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

IN THE MATTER OF:	)	
TRADEZERO AMERICA, INC.,	)	Docket No. E-2024-0374
RESPONDENT.	)	

CONSENT ORDER

I. PRELIMINARY STATEMENT

This Consent Order (the "Order") is entered into by the Securities Division of the Office of the Secretary of the Commonwealth of Massachusetts (the "Division") and TradeZero America, Inc. ("Respondent" and "TradeZero") with respect to the above-captioned investigation (the "Investigation") by the Enforcement Section of the Division into whether Respondent's acts and practices constituted violations of the Massachusetts Uniform Securities Act, M.G.L. c. 110A (the "Act"), and the regulations promulgated thereunder at 950 CMR 10.00-14.413 (the "Regulations"). Through the Investigation, the Division established that TradeZero violated Section 204(J) of the Act by failing to establish, implement, and maintain reasonable cybersecurity controls necessary to properly assess the risk of the company's third-party service providers. As a result, on July 29, 2024, TradeZero discovered that an unidentified and unauthorized person (the "Threat Actor") gained access to customers' personally identifiable information, impacting up to 14,543 people, including 346 Massachusetts residents (the "Data Breach"). The Division further established that

TradeZero violated Section 204(J) of the Act by failing to reasonably supervise its agents and representatives in connection with the use of an automated account approval program for reviewing customer margin account applications ("Robo Approval"), resulting in the improper approval of certain customers who presented patently inaccurate information, and in its failure to reasonably supervise its agents and representatives in the manual review of options trading applications.

On September 10, 2026, Respondent submitted an Offer of Settlement (the "Offer") to the Division. Respondent neither admits nor denies the Statement of Facts set forth in Section VI below and neither admits nor denies the Violations of Law set forth in Section VII below, and consents to the entry of this Order by the Division, consistent with the language and terms of the Offer, settling the Investigation with prejudice. Pursuant to M.G.L. c. 110A, § 412(b), this Order "is necessary or appropriate in the public interest or for the protection of investors and consistent with the purposes fairly intended by the policy and provisions of [the Act]."

II. JURISDICTION AND AUTHORITY

1. The Division has jurisdiction over matters related to securities pursuant to the Act and Regulations.

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

III. RELEVANT TIME PERIOD

3. Except as otherwise expressly stated, the acts and practices described herein occurred during the approximate time period of January 1, 2018 to April 31, 2025 (the "Relevant Time Period").

IV. RESPONDENT

4. TradeZero America, Inc. ("Respondent" and "TradeZero") is a corporation formed under the laws of the State of Delaware on September 2, 2015, with a principal office located at 67 35th Street, Suite B450, Brooklyn, New York 11232. Massachusetts approved TradeZero's registration as a broker-dealer on September 27, 2016. TradeZero maintains a Financial Industry Regulatory Authority ("FINRA") Central Registration Depository ("CRD") number of 282940.

V. RELATED PARTY

5. TradeZero Holding Corp. ("TradeZero Holding") is a corporation formed under the laws of the State of Delaware with a principal office at 67 35th Street, Suite B450, Brooklyn, New York 11232. TradeZero Holding is the ultimate parent entity of TradeZero. "TradeZero Affiliates" include any entity that is directly or indirectly owned, controlled by, or under common control with TradeZero Holding.

VI. STATEMENT OF FACTS

A. TradeZero's Failure to Establish and Enforce Necessary Cybersecurity Policies and Procedures Concerning Third-Party Vendors Resulted in a Data Breach That Impacted All of its Brokerage Customers.

6. TradeZero is an online brokerage platform that offers self-directed trading to its customers.

7. In 2018, TradeZero's founders started TradeZero America, Inc. to offer the TradeZero platform to customers in the United States, including customers in Massachusetts.

1. *State and Federal Laws and Regulations Require Broker-Dealers to Implement and Enforce Reasonable Cybersecurity Policies and Procedures to Protect Customer Information.*

8. Massachusetts-registered broker-dealers, such as TradeZero, are required to establish, maintain, and enforce reasonable cybersecurity programs to protect sensitive customer information, including *Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information*[1] ("Regulation S-P") and other applicable Massachusetts laws and regulations concerning cybersecurity and data privacy.

9. Regulation S-P requires registered financial firms, including broker dealers, to adopt "written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer information."[2]

10. Regulation S-P further requires that these policies and procedures "protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."[3]

2. *Prior Regulatory Guidance Explicitly Placed Broker-Dealers on Notice of Their Obligations Concerning Cybersecurity and Vendor Management.*

11. Broker-dealers' cybersecurity and data protection requirements extend to their third-party vendors.

[1] 17 C.F.R. § 248 (2000).
[2] 17 C.F.R. § 248.30(a) (2004).
[3] 17 C.F.R. § 248.30(a)(3) (2004).

12. FINRA has previously issued regulatory guidance to member firms covering issues related to member firms' use and supervision of vendors.

13. In February 2015, FINRA issued a *Report on Cybersecurity Practices*[4] (the "2015 Cybersecurity Report") to help FINRA member firms, including broker-dealers, identify and respond to cybersecurity threats.

14. In the 2015 Cybersecurity Report, FINRA highlighted the increasing frequency of member firms relying upon third-party vendors for a range of services, and warned member firms of cybersecurity risks in the event that a vendor is subject to a cybersecurity incident.

15. FINRA cautioned its member firms that "[r]isk-based due diligence on a prospective vendor's cybersecurity practices is a critical first step in selecting third-party service providers."[5]

16. FINRA further warned that firms must "establish appropriate contractual language to govern vendor relationships."[6]

17. Such governing contracts are necessary to clearly outline the rights and obligations of the vendor and broker-dealer, including "ongoing oversight of the vendor."[7]

18. FINRA specifically advised member firms to conduct due diligence on their vendors' controls and processes, even after the firm begins a vendor's service. FINRA found that such continued diligence is required to provide the firm with "sufficient information to assess whether the vendor is upholding its contractual commitments with respect to cybersecurity."[8]

---

[4] FINRA, REP. ON CYBERSECURITY PRAC. (2015), https://www.finra.org/sites/default/files/2020-07/2015-report-on-cybersecurity-practices.pdf.
[5] *Id.* at 26.
[6] *Id.* at 28.
[7] *Id.*
[8] *Id.* at 29.

19. Finally, the 2015 Cybersecurity Report recommended that "vendor systems and processes should be included in a firm's overall risk assessment process,"[9] meaning a firm must take appropriate steps to mitigate the risk in accordance with its internal governance process.

20. On August 13, 2021, FINRA published *Regulatory Notice 21-29: FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors*[10] ("Regulatory Notice 21-29").

21. Regulatory Notice 21-29 again reminded member firms of their compliance obligations under Regulation S-P with respect to cybersecurity and data protection.[11]

22. Regulatory Notice 21-29 specifically instructed that member firms:

- establish and maintain a supervisory system for activities or functions provided by third-party vendors that are reasonably designed to achieve compliance with applicable securities laws and regulations and with applicable FINRA rules;[12]
- institute a decision-making process as to whether a vendor should be used at all, including a consideration of the risks of outsourcing an activity to a vendor;[13]
- conduct due diligence on potential vendors, including consideration of the vendor's familiarity with regulatory requirements, risk management programs, information security controls, and reputation, among other factors;[14]

[9] *Id.*
[10] FINRA, REGULATORY NOTICE 21-29: VENDOR MGMT. AND OUTSOURCING (2021), https://www.finra.org/sites/default/files/2021-08/Regulatory-Notice-21-29.pdf.
[11] *Id.* at 4.
[12] *Id.* at 1.
[13] *Id.* at 8.
[14] *Id.*

- review their own diligence process and ask whether it evaluates the vendor's own cybersecurity controls and the vendor's risk to the firm's customers;[15] and
- consider putting a written contract in place that addresses the firm's and vendor's roles with respect to outsourced regulatory obligations.[16]

23. Finally, FINRA reminded member firms that they have a "continuing responsibility to oversee, supervise and monitor" the vendor's performance of the outsourced activity.[17]

3. *TradeZero Used the Vendor Tawk.to to Communicate With its Customers About Their Accounts*.

24. As an online trading platform, TradeZero does not maintain a physical location within Massachusetts where customers can meet with TradeZero representatives.

25. TradeZero customers must engage with TradeZero remotely to open an account, ask an account-related question, or obtain general customer support.

26. TradeZero's communication channels for its customers were limited to: an e-mail address, a telephone number to speak with a TradeZero representative, and a live chat service hosted on TradeZero's website.

27. From April 2018 through November 2024, TradeZero used a third-party vendor to facilitate its live chat service.

28. The vendor, Tawk.to, Inc. ("Tawk.to"), purports to operate as a software company that provides live chat services for company websites.

29. Live chat services are available through an application on TradeZero's website, located in the bottom corner of the viewer's screen (a "chat widget").

[15] *Id.* at 9.
[16] *Id.* at 10.
[17] *Id.* at 11.

30. Tawk.to offers a flexible pricing model for its chat services. Chat services begin at no cost, and companies can pay more money to enhance the service on their website.

31. For example, companies can pay to "white label" their Tawk.to chat service. "White labeling" removes the Tawk.to branding from the chat widget on the company website.

32. Tawk.to also provides live human agents who can monitor chat services at a cost beginning at $1 per hour.

33. Beginning in April 2018, TradeZero used a chat widget provided by Tawk.to on its website to communicate with TradeZero customers.

34. Customers visiting TradeZero's website could open a chat widget, enter their contact information and TradeZero account number (if applicable), and send a message to TradeZero through the chat widget.

35. From April 27, 2018 through April 27, 2025, TradeZero paid Tawk.to $144 annually to white label their chat widget.

36. From December 4, 2018 through February 4, 2021, TradeZero paid Tawk.to $610 per month to have live Tawk.to agents monitor and respond to messages coming through the chat widget on TradeZero's website outside of normal business hours and to create tickets for TradeZero's representatives to respond to. Tawk.to's live agents had standard FAQs provided by TradeZero.

37. From February 5, 2021 through August 5, 2022, TradeZero paid Tawk.to $1,200 per month for live chat monitoring services.

38. TradeZero also paid $380 to have Tawk.to agents monitor live chats between October 23, 2022 and November 23, 2022.

39. TradeZero failed to verify the identities or qualifications of the Tawk.to agents who monitored chats with TradeZero customers.

40. TradeZero permitted at least one of its new employees sign up for Tawk.to using his personal, non-TradeZero e-mail address, instead of an e-mail address associated with the company.

41. Even after adding a TradeZero e-mail address to his Tawk.to account, the employee was unable to remove his personal e-mail address from Tawk.to.

42. As a result, at least one TradeZero employee received TradeZero customer messages in his personal e-mail account.

4. *TradeZero's Failure to Implement, Maintain, and Enforce Reasonable Policies and Procedures Concerning Cybersecurity Culminated in a Data Breach Exposing Sensitive Information of Thousands of its Customers.*

43. On July 29, 2024, a Tawk.to account associated with a Canadian TradeZero Affiliate employee posted a suspicious message in an internal TradeZero chat.

44. The message stated that the employee's Tawk.to account had been compromised, and that an unknown threat actor (the "Threat Actor") claimed it had obtained access to over 185 gigabytes of TradeZero data.

45. The compromised information included sensitive customer information and personally identifiable information ("PII") of Massachusetts residents, including names and TradeZero account numbers.

46. Specifically, the Threat Actor claimed to have obtained data from "TradeZero Global, TradeZero America, and TradeZero Canada."

47. The Threat Actor demanded that TradeZero Holding pay a ransom of $250,000 in cryptocurrency in exchange for the deletion of the stolen information, or the Threat Actor would report the breach to news outlets and sell the data to "bad actors."

48. TradeZero Holding subsequently hired a cybersecurity consulting firm to communicate with the Threat Actor and negotiate the ransom demand.

49. TradeZero Holding ultimately paid $40,000 in Bitcoin to the Threat Actor in exchange for the Threat Actor's promise to return the data to TradeZero, and to suppress and delete the data.

50. TradeZero did not receive proof that the Threat Actor deleted the stolen information.

51. Tawk.to refused to provide TradeZero with security logs, user records, and suspicious access attempts to help TradeZero diagnose the source and scope of the Data Breach.

52. Because TradeZero had no contract with Tawk.to governing how the parties would address a security incident, TradeZero had no way to compel Tawk.to to produce the requested information needed to identify the scope of the compromised data.

53. In addition, TradeZero had no confidentiality agreement with Tawk.to to protect PII entered into the Tawk.to chat widget by TradeZero customers.

54. Certain TradeZero agents received PII from its customers through the chat widget.

55. TradeZero had no way to prevent customers from putting their PII into the chat widget.

56. TradeZero did not ascertain which of its customers were impacted by the Data Breach and instead chose to notify all of its potentially affected current and former

customers of the incident of all types of information potentially contained in the Tawk.to platform.

57. On September 19, 2024, TradeZero notified 14,543 individuals, including 346 Massachusetts residents, that their PII had been potentially compromised in the Data Breach.

58. TradeZero did not, however, notify all joint TradeZero account holders whose information was potentially exposed because TradeZero failed to provide required notification concerning the Data Breach to five Massachusetts residents who were joint account holders on TradeZero accounts.

5. *TradeZero Failed to Implement Reasonable Security Controls and Failed to Enforce its Existing Policies and Procedures With Respect to Third-Party Vendors*.

59. TradeZero Holding directed an affiliate, TradeZero USA, Inc., to handle all matters relating to information security on behalf of TradeZero, including the adoption of policies and procedures, as well as the establishment and implementation of cybersecurity and risk management systems.

60. TradeZero, the registered broker-dealer, has its own cybersecurity policies and procedures and cybersecurity incident response program, contained as a section within its Written Supervisory Procedures ("WSPs").

61. As part of its approach to security and risk mitigation, TradeZero Holding created an Information Security Steering Committee (the "ISSC"), comprised of representatives from TradeZero and other TradeZero Affiliates.

62. Under the ISSC's charter, ISSC meetings are held "quarterly or as otherwise determined by the [Chief Security Officer]."

63. The ISSC is responsible for ensuring that the organization's information security strategy and business objectives are aligned, reviewing organization policies and procedures pertaining to information security, approving the organization's risk governance structure, and monitoring cybersecurity risks.

64. The ISSC's recommendations apply to TradeZero Holding, and by extension, to all TradeZero Affiliates worldwide, including TradeZero America, Inc.

65. The ISSC was ineffective in ensuring that TradeZero had reasonable cybersecurity systems in place with regard to third-party vendor services, and failed to identify security flaws, such as those associated with the use of Tawk.to.

6. *TradeZero Failed to Establish, Maintain, and Enforce Policies Necessary to Supervise to a Third-Party Vendor it Used to Communicate With Brokerage Customers.*

66. TradeZero maintains an Information Security Policy ("ISP"), which "establishes control principles and policies" that apply to all TradeZero Affiliates, staff, and third parties who have access to TradeZero workplace environments, systems, or sensitive information ("Third Parties").

67. Prior to the implementation of the TradeZero ISP in November 2022, TradeZero had its own cybersecurity policies in place through its WSPs.

68. TradeZero added cybersecurity provisions to its WSPs in January 2021, nearly four years after TradeZero began operations in the United States.

69. TradeZero's use of Tawk.to predates the ISP. TradeZero did not maintain any similar policies and procedures in place at the time TradeZero began using Tawk.to.

70. Even in 2021, the cybersecurity provisions in TradeZero's WSPs required diligence and supervision of third-party vendors.

71. Despite these requirements, TradeZero took no steps to ensure that Tawk.to protected customer information.

72. The ISP imposes obligations with respect to "existing" Third Parties, but TradeZero failed to ensure that their use of Tawk.to complied with those obligations.

73. Section 1.5.1 of the ISP requires that the Legal Team "[u]se reasonable efforts to obtain contractual agreements with Third Parties that meet the specifications set forth in section 15.2."

74. Section 15.2.1 requires that Third-Party Agreements include security requirements, assignment of liabilities, and language that outlines the process of notification in the event the Third Party suffers an information or security breach.

75. TradeZero's failure to maintain a contract or service agreement with Tawk.to was inconsistent with Section 1.5.1 and Section 15.2.1 of its own ISP.

76. Each TradeZero employee had a Tawk.to account.

77. Thus, Tawk.to's terms of service, privacy policy, and data protection policy applied to the individual employees, not TradeZero.

78. Section 15.1.1 of the ISP requires TradeZero to perform risk assessments "to ensure that the Third Party controls are compliant with TZ information security requirements" ("Third-Party Risk Assessments").

79. The ISP requires that TradeZero reassess the risk of existing Third Parties "on an annual basis" to ensure that any risk associated with the Third Party has not increased.

80. TradeZero never performed any Third-Party Risk Assessments on Tawk.to, despite using the service since 2018.

81. TradeZero similarly never performed any sort of annual or periodic reviews of Tawk.to.

82. As a result, TradeZero failed to recognize or mitigate the cybersecurity risks that Tawk.to posed to TradeZero's business, and ultimately, its customers.

83. Section 15.4 of the ISP requires Third Parties with access to TradeZero information systems and information to comply with TradeZero's information security requirements and other "acceptable standards of security."

84. To ensure this, Section 15.4 of the ISP mandates "[m]onitoring and review of Third Party services" to ensure proper management of information security incidents and problems.

85. Although TradeZero's use of Tawk.to predated the ISP, as a Third Party, Tawk.to should have been subject to the provisions of the ISP upon its adoption.

86. TradeZero implemented a vendor monitoring program through a cybersecurity compliance firm, but did not use the program to monitor Tawk.to.

87. TradeZero did not retain any records or documentation concerning due diligence performed on Tawk.to prior to its implementation in 2018 because the TradeZero agent responsible for onboarding Tawk.to left the company in 2023.

88. As a result, TradeZero has no record of any vetting of the potential cybersecurity risks associated with Tawk.to.

89. TradeZero's WSPs in effect since January 2021 require TradeZero to keep a record of (i) due diligence performed on the vendor, (ii) the written contract with the vendor, (iii) reviews of vendor contracts, and (iv) actions taken regarding vendor vulnerabilities.

90. TradeZero did not have a written contract with Tawk.to, and did not keep record of any diligence or review of Tawk.to.

7. *TradeZero Failed to Establish Reasonable Policies and Procedures to Guide Employees on Cybersecurity Incident Response.*

91. TradeZero's WSPs contain limited cybersecurity incident response provisions.

92. However, prior to July 29, 2024, the date of the Data Breach, TradeZero did not have reasonable policies and procedures in place to protect against and mitigate the impact of cybersecurity incidents.

93. In an April 5, 2024 ISSC meeting, committee members discussed updates to TradeZero's policies, including "the new incident response policy."

94. Although the ISSC contemplated an incident response policy, no such policy was established before the Data Breach.

95. On July 29, 2024, after learning the Data Breach occurred, TradeZero Holding implemented a Security Incident Response Policy (the "SIRP").

96. The SIRP describes how TradeZero Holding and its Affiliates identify threats, respond to them before they spread, and remediate them before they cause harm.

97. TradeZero Holding's Chief Information Security Officer (the "CISO") is responsible for managing the SIRP and communicating the SIRP's requirements to TradeZero Affiliate's employees.

98. TradeZero had been in operation and registered as a broker-dealer in Massachusetts for nearly eight years prior to the implementation of the SIRP.

99. During this time, TradeZero operated with only the limited guidelines contained in its WSPs on how to respond to cybersecurity incidents.

8. *TradeZero Failed to Implement Basic Security Controls Such as Multi-Factor Authentication for its Representatives' Tawk.to Accounts.*

100. TradeZero failed to implement basic security controls, such as Multi-Factor Authentication ("MFA") for Tawk.to.

101. MFA requires a user attempting to log into an account to provide a second form of authentication—in addition to a username and password—before obtaining access to the account.

102. Common forms of MFA include text message codes sent to a user's cell phone number, or push notifications sent through an authenticator application that the user can access.

103. These secondary forms of verification are often only accessible to the account owner, and result in a lower likelihood of an unauthorized user successfully obtaining access to another individual's account.

104. TradeZero representatives with Tawk.to accounts commonly logged in to Tawk.to through their web browsers, using standard login credentials.

105. While Tawk.to accounts had an MFA setting, TradeZero did not have the capability to enable MFA for all TradeZero users of Tawk.to.

106. Instead, each TradeZero user needed to manually enable MFA for his or her own account.

107. Even after the Data Breach, TradeZero failed to take meaningful steps to ensure MFA was being used in connection with Tawk.to accounts.

B. TradeZero Failed to Establish and Enforce Reasonable Safeguards for the Review of Customer Applications for Margin Account and Options Trading.

108. TradeZero utilizes a multi-step, semi-automated account review process to verify applicant identities and approve client accounts.

109. TradeZero also used this semi-automated review process to approve customer accounts for margin trading.

110. First, TradeZero relies on its know-your-customer vendor (the "KYC Vendor") to verify applicant identities and identification documents, such as drivers' licenses.

111. Once the KYC Vendor verifies an applicant's identity, TradeZero uses proprietary software to automatically review account applications to determine whether an applicant should be approved for an account ("Robo Approval").

112. Robo Approval checks to ensure that the account type is suitable for the applicant, including an analysis of the applicant's age, employment history, and investment experience, among other factors.

113. If an application passes both the KYC Vendor and Robo Approval, TradeZero sends the application to TradeZero's clearing firm (the "Clearing Firm"), who conducts its own verification, including a credit check, of the applicant.

114. Separately, TradeZero's compliance team ("TradeZero Compliance") runs a background search on each applicant using a private search firm.

115. An application that passes the KYC Vendor, Robo Approval, and Clearing Firm is provisionally approved for an account.

116. Once provisionally approved, a TradeZero operations supervisor manually reviews the account to confirm its approval.

117. If the application fails meet any of the necessary criteria, the application is flagged and removed from the Robo Approval process.

118. A TradeZero operations associate then reviews the application manually, and may contact the applicant to request additional information, or reject the application.

119. TradeZero began using Robo Approval in June 2020 to speed up approval of customer account applications in response to increased customer growth during the COVID-19 pandemic.

120. TradeZero uses Robo Approval to review all brokerage account and margin account applications.

121. TradeZero does not use Robo Approval to review options trading applications.

1. *TradeZero Lacked Adequate Policies and Procedures Concerning its use of Robo Approval.*

122. TradeZero must follow SEC and FINRA rules and regulations with respect minimum required deposits in new margin accounts.

123. As of April 2025, TradeZero's WSPs require that a customer deposit the lesser of the amount specified in 12 C.F.R. § 220.12 ("Regulation T"), the amount specified in FINRA Rule 2520(c)(3), any greater amount that FINRA may require for specific securities, and $2,000.

124. Although the April 2025 WSPs reference FINRA Rule 2520, on May 22, 2024, FINRA adopted Rule 4210, which superseded Rule 2520.

125. While the specific requirements of Rules 2520 and 4210 are similar, TradeZero did not revise its policies and procedures in response to FINRA's adoption of its newer rule.

126. Additionally, TradeZero had insufficient policies and procedures in place with respect to Robo Approval use.

127. Instead, TradeZero had a one-page document outlining the minimum criteria required for automatic approval of an account (the "Robo Approval Guidelines").

128. The criteria include (i) passing a KYC check; (ii) the applicant is a United States citizen or visa holder; (iii) the applicant did not indicate "never employed" on their application; (iv) for margin accounts specifically, the applicant was at least 21 years old; (v) another KYC vendor matches the applicant's tax identification number and address; and (vi) the applicant is screened for risk associated with their identity.

129. The Robo Approval Guidelines require that a TradeZero principal review the documentation and run a background search on the applicant.

130. The Robo Approval Guidelines conclude that Robo Approval is used to "facilitate a timely on boarding of the customer."

131. The Robo Approval Guidelines do not address how to handle an application that does not meet the Robo Approval criteria.

132. The Robo Approval Guidelines also do not address how the TradeZero principal should manually review the documentation.

133. The document does not address how to consider an application with implausible or potentially incorrect information. Instead, Robo Approval simply checks whether the application contains a response within the set parameters, and if so, approves the application.

2. *TradeZero's Inadequate Policies and Procedures Concerning Customer Applications Resulted in the Improper Approval of Certain Applicants for Margin Accounts and Options Trading.*

134. The Robo Approval Guidelines failed to prevent TradeZero from opening accounts for certain customers who may not have been suited for margin accounts.

135. In several instances, Robo Approval failed to identify obvious issues in customer applications that would warrant a manual review, if not an outright rejection.

136. Such issues involved inconsistencies in age, trading experience, or occupation of the applicant that could be verified by a TradeZero agent during a manual review, but not necessarily flagged by an automated review process.

137. However, as long as the application met the criteria listed in the Robo Approval Guidelines, Robo Approval would approve the account.

138. As early as January 2021, TradeZero was aware that Robo Approval was approving applications that failed other stages of review.

139. On January 20, 2021, the TradeZero CEO sent a message to a colleague regarding "an account failed [KYC Vendor review] and went through Robo apprve [sic]."

a. Investor 1

140. Investor 1 is a natural person who resided in Massachusetts during the Relevant Time Period.

141. Investor 1 applied for an individual margin account on September 3, 2020.

142. At the time of his application, Investor 1 was a 21-year-old student.

143. In his application, Investor 1 claimed to have eight years of stock trading experience, and an annual income between $25,000 and $80,000 per year.

144. Essentially, Investor 1's application would mean that he was just 13 years old when he began trading stocks.

145. Investor 1 listed his employer as "University" and his occupation as "Finance."

146. Investor 1's account was opened and his margin application approved by Robo Approval on September 3, 2020.

147. Robo Approval did not detect the obvious discrepancy between Investor 1's age and his claimed trading experience.

148. Robo Approval also did not question whether a student without a clearly identified occupation had an income between $25,000 and $80,000 per year.

149. As a result, Robo Approval did not flag Investor 1's application for manual review.

150. TradeZero took no additional steps to verify that Investor 1 had eight years of stock trading experience, worked for the University, or earned an annual income between $25,000 and $80,000 per year.

b. Investor 2

151. Investor 2 is a natural person who resided in Massachusetts during the Relevant Time Period.

152. Investor 2 applied for an individual margin account on October 29, 2020.

153. At the time of his application, Investor 2 was 23 years old and self-employed.

154. In his application, Investor 2 disclosed that he had an annual income below $25,000 per year.

155. Investor 2 stated that he makes approximately 1,000 trades per year, with an average trade value of approximately $2,000.

156. Investor 2 also stated that he had just one year of investment experience at the time of his application.

157. Investor 2's account was opened on October 29, 2020, and his margin application was approved by Robo Approval on December 1, 2020.

158. Robo Approval did not contain criteria to prompt a manual review of a self-employed 23-year-old with a low income claiming to trade as frequently as Investor 2 claimed.

159. Robo Approval was not designed to compare an applicant's stated trading experience to the average amount and size of trades claimed in their application.

160. As a result, Robo Approval did not flag Investor 2's application for manual review.

161. TradeZero took no further steps to verify whether Investor 2 had the trading experience he claimed in his application.

162. TradeZero took no further steps to determine whether a margin account was suitable for Investor 2.

c. Investor 3

163. Investor 3 is a natural person who resided in Massachusetts during the Relevant Time Period.

164. Investor 3 applied for a margin account on January 28, 2021.

165. At the time of application, Investor 3 was a 23-year-old student.

166. Investor 3 listed his employer as "University" and his occupation as "Biology."

167. Investor 3 stated that his account would be funded by income, gifts, inheritance, and funds from another account.

168. Investor 3's account was opened and his margin application approved by Robo Approval on February 1, 2021.

169. TradeZero did not design Robo Approval with parameters to determine whether someone who stated their occupation as "Student" and claimed an income of under

$25,000, like Investor 3, had the financial ability to open a margin account and maintain the required minimum margin balance.

170. As a result, Robo Approval did not flag Investor 3's application for manual review.

171. TradeZero took no steps to verify that Investor 3 had the financial ability to fund his account.

172. TradeZero took no further steps to determine whether a margin account was suitable for Investor 3.

d. Investor 4

173. Investor 4 is a natural person who resided in Massachusetts during the Relevant Time Period.

174. Investor 4 applied for a margin account on January 28, 2021.

175. In his application, Investor 4 listed his employment status as "Not Employed."

176. However, Investor 4 also listed an employer, and stated that his annual income was between $25,000 and $80,000.

177. At the time of his application, Investor 4 was 26 years old and claimed to have eight years of investment experience.

178. Investor 4's account was opened and his margin application approved by Robo Approval on January 28, 2021.

179. TradeZero did not manually verify the discrepancy in Investor 4's employment information, and thus did not confirm whether Investor 4 was employed or not at the time of his application.

180. TradeZero took no further steps to determine whether an Investor 4's level of risk was in line with the information disclosed in his application.

3. *TradeZero Failed to Reasonably Supervise its Agents in Connection With Margin Account and Options Trading Applications.*

181. TradeZero failed to reasonably supervise its agents in connection with options trading applications and manual review of margin account applications which led to agents approving applications containing highly improbable—and in some cases, factually impossible—information.

182. For example, on November 30, 2020, a TradeZero agent ("TradeZero Agent 2") approved an application where the applicant ("Investor 5") stated that she had 100 years of securities trading experience.

183. Investor 5 is a natural person who resided in Massachusetts during the Relevant Time Period.

184. Investor 5 was 35 years old at the time of her application.

VII. VIOLATIONS OF LAW

Count I – Violations of M.G.L. c. 110A, § 204(a)(2)(J)

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

> (a) 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:—
> …
> (J) has failed reasonably to supervise agents, investment adviser representatives or other employees to assure compliance with this chapter;

M.G.L. c. 110A, § 204(a)(2)(J).

186. Respondent's acts and practices, as described above, constitute violations of M.G.L. c. 110A, § 204(a)(2)(J).

VIII. STATUTORY BASIS FOR RELIEF

Section 407A of the Act provides, in pertinent part:

> (a) If the secretary determines, after notice and opportunity for hearing, that any person has engaged in or is about to engage in any act or practice constituting a violation of any provision of this chapter or any rule or order issued thereunder, he may order such person to cease and desist from such unlawful act or practice and may take such affirmative action, including the imposition of an administrative fine, the issuance of an order for an accounting, disgorgement or rescission or any other such relief as in his judgment may be necessary to carry out the purposes of [the Act].
>
> M.G.L. c. 110A, § 407A.

IX. ORDER

IT IS HEREBY ORDERED:

A. Respondent shall permanently cease and desist from further acts and practices in violation of the Act and Regulations;

B. Respondent is censured by the Division;

C. Within thirty (30) days of the entry of this Order, Respondent shall:

1. Submit an accounting (the "Accounting") identifying all net trading losses incurred by the individuals identified as Investors 1 – 5 related to options or margin trading activity in a form that is not unacceptable to the Division;
2. Within five (5) days of submitting the Accounting, Respondent shall make payment of restitution in an amount equal to the total net trading loss incurred by each Investor in a form and manner not unacceptable to the Division; and

3. Respondent shall provide the Division with proof of payment of restitution in a form and manner not unacceptable to the Division within ten (10) days of making such payment.

D. Respondent shall pay an administrative fine in the amount of seven hundred fifty thousand dollars ($750,000 (USD)) to the Commonwealth of Massachusetts. The fine shall be paid in three (3) installments according to the following schedule:

1. Within ten (10) days of the entry of this Order, Respondent shall pay the first installment in the amount of two hundred fifty thousand dollars ($250,000 (USD));
2. Within one hundred twenty (120) days of the entry of this Order, Respondent shall pay the second installment in the amount of two hundred fifty thousand dollars ($250,000 (USD)); and
3. Within two hundred forty (240) days of the entry of this Order, Respondent shall pay the third and final installment in the amount of two hundred fifty thousand dollars ($250,000 (USD)).

Each payment shall be: (1) made by wire transfer, certified check, bank cashier's check, United States postal money order, or bank money order; (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, Respondent shall provide the Enforcement Section written notice of the form of payment and timing of payment at least three (3) business days prior to the payment;

E. Within sixty (60) days of the entry of this Order, Respondent shall retain an independent compliance consultant not unacceptable to the Division (the "Independent Cybersecurity Compliance Consultant") to review, report, and make recommendations concerning TradeZero's policies and procedures relating to:

1. Cybersecurity and data protection;
2. Cybersecurity incident response; and
3. Vetting, management, and review of third-party vendors.

F. Within ninety (90) days of the retention of the Independent Cybersecurity Compliance Consultant pursuant to Section IX(E):

1. Respondent shall submit a report to the Division containing the findings of the comprehensive review conducted pursuant to Section IX(E) (the "Cybersecurity Report"). The Cybersecurity Report shall include, without limitation, a description of the review performed, the conclusions reached, and the recommendations for changes to Respondent's policies and procedures relating to cybersecurity systems, cybersecurity incident response, third-party vendor vetting, review, and policies and procedures concerning the use of artificial intelligence;
2. The Cybersecurity Report's recommendations shall not be unacceptable to the Division; and
3. If the recommendations are not unacceptable to the Division, Respondent shall promptly adopt all recommendations in the Cybersecurity Report.

G. Within ninety (90) days of the entry of this Order, TradeZero's Chief Compliance Officer shall certify in writing to the Division that it has conducted a comprehensive review

of its policies and procedures relating to margins and options account approvals and use of TradeZero's Robo Approval system (the "TradeZero Certification").

H. The TradeZero Certification shall not be unacceptable to the Division, and shall include, without limitation, a description of the review performed, the conclusions reached, and shall specify the changes made to Respondent's policies and procedures relating to margins and options approval, and use of the Robo Approval system.

I. Respondent shall undertake an additional review and notification of all Massachusetts residents ("Impacted Residents") with PII involved in the Data Breach and not previously notified by Respondent. The identification and notification process shall be completed within ninety (90) days of the entry of the Order:

1. Within thirty (30) days of entry of this Order, Respondent shall submit to the Division a list of all Impacted Residents along with a proposed written notice ("Notice Letter") identifying the specific PII of the Impacted Resident and providing two (2) years of credit monitoring and identify theft protection service;
2. A finalized Notice Letter not unacceptable to the Division shall be mailed within fifteen (15) days after approval by the Division to all Impacted Residents;
3. Respondent shall provide the Division with a list of all Impacted Residents for whom Respondent receives a Notice Letter as returned to sender ("Undeliverable Residents"); and
4. To the extent the Division has access to different mailing address information for Undeliverable Residents, Respondent shall mail a second

Notice Letter within five (5) days of the Division providing such different address;

J. For purposes of this Order, the last day of the time period so computed is to be included unless it is a Saturday, Sunday, or legal holiday or any other day on which the Division is not open for regular business, in which event the period shall run until the end of the next following business day;

K. Respondent 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;

L. Respondent 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 Respondent shall pay pursuant to this Order;

M. If Respondent is the subject of a voluntary or involuntary bankruptcy petition within one (1) year of the entry of this Order, Respondent shall provide written notice to the Division within five (5) days of the date of the petition;

N. Any fine, penalty, and/or money that Respondent shall pay in accordance with this Order is intended by Respondent and the Division to be a contemporaneous exchange for new value given to Respondent 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);

O. If Respondent fails to comply with any of the terms set forth in this Order, the Division may institute an action to have this agreement declared null and void. After notice and an opportunity for hearing, and the issuance of an order finding that Respondent has

not complied with this Order, the Division 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 Respondent;

P. Failure to fully comply with any of the terms set forth in this Order is a violation of the Act and Regulations, and the Division may take action seeking compliance of any such terms or any such relief as may be necessary to carry out the purposes of the Act and Regulations; and

Q. For good cause shown, the Division may agree to extend any of the procedural dates set forth above. Respondent shall make any requests for extensions of the dates set forth above in writing to the Division.

IX. WAIVER

Respondent waives any right to contest this Order, including whether the Order is fair, reasonable, and in the public interest, any right to a hearing, to written findings of fact, conclusions of law, or to any other process provided by the Act and Regulations, and waives any right to judicial review of this Order under M.G.L. c. 110A, § 411 and M.G.L. c. 30A, § 14(7).

X. NO DISQUALIFICATION

This Order waives any disqualification in the laws of Massachusetts, 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 a 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 disqualification under 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 of 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

Anthony R. Leone, Esq.
Director
Securities Division
Office of the Secretary of the Commonwealth
John W. McCormack Building, 17th Floor
One Ashburton Place
Boston, MA 02108

Dated: 9/14/26