procedures established by Robinhood Markets.
- E. Within ninety (90) days of the entry of this Order:
- a. Robinhood shall submit a report to the Division containing the findings of the comprehensive review conducted pursuant to Section VIII(D) (the “Report”). The Report shall include, without limitation, a description of the review performed, the conclusions reached, and the recommendations for changes to the Application or relevant improvements.
  - b. The Report’s recommendations shall not be unacceptable to the Division, provided that the Division will not unreasonably withhold its consent of the recommendations; and
  - c. If the recommendations are not unacceptable to the Division, Robinhood shall promptly adopt all recommendations in the Report.

F. Within forty-five (45) days of the submission of the Supervisory Report to the Division, Robinhood shall implement all recommended changes to its platform and provide all recommended training to all Robinhood associated persons;

G. Within fifteen (15) business days of the entry of this Order, Robinhood shall pay an administrative fine in the amount of \$7,500,000 to the Commonwealth of Massachusetts. Payment shall be: (1) made by United States postal money order, certified check, bank cashier's check, bank money order, or wire transfer; (2) made payable to the Commonwealth of Massachusetts; (3) either hand-delivered or mailed to One Ashburton Place, Room 1701, Boston, Massachusetts 02108, or wired per Division instructions; and (4) submitted under cover letter or other documentation that identifies the payor making the payment and the docket number of the proceedings. Additionally, Robinhood shall provide the Division with notice twenty-four (24) hours prior to the payment;

H. Robinhood shall not claim, assert, or apply for a tax deduction or tax credit with regard to any state, federal or local tax for any amounts that Respondent shall pay pursuant to this Order;

I. Robinhood shall not seek or accept, directly or indirectly, reimbursement or indemnification, including, but not limited to, any payments made pursuant to any insurance policy, with regard to any amount that Robinhood shall pay pursuant to this Order;

J. If Robinhood is the subject of a voluntary or involuntary bankruptcy petition under Title 11 of the United States Code within three hundred sixty-five (365) days of the entry of this Order by the Division, Robinhood shall provide written notice to the Enforcement Section within five (5) days of the date of the petition;



K. Any fine, penalty, and/or money that it shall pay in accordance with this Order is intended by Robinhood and the Division to be a contemporaneous exchange for new value given to Robinhood pursuant to 11 U.S.C. § 547(c)(1)(A) and is, in fact, a substantially contemporaneous exchange pursuant to 11 U.S.C. § 547(c)(1)(B);

L. If Robinhood fails to comply with any of the terms set forth in this Order, the Enforcement Section may institute an action to have this agreement declared null and void. Additionally, Robinhood agrees that, after a fair hearing and the issuance of an order finding that Robinhood has not complied with this Order, the Enforcement Section may move to have this Order declared null and void, in whole or in part, and re-institute the associated proceeding that had been brought against Robinhood; and

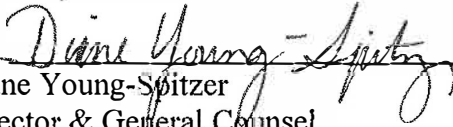
M. For good cause shown, the Enforcement Section may extend any of the procedural dates set forth above. Robinhood agrees to make any requests for extensions of the procedural dates set forth above in writing to the Enforcement Section.

#### **IX. NO DISQUALIFICATION**

This Order waives any disqualification in the Massachusetts laws, or rules or regulations thereunder, including any disqualification from relying upon the registration exemptions or safe harbor provisions to which Respondent may be subject. This Order is not intended to be a final order based upon violations of the Act that prohibit fraudulent, manipulative, or deceptive conduct. This Order is not intended to form the basis of any disqualifications under Section 3(a)(39) of the Securities Exchange Act of 1934; or Rules 504(b)(3) and 506(d)(1) of Regulation D, Rule 262(a) of Regulation A and Rule 503(a) of Regulation CF under the Securities Act of 1933. This Order is not intended to form the basis of disqualification under the FINRA rules prohibiting continuance in membership

absent the filing of a MC-400A application or disqualification under SRO rules prohibiting continuance in membership. This Order is not intended to form a basis of a disqualification under Section 204(a)(2) of the Uniform Securities Act of 1956 or Section 412(d) of the Uniform Securities Act of 2002. Except in an action by the Division to enforce the obligations this Order, any acts performed or documents executed in furtherance of this Order: (a) may not be deemed or used as an admission of, or evidence of, the validity of any alleged wrongdoing, liability, or lack of any wrongdoing or liability; or (b) may not be deemed or used as an admission of, or evidence of, any such alleged fault or omission of Respondent in any civil, criminal, arbitration, or administrative proceeding in any court, administrative agency, or tribunal.

**WILLIAM FRANCIS GALVIN  
SECRETARY OF THE COMMONWEALTH**

By:   
Diane Young-Spitzer  
Director & General Counsel  
Massachusetts Securities Division  
One Ashburton Place, Room 1701  
Boston, MA 02108

Date: January 18, 2024