

UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

INVESTMENT ADVISERS ACT OF 1940
Release No. 7028 / October 23, 2026

ADMINISTRATIVE PROCEEDING
File No. 3-22777

In the Matter of

TAG ASSOCIATES LLC,

Respondent.

**ORDER INSTITUTING ADMINISTRATIVE
AND CEASE-AND-DESIST PROCEEDINGS
PURSUANT TO SECTIONS 203(e) AND
203(k) OF THE INVESTMENT ADVISERS
ACT OF 1940, 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 203(e) and 203(k) of the Investment Advisers Act of 1940 (“Advisers Act”) against TAG Associates LLC (“TAG” or “Respondent”).

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 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 203(e) and 203(k) of the Investment Advisers Act of 1940, 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 finds¹ that:

¹ The findings herein are made pursuant to Respondent’s Offer of Settlement and are not binding on any other person or entity in this or any other proceeding.

Summary

1. This proceeding arises out of the failure of registered investment adviser TAG to obtain independent verification of certain client funds and securities over which it had custody and its failure to maintain certain securities with a qualified custodian in violation of Advisers Act Section 206(4) and Rule 206(4)-2 thereunder, commonly referred to as the “Custody Rule,” between December 2015 and September 2026.

2. Additionally, between June 2014 and December 2023, TAG violated Rule 201 of Regulation S-ID (17 C.F.R. § 248.201) because it failed to implement its written identity theft prevention program (the “Program”) by not undertaking any internal review of the Program and ensuring that the Program was updated periodically to address red flags TAG had detected in the course of its operations. TAG also violated Rule 201 of Regulation S-ID during this period because it did not provide for the continued administration of its Program by failing to involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, implementation, and administration of the Program.

Respondent

3. TAG is a Delaware limited liability company with its principal office and place of business in New York, New York. TAG provides investment advice to high-net-worth individuals and private funds and has been registered with the Commission as an investment adviser since January 2002. As of June 26, 2026, TAG held more than \$7 billion in regulatory assets under management for 90 clients.

TAG Violated the Custody Rule

4. The Custody Rule is designed to protect investment advisory clients from, among other things, the loss, misuse, or misappropriation of their funds and securities. The Custody Rule requires that registered investment advisers who have custody of client funds or securities implement an enumerated set of requirements.

5. An investment adviser has custody if it, or a related person, holds, directly or indirectly, client funds or securities, or if it, or a related person, has the authority to obtain possession of those funds and securities. *See* Advisers Act Rule 206(4)-2(d)(2). Custody includes, among other things, “[a]ny arrangement (including a general power of attorney) under which [the adviser is] authorized or permitted to withdraw client funds or securities maintained with a custodian upon [its] instruction to the custodian” and “[a]ny capacity (such as . . . managing member of a limited liability company or a comparable position for another type of pooled investment vehicle, or trustee of a trust) that gives [the adviser or its] supervised person legal ownership of or access to client funds or securities.” *Id.* A “related person” is defined as any person, directly or indirectly, controlling or controlled by the adviser, and any person that is under common control with the adviser. *See* Advisers Act Rule 206(4)-2(d)(7).

6. Under the Custody Rule, an investment adviser who has custody of client funds and securities must, among other things: (i) ensure that a qualified custodian maintains the client funds

and securities; (ii) notify the client in writing of accounts opened by the adviser at a qualified custodian on the client's behalf; (iii) have a reasonable basis for believing that the qualified custodian sends account statements at least quarterly to clients, except if the client is a limited partnership or limited liability company for which the adviser or a related person is a general partner or managing member, the account statements must be sent to each limited partner or member; and (iv) ensure that client funds and securities are verified by actual examination each year by an independent public accountant pursuant to a written agreement at a time chosen by the accountant without prior notice or announcement to the adviser. *See* Advisers Act Rules 206(4)-2(a)(1) – 206(4)-2(a)(5).

7. TAG had custody of client funds and securities held in certain managed accounts and was subject to the Custody Rule, including the Rule's requirement to have an independent public accountant conduct an annual surprise examination to verify such client funds and securities.

8. In 2015, Division of Examinations ("EXAMS") staff conducted an examination of TAG and identified certain client accounts for which TAG had custody but which were not subject to the annual surprise examination set forth in Rule 206(4)-2(a)(4), for the period March 2014 through February 2015, because TAG had failed to identify such accounts for the independent public accountant that it engaged to conduct surprise examinations. In March 2016, TAG included the accounts EXAMS staff identified with the accounts TAG identified for its independent public accountant for surprise examinations.

9. Nevertheless, TAG violated the Custody Rule with respect to 116 clients or client accounts, with more than \$129 million in regulatory assets under management.

10. For 112 client accounts, one or more TAG employees: (i) held signatory authority, whereby such TAG employees had the same ability to instruct the broker as to delivery of the accounts' funds and securities as did the beneficial owner of the account; (ii) had power of attorney agreements with trust advisory clients, which permitted TAG employees to execute financial transactions on behalf of clients; or (iii) served as trustee or co-trustee on trusts that were advisory clients, through which the TAG employees had access to and/or the ability to obtain possession of trust funds and securities without the consent of the respective co-trustees.

11. As a result of these arrangements, TAG had custody of client funds and securities held in these client accounts under the Custody Rule and was therefore required to obtain surprise examinations in accordance with Advisers Act Rule 206(4)-2(a)(4).

12. However, from approximately December 2015 through July 2024, TAG failed to identify these client accounts for its independent public accountant, and thus the client funds and securities held in these accounts were not subject to surprise examination as provided for in Advisers Act Rule 206(4)-2(a)(4).

13. In July 2024, after EXAMS staff identified certain of the 112 client accounts during another examination, TAG identified these client accounts for its independent public accountant for surprise examination and updated its policies and procedures concerning the identification of client accounts for which it had custody.

14. For four limited liability company clients, one or more TAG employees were identified as a manager, a co-manager or an officer of each limited liability company such that a TAG employee had authority to obtain possession of client funds and securities. Each of these limited liability company clients held privately offered securities that were not maintained at a qualified custodian for various periods of time beginning in December 2015. With respect to these securities, TAG purported to rely on the exception to the qualified custodian requirement that is available for certain privately offered securities. That exception, contained in Advisers Act Rule 206(4)-2(b)(2), only extends to limited liability companies when such entities are audited and audited financial statements are distributed as described in Rule 206(4)-2(b)(4) (the “Privately Offered Securities Exception”).

15. TAG did not obtain an audit of any of these limited liability company clients and did not distribute audited financials of these limited liability companies as required by the Privately Offered Securities Exception. TAG did not satisfy the requirements of the Privately Offered Securities Exception and was thus required to comply with Advisers Act Rule 206(4)-2(a)(1), which TAG failed to do. Furthermore, TAG failed to comply with the requirements otherwise set forth in Advisers Act Rule 206(4)-2(a) for such clients.

16. TAG removed the TAG employees that served as managers, co-managers, and/or officers from these limited liability company clients by September 2026.

TAG Violated Regulation S-ID

17. Regulation S-ID requires financial institutions, including investment advisers registered with the Commission with 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.” 17 C.F.R. § 248.201(a)(1), (d)(1). The rule defines a “covered account” to include an account that a financial institution “offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions.” 17 C.F.R. § 248.201(b)(3)(i). 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).

18. Under Regulation S-ID, an Identity Theft Prevention Program must include reasonable policies and procedures to: (i) identify relevant “red flags” for the covered accounts and incorporate them into the program; (ii) detect the red flags that have been incorporated into the program; (iii) respond appropriately to any red flags that are detected pursuant to the program to prevent and mitigate identity theft; and (iv) ensure that the program, including red flags determined to be relevant, is updated periodically to reflect changes in risks to customers and to the safety and soundness of the firm from identity theft. 17 C.F.R. § 248.201(d)(2)(i)-(iv). “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).

19. 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 maintains, methods it provides to open covered accounts, methods it provides to access covered accounts, and its previous experiences with identity theft. 17 C.F.R. § 248.201(f) & app. A, sec. II(a)(1)-(4). 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. Identity Theft Red Flags Rule, 78 Fed. Reg. 23638, 23645 (Apr. 19, 2013); *see* 17 C.F.R. § 248.201, app. A, sec. II(a)(2).

20. With respect to responding to detected red flags in order to prevent and mitigate identity theft, Appendix A of Regulation S-ID provides that an Identity Theft Prevention Program should include policies and procedures that "provide for appropriate responses" to detected red flags "that are commensurate with the degree of risk posed." 17 C.F.R. § 248.201 app. A, sec. IV. In determining an appropriate response, a firm "should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records." *Id.*

21. 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 firm with identity theft; (ii) changes in methods of identity theft; (iii) changes in methods to detect, prevent, and 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. 17 C.F.R. § 248.201 app. A, sec. V(a)-(e).

22. 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. 17 C.F.R. § 248.201(e)(2).

23. The oversight by the board of directors, an appropriate committee thereof, or senior management should include reviewing reports of compliance with Regulation S-ID at least annually. 17 C.F.R. § 248.201, app. A, sec. VI(a), (b)(1). Those reports should address material matters related to the Identity Theft Prevention Program, such as effectiveness of the program's policies and procedures, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for material changes to the program. 17 C.F.R. § 248.201, app. A, sec. VI(b)(2).

24. The compliance date for Regulation S-ID was November 20, 2013.

25. TAG first developed and implemented its Program on June 12, 2014, which it referred to internally as the "Red Flag Program."

26. The Program included a section for the identification of red flags, which was based largely on the set of sample red flags provided in the Supplement A to Appendix A of Regulation S-ID. The Program also provided for a mechanism to update the Program, in a

section titled, “Updates and Annual Review.” It required TAG to update its Program when TAG had a material change to its operations, structure, business, or location, or when TAG experienced a material identity theft incident or a series of related identity theft incidents to covered accounts. This section further stated that TAG would “follow new ways that identities can be compromised and evaluate the risk they pose for [the] firm.” This section also required TAG’s chief compliance officer to include a review of the Program as part of the annual review of TAG’s compliance policies and procedures.

27. Beginning in at least 2015 and continuing through December 2023, TAG retained compliance consultants to perform an annual review of its compliance policies and procedures. Though TAG sent these compliance consultants copies of its policies and procedures, including the Program, the scope of work for each of these compliance consultants did not reference the Program nor did they reference Regulation S-ID.

28. In fact, in a report from one of its compliance consultants for the year 2017, TAG was advised that it should undertake its own reviews of the Program to ensure that it remained comprehensive and appropriate to TAG’s business model.

29. Between June 2014 and December 2023, TAG employees frequently exchanged emails discussing: (1) attempted, unsuccessful identity thefts on covered accounts at TAG; (2) email phishing scams occurring throughout the financial services industry and at service providers; and (3) identity theft that had occurred at other firms. In that same period, TAG was the target of dozens of unsuccessful identity theft attempts.

30. For example, in November 2017, a TAG employee sent an email to all TAG employees letting them know that TAG had just received a fake wire transfer request, writing “[p]lease be sure to double check all email addresses and get all verbal confirms. This request used the client’s correct email address up to the @ but everything after that was fake.”

31. In another example, in April 2021, TAG’s chief executive officer emailed all TAG employees informing them that TAG encountered “another fraud attempt today on a client’s account. Hackers accessed a client email account and requested a wire transfer from the bank.” TAG’s chief executive officer went on to state that certain processes had prevented the hacker from being successful, including verifying new vendors or wire information before sending money and reminding employees not to use the phone number included on the email to do the verification.

32. Nevertheless, between June 2014 and December 2023, TAG failed to implement its Program because it did not undertake any internal review of the Program, did not evaluate these newly identified risks vis-à-vis the red flags in its Program, and did not assess whether any updates should be made to the Program.

33. TAG also failed to provide for the continued administration of the Program by failing to involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, implementation, and administration of the Program during this same period.

34. In a Program section titled “Internal Compliance Reporting,” a designated TAG employee was required to report annually to TAG’s chief executive officer on compliance with the Program. This section specified that “[t]he report will address” various categories, including: (i) the effectiveness of the Program in addressing identity theft risks in connection with covered accounts; (ii) significant incidents involving identity theft and management’s response; and (iii) recommendations for changes and improvements to the Program.

35. Neither the designated TAG employee nor anyone else made any such annual reports regarding the Program, its effectiveness, significant identity theft incidents, or any recommendations to change or improve the Program to TAG’s chief executive officer between June 2014 and December 2023.

36. In December 2023, TAG updated the Program for the first time. TAG incorporated the updated Program in the firm’s compliance manual and added additional red flags specific to email-related identity theft and wire transfers.

Violations

37. As a result of the conduct described above, Respondent willfully² violated Advisers Act Section 206(4) and Rule 206(4)-2 thereunder.

38. As a result of the conduct described above, Respondent willfully violated Rule 201 of Regulation S-ID (17 C.F.R. § 248.201).

TAG’s Cooperation and Remedial Efforts

39. In determining to accept the Offer, the Commission considered the cooperation TAG afforded the Commission staff and remedial acts TAG promptly undertook.

² “Willfully,” for purposes of imposing relief under Section 203(e) of the Advisers 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).

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 Advisers Act Sections 203(e) and 203(k), it is hereby ORDERED that:

A. Respondent cease and desist from committing or causing any violations and any future violations of Advisers Act Section 206(4) and Rule 206(4)-2 thereunder and Rule 201 of Regulation S-ID (17 C.F.R. § 248.201).

B. Respondent TAG is censured.

C. Respondent shall, within ten (10) days of the entry of this Order, pay a civil money penalty in the amount of \$175,000 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Section 21F(g)(3) of the Securities Exchange Act of 1934. 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 TAG Associates LLC as a 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 Lee A. Greenwood, Deputy Chief, Asset Management Unit, Division of Enforcement, Securities and Exchange Commission, 100 Pearl Street, Suite 20-100, New York, NY 10004.

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