

No Client Harm, but SEC Still Charges Investment Adviser with Reg S-ID Failures

October 26, 2026

On October 23, 2026, the Securities and Exchange Commission (“SEC”) brought a [settled enforcement action](#) against registered investment adviser TAG Associates LLC (“TAG”) for violations of Rule 201 of Regulation S-ID (“Reg S-ID”), also known as the Identity Theft Red Flags Rule (“Red Flags Rule”). The SEC found that TAG failed to adequately implement and update its written Identity Theft Prevention Program (“ITPP”) over a nearly decade-long period, despite encountering numerous attempted identity theft incidents and being aware of evolving fraud risks.

Notably, the SEC’s order does not identify any successful identity theft, fraudulent transfer or resulting client loss. To the contrary, the order describes dozens of unsuccessful fraud attempts, including an incident in which existing verification procedures prevented an unauthorized wire transfer. Nevertheless, the SEC concluded that TAG violated Reg S-ID by failing to periodically review its ITPP, assess whether identified risks warranted updates, and provide appropriate senior management oversight.

The action reinforces that firms may face Reg S-ID enforcement exposure for deficiencies in their identity theft prevention programs even absent identified successful fraud or customer harm. Reg S-ID enforcement risk can arise when firms fail to review and update their ITPPs in light of attempted fraud and evolving threats and maintain meaningful senior management oversight.

Without admitting the SEC’s findings, TAG consented to a censure, a cease-and-desist order and a \$175,000 civil penalty in a settlement that also resolved separate violations of the Advisers Act Custody Rule. The Custody Rule violations were significant, involving 116 clients or client accounts with more than \$129 million in regulatory assets under management. Although it is unclear whether the SEC would have pursued the Reg S-ID violations as a standalone enforcement action, the settlement illustrates how deficiencies in an identity theft prevention program can provide an additional and relatively identifiable enforcement hook in cases involving separate substantive violations—even where the SEC identifies no successful identity theft or resulting client harm.

Reg S-ID's Requirements. Reg S-ID requires SEC-registered financial institutions and creditors with "covered accounts" to maintain a written identity theft prevention program designed to detect, prevent and mitigate identity theft. Covered accounts include certain accounts maintained for personal, family or household purposes involving multiple transactions, as well as other accounts presenting a reasonably foreseeable risk of identity theft. The rule defines identity theft to include both completed and attempted fraud involving the unauthorized use of another person's identifying information.

An ITPP must include reasonable policies and procedures to:

- identify relevant red flags for covered accounts;
- detect and appropriately respond to those red flags;
- periodically update the program to reflect changing identity theft risks; and
- provide for continued administration and oversight by the board of directors, an appropriate committee or designated senior management personnel.

Firms must implement their Reg S-ID programs and periodically assess whether their red flags and procedures remain appropriate in light of their operations, experiences with identity theft and evolving threats.

The SEC's Findings Against TAG. TAG adopted its ITPP in June 2014, incorporating many of the sample red flags identified in Reg S-ID. According to the SEC, however, TAG failed to undertake an internal review or update the program until December 2023, notwithstanding repeated attempted identity theft incidents and its own policies requiring periodic review. The SEC identified three principal deficiencies. Significantly, the SEC did not identify any successful identity theft or resulting client loss. Instead, the Reg S-ID charges rested on TAG's failure to review, update and oversee its written ITPP despite its awareness of attempted fraud and evolving risks.

Failure to Review and Update the ITPP. Between June 2014 and December 2023, TAG encountered dozens of unsuccessful identity theft attempts. In November 2017, for example, a TAG employee warned colleagues of a fraudulent wire request sent from an email address that matched a client's address except for the domain name. In April 2021, TAG's CEO circulated a warning after hackers accessed a client's email account and requested a wire transfer from the bank. Existing verification procedures prevented the attempted fraud.

Despite these incidents, TAG did not conduct an internal review of its ITPP, evaluate the newly identified risks against its existing red flags, or assess whether updates were warranted. The firm did not revise its program until December 2023, when it added red flags addressing email-related identity theft and wire transfers.

Inadequate Compliance Reviews. Although TAG engaged outside compliance consultants to conduct annual reviews and provided them with its ITPP, the consultants' work mandates did not specifically address the program or Reg S-ID. A consultant advised TAG in 2017 to conduct its own ITPP reviews, but TAG failed to do so. The SEC found that TAG did not undertake the internal reviews necessary to evaluate its program and determine whether updates were appropriate.

Lack of Senior Management Oversight. TAG's ITPP required annual reports to the CEO addressing the program's effectiveness, significant identity theft incidents, management's responses and recommended improvements. According to the SEC, no such reports were provided between June 2014 and December 2023. The SEC found that TAG also failed to involve its board, an appropriate committee or designated senior management personnel in the program's ongoing oversight, implementation and administration.

Key Takeaways for Reg S-ID Compliance. The TAG settlement offers several practical lessons for Reg S-ID compliance:

- **Effective Fraud Controls Do Not Substitute for Reg S-ID Compliance.** The SEC pursued charges despite TAG's success in preventing attempted fraud. Firms should ensure that their ITPPs satisfy Reg S-ID's independent requirements for periodic review, updating and oversight, even where existing fraud prevention controls are effective.
- **Use Attempted Fraud to Inform—and Document—ITPP Reviews.** Firms should assess whether attempted fraud, including unsuccessful phishing and fraudulent transfer requests, warrants changes to their red flags or procedures. Firms should consider documenting their reviews, including the rationale for decisions not to update the program. Not every attempted fraud requires a substantive update, but relevant incidents should inform the firm's ongoing risk assessment.
- **Establish Meaningful Senior Management Oversight.** Firms should ensure that their boards, appropriate committees or designated senior management personnel receive periodic reports on ITPP effectiveness, significant incidents and recommended improvements. Appendix A to Reg S-ID contemplates at least annual reporting. Informal communications about particular fraud attempts may not suffice to demonstrate meaningful program oversight.

- **Ensure Compliance Reviews Specifically Address Reg S-ID.** Firms should confirm that internal reviews and outside compliance engagements expressly cover their ITPPs, rather than assuming that general compliance reviews are sufficient. Reviews should draw on relevant expertise across compliance, cybersecurity and operations, as appropriate, to ensure that written policies reflect current risks and actual practices.

To subscribe to the Data Blog, please [click here](#).

The cover art used in this blog post was generated by ChatGPT 6 Astra.

* * *

Please do not hesitate to contact us with any questions.



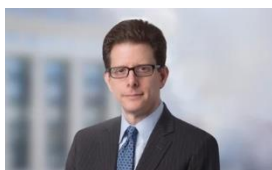
Andrew J. Ceresney
Partner, New York
+1 212 909 6947
aceresney@debevoise.com



Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandrasekhar@debevoise.com



Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com



Robert B. Kaplan
Partner, Washington, D.C.
+1 202 383 8060
rbkaplan@debevoise.com



Julie M. Riewe
Partner, Washington, D.C.
San Francisco
+1 202 383 8070
jriewe@debevoise.com



Kristin A. Snyder
Partner, San Francisco
+1 415 738 5718
kasnyder@debevoise.com

This publication is for general information purposes only. It is not intended to provide, nor is it to be used as, a substitute for legal advice. In some jurisdictions it may be considered attorney advertising.