UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 95369 / July 27, 2022

ADMINISTRATIVE PROCEEDING
File No. 3-20938

In the Matter of **TRADESTATION SECURITIES, INC.** **Respondent.**	**ORDER INSTITUTING ADMINISTRATIVE AND CEASE-AND-DESIST PROCEEDINGS, PURSUANT TO SECTIONS 15(b) AND 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING REMEDIAL SANCTIONS AND A CEASE-AND-DESIST ORDER**

I.

The Securities and Exchange Commission ("Commission") deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934 ("Exchange Act") against TradeStation Securities, Inc. ("Respondent" or "TradeStation").

II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer") which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over it and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order ("Order"), as set forth below.

III.

On the basis of this Order and Respondent's Offer, the Commission finds that:

Summary

1. These proceedings arise out of TradeStation's failure to adequately develop and implement a written Identity Theft Prevention Program as required by Rule 201 of Regulation S-ID (17 C.F.R. § 248.201).

2. TradeStation is a broker-dealer registered with the Commission. From at least January 1, 2017, through October 31, 2019 (the "Relevant Period"), TradeStation violated Rule 201 of Regulation S-ID because its written Identity Theft Prevention Program (the "Program") lacked reasonable policies and procedures to: (i) identify relevant red flags for the covered accounts TradeStation offered and maintained and incorporate those red flags into its Program; (ii) respond appropriately to detected red flags to prevent and mitigate identity theft; and (iii) ensure that the Program was updated periodically.

3. Moreover, TradeStation violated Rule 201 of Regulation S-ID during the Relevant Period because it did not provide for the continued administration of its Program by failing to: (i) involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program; and (ii) exercise appropriate and effective oversight of service provider arrangements.

Respondent

4. TradeStation Securities, Inc. is a Florida corporation headquartered in Plantation, Florida that provides primarily commission-free, directed online brokerage services to retail and institutional customers. Its downloadable platform and web and mobile applications offer its customers access to equities, options, and futures trading. TradeStation has been a broker-dealer registered with the Commission pursuant to Section 15(b) of the Exchange Act since January 1996. The parent company of Respondent is TradeStation Group, Inc.

Background

5. During the Relevant Period, TradeStation's Identity Theft Prevention Program failed to comply with the requirements of Regulation S-ID.

6. Regulation S-ID went into effect on May 20, 2013, with a compliance date of November 20, 2013.[1]

[1] 78 Fed. Reg. 23638 (Apr. 19, 2013).

7. Regulation S-ID requires financial institutions, including broker-dealers registered with the Commission with covered accounts,[2] to "develop and implement a written Identity Theft Prevention Program . . . that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account."[3]

8. The written Identity Theft Prevention Program may incorporate by reference policies outside of the Identity Theft Prevention Program in order to satisfy the requirements of Regulation S-ID, but such incorporation must be explicit.[4]

9. An Identity Theft Prevention Program must include reasonable policies and procedures to: (i) identify relevant "red flags"[5] for the covered accounts and incorporate them into the Identity Theft Prevention Program; (ii) detect the red flags that have been incorporated into the Identity Theft Prevention Program; (iii) respond appropriately to any red flags that are detected pursuant to the Identity Theft Prevention Program; and (iv) ensure that the Identity Theft Prevention Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the firm from identity theft.[6]

10. The written Identity Theft Prevention Program "must be appropriate to the size and complexity of the financial institution . . . and the nature and scope of its activities."[7] With respect to the identification of relevant red flags, Regulation S-ID requires firms to consider several factors specific to the firm in order to identify red flags that are relevant to the firm's business and the nature and scope of its activities, such as the types of covered accounts it offers or maintains, methods it provides to open accounts, methods it provides to access accounts, and its previous experiences with identity theft.[8] In this regard, red flags relevant to accounts that may be opened or accessed remotely may differ from those relevant to accounts that require face-to-face contact.[9]

---

2 The rule defines a "covered account" to include an account that a broker-dealer or investment adviser "offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer." 17 C.F.R. § 248.201(b)(3)(i).

3 17 C.F.R. § 248.201(a)(1), (d)(1). The rule defines "identity theft" as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(b)(9).

4 *See* 17 C.F.R. § 248.201 app. A, sec. I.

5 "Red flags" are defined as "a pattern, practice, or specific activity that indicates the possible existence of identity theft." 17 C.F.R. § 248.201(b)(10).

6 17 C.F.R. § 248.201(d)(2)(i)-(iv).

7 17 C.F.R. § 248.201(d)(1).

8 17 C.F.R. § 248.201 app. A, sec. II(a)(1)-(4).

9 78 Fed. Reg. 23638, 23645; *see* 17 C.F.R. § 248.201, app. A, sec. II(a)(2).

11. Appendix A to Regulation S-ID, which contains guidelines intended to assist firms in the formulation and maintenance of a written Identity Theft Prevention Program that satisfies the requirements of Regulation S-ID, lists categories of red flags that firms consider incorporating in an Identity Theft Prevention Program "as appropriate,"[10] and includes, in Supplement A to Appendix A, a non-comprehensive list of examples of red flags for each of these categories that the firm "may consider incorporating into its Program, whether singly or in combination . . . from the following illustrative examples in connection with covered accounts."[11] As explained in the Regulation S-ID Adopting Release, "[r]ather than singling out specific red flags as mandatory or requiring specific policies and procedures to identify possible red flags, this first element provides financial institutions and creditors with flexibility in determining which red flags are relevant to their businesses and the covered accounts they manage over time . . . . Given the changing nature of identity theft, the Commissions believe that this element allows financial institutions or creditors to respond and adapt to new forms of identity theft and the attendant risks as they arise."[12]

12. With respect to responding to detected red flags in order to prevent and mitigate identity theft, the Identity Theft Prevention Program "should provide for appropriate responses" to detected red flags "that are commensurate with the degree of risk posed."[13] In determining an appropriate response, a firm "should consider aggravating factors that may heighten the risk of identity theft."[14] In that regard, appropriate responses might include, among others, contacting the consumer, not opening a new account, or notifying law enforcement.[15]

13. With respect to periodically updating the written Identity Theft Prevention Program, Appendix A provides that firms should consider factors such as: (i) experiences of the entity with identity theft; (ii) changes in methods of identity theft; (iii) changes in methods to detect, prevent or mitigate identity theft; (iv) changes in the types of accounts offered or maintained; and (v) changes in the firm's structure or service provider arrangements.[16]

14. Regulation S-ID also requires firms to provide for the continued administration of the written Identity Theft Prevention Program by involving the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Identity Theft Prevention Program,

---

[10] 17 C.F.R. § 248.201 app. A, sec. II(c).

[11] 17 C.F.R. § 248.201 app. A, supp. A.

[12] 78 Fed. Reg. 23638, 23646.

[13] 17 C.F.R. § 248.201 app. A, sec. IV.

[14] *Id.*

[15] 17 C.F.R. § 248.201 app. A, sec. IV(b), (e), (h).

[16] 17 C.F.R. § 248.201 app. A, sec. V(a)-(e).

training staff, as necessary, to effectively implement the Identity Theft Prevention Program, and exercising appropriate and effective oversight of service provider arrangements.[17]

15. The oversight by the board of directors, an appropriate committee thereof, or senior management should include reviewing reports of compliance with Regulation S-ID with at least an annual report that addresses matters related to the Identity Theft Prevention Program, such as effectiveness of the program's policies and procedures, service provider arrangements, and recommendations for material changes to the program.[18] With respect to the oversight of service provider arrangements in connection with one or more covered accounts, the firm "should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft."[19]

TradeStation's Identity Theft Prevention Program

16. Since May 20, 2013 and throughout the Relevant Period, TradeStation made no material changes to its Program.

17. During the Relevant Period, TradeStation's Program did not have or otherwise incorporate by reference reasonable policies and procedures to identify relevant red flags and incorporate them into the Program. TradeStation did not consider factors applicable to the firm in order to identify relevant red flags tailored to its particular business, such as the types of covered accounts it offers or maintains, methods to open accounts, methods to access accounts, and previous experiences with identity theft. TradeStation's Program only identified those red flags that were provided as non-comprehensive examples in Supplement A to Appendix A of Regulation S-ID and did not identify certain red flags relevant to its business and the nature and scope of its brokerage activities.

18. For example, TradeStation's Program referenced red flags related to a customer's physical appearance that were taken from the list of non-comprehensive red flags contained in Supplement A to Appendix A of Regulation S-ID. In that regard, TradeStation's Program provided that there would be a red flag where "[t]he photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification." However, nearly all of TradeStation's accounts were opened online during the Relevant Period, such that TradeStation would not have had the opportunity to compare a customer's physical appearance with the identification presented. In addition, the Program during the Relevant Period did not address photographic identification in conjunction with the firm's online account opening process. Moreover, TradeStation's Program referenced eight other red flags regarding information received from consumer reporting agencies that were again copied from the non-comprehensive list of examples contained in Supplement A. However, TradeStation

---

17 17 C.F.R. § 248.201(e)(2)-(4).

18 17 C.F.R. § 248.201, app. A, sec. VI(b)(2).

19 17 C.F.R. § 248.201, app. A, sec. VI(c).

did not obtain and review such consumer reports in connection with the opening of covered accounts during the Relevant Period.

19. During the Relevant Period, TradeStation's Program did not have or otherwise incorporate by reference reasonable policies and procedures to respond appropriately to red flags in order to prevent and mitigate identify theft. For example, TradeStation's Program provided only that, when employees identified a red flag associated with potential identity theft, "additional due diligence" should be performed. However, TradeStation's Program did not contain any policies or procedures regarding what specific steps TradeStation employees should actually undertake when performing any due diligence, the scope of the due diligence to be performed, or which persons to contact in connection with any such due diligence. Moreover, the Program did not contain other potentially appropriate responses to the detection of red flags, such as not opening a new account or notifying law enforcement.

20. During the Relevant Period, TradeStation's Program did not contain or otherwise incorporate by reference reasonable policies and procedures to ensure that it was updated periodically. While TradeStation's Program provided that the firm would periodically review and update the program, as necessary, to reflect changes in risks from identity theft, the Program failed to sufficiently identify red flags relevant to the firm's business and the covered accounts it managed over time, describe when the Program would be reviewed on a periodic basis, the process for how the Program would be updated, or factors that would necessitate an update to the Program. Moreover, despite significant changes in external cybersecurity risks related to identity theft,[20] there were no material changes to the Program from May 20, 2013, and throughout the relevant time period.

21. During the Relevant Period, TradeStation failed to adequately provide for the continued administration of its Program. For example, TradeStation did not provide reports specific to its Program or compliance with Regulation S-ID to the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management. The only reports potentially related to identity theft provided to the board of directors and/or senior management were limited to risk tolerance limit breaches triggered when one or more fraud incidents caused losses in excess of $50,000 in the prior quarter. Moreover, during the Relevant Period, TradeStation's Program did not include or incorporate by reference any policies and procedures for the oversight of service providers in order to ensure their activities were conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate risk of identity theft.

---

[20] *See, e.g.*, 78 Fed. Reg. 23638, 23638 ("Advancements in technology also have led to increasing threats to the integrity and privacy of personal information.") (footnote omitted).

Violation

22. As a result of the conduct described above, Respondent willfully[21] violated Rule 201 of Regulation S-ID (17 C.F.R. § 248.201), which requires registered broker-dealers that offer or maintain covered accounts to develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

TradeStation's Remedial Efforts

23. TradeStation has undertaken substantial remedial acts, including auditing and revising its Program.

24. In particular, TradeStation voluntarily retained an outside consulting firm to review its Program, which recommended various enhancements involving, among other things, identifying and responding to red flags and the administration and periodic updating of the Program, all of which TradeStation adopted. TradeStation also voluntarily provided the outside consulting firm's report and recommendations and made detailed presentations to the Commission's staff.

25. In determining to accept the Offer, the Commission considered the remedial acts undertaken by Respondent.

IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in Respondent's Offer.

Accordingly, pursuant to Sections 15(b) and 21C of the Exchange, it is hereby ORDERED that:

A. Respondent cease and desist from committing or causing any violations and any future violations of Rule 201 of Regulation S-ID (17 C.F.R. § 248.201).

B. Respondent is censured.

---

[21] "Willfully," for purposes of imposing relief under Section 15(b) of the Exchange Act, "'means no more than that the person charged with the duty knows what he is doing.'" *Wonsover v. SEC*, 205 F.3d 408, 414 (D.C. Cir. 2000) (quoting *Hughes v. SEC*, 174 F.2d 969, 977 (D.C. Cir. 1949)). There is no requirement that the actor "also be aware that he is violating one of the Rules or Acts." *Tager v. SEC*, 344 F.2d 5, 8 (2d Cir. 1965). The decision in *The Robare Group, Ltd. v. SEC*, which construed the term "willfully" for purposes of a differently structured statutory provision, does not alter that standard. 922 F.3d 468, 478-79 (D.C. Cir. 2019) (setting forth the showing required to establish that a person has "willfully omit[ted]" material information from a required disclosure in violation of Section 207 of the Advisers Act).

C. Respondent shall, within 30 days of the entry of this Order, pay a civil money penalty in the amount of $425,000.00 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Exchange Act Section 21F(g)(3). If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. § 3717.

Payment must be made in one of the following ways:

(1) Respondent may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

(2) Respondent may make direct payment from a bank account via Pay.gov through the SEC website at http://www.sec.gov/about/offices/ofm.htm; or

(3) Respondent may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center
Accounts Receivable Branch
HQ Bldg., Room 181, AMZ-341
6500 South MacArthur Boulevard
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying TradeStation Securities, Inc. as the Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Carolyn Welshhans, Division of Enforcement, Securities and Exchange Commission, 100 F St., NE, Washington, DC 20549.

D. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, it shall not argue that it is entitled to, nor shall it benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that it shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

By the Commission.

Vanessa A. Countryman
Secretary