BCLP. Client Intelligent

Insights

FINRA FILES COMPLAINT AGAINST FIRM CEO/CCO FOR CAUSING REGULATION S-ID VIOLATIONS, IN FIRST-EVER FINRA ENFORCEMENT CASE OF ITS KIND

Apr 15, 2021

FINRA recently filed a Complaint against a Chief Executive Officer and Chief Compliance Officer of a registered broker-dealer alleging, among other things, that the individual caused the broker-dealer to have wide-ranging violations of the SEC's Identity Theft Red Flags Rule, Regulation S-ID. This is believed to be the first case FINRA has ever brought against an individual in the Reg. S-ID space, although the SEC previously brought a similar action against Voya Financial Advisors, Inc. The recent Complaint comes on the heels of a settlement in December 2020 by the CEO/CCO's broker-dealer, in which FINRA: (1) found that the firm violated Reg. S-ID and FINRA Rule 2010 by failing to develop and implement an appropriate written Identify Theft Program, (2) fined the firm $65,000, and (3) required the firm to notify potential impacted customers that their personal identifying information may have been compromised. The cases provide a stark reminder that executives and compliance officer of broker-dealers must develop appropriate Identity Theft Procedures tailored to their firm's business model and, of far more significance, when confronted with "red flags" of a potential data breach, immediately take appropriate steps to notify potential impacted customers and appropriate regulators and law enforcement agencies. Indeed, the clear message of these actions is that paper policies without operationalization of the policies is not enough. Any failure to develop and implement appropriate procedures, or take swift and comprehensive steps in the face of a potential data breach can (as these cases make clear) result in a potential loss of securities licenses, significant fines and reputational harm.

Rule 201 of Regulation S-ID requires SEC registered broker-dealers 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." "Covered account" includes a retail broker-dealer account. Under Rule 201, a broker-dealer's Identity Theft Prevention Program ("ID Theft Program") must include "reasonable policies and procedures" to identify red flags of identity theft relevant to the firm's business, detect those red flags and appropriately respond to them, and ensure that the Program remains up-to-date with respect to the Identity Theft risks. Like many other data privacy regimes, the ID Theft Program is not overly

prescriptive—regulated entities have flexibility in crafting procedures specific to their operations and size. But, such programs must also be acted upon when circumstances arise.

FINRA's Complaint filed against Henry Clay Smith II on April 7, 2021 alleges that Smith, as Supreme Alliance, LLC's ("Supreme Alliance") CEO and CCO, was responsible for designing and implementing Supreme Alliance's ID Theft Program. Of particular note, the firm maintained no written procedures regarding how to identify and detect red flags of Identity Theft. Further, while the firm maintained some minimal procedures regarding responding to potential Identity Theft issues, these procedures were inadequate because they simply stated that "appropriate law enforcement agencies" should be contacted. The procedures did not identify what constituted "Identity Theft," what information was to be provided to law enforcement in the event of potential Identify Theft, or a timeframe for contacting law enforcement and providing information about the matter. Of course, notification obligations vary significantly by state, not only with respect to what data triggers a reporting obligations, but also when and to whom such reports must be made. The Complaint further alleges that the procedures were not tailored to Supreme Alliance's business model – for instance, the procedures provided that the firm's legal department would take an active role in investigating suspected incident of Identity Theft. Supreme Alliance, however, never had any legal department during the Relevant Period.

Most problematic, though, are the Complaint's allegations regarding Smith's inaction after receiving unmistakable indications that his Supreme Alliance e-mail account had been compromised. Beginning on April 18, 2018, Smith began receiving notifications that e-mail messages previously sent from his firm account could not be delivered to a certain external e-mail address. On that day, Smith received eight (8) such undeliverable notifications. Between April 18 and August 30, 2018, Smith received 120 such undeliverable notifications. On August 30, 2018, after forwarding one of these undeliverable e-mail messages to Supreme Alliance's e-mail vendor, Smith learned that his e-mail account had likely been compromised. FINRA alleged in its Complaint that between April 18 and August 30, 2018, approximately 200 e-mails or attachments had customer identifying information, including social security numbers, account numbers and birth dates. Smith, however, failed to notify law enforcement authorities (as the procedures required) or impacted customers, nor did he assess whether applicable state laws required notifying any state authorities of any potential identity theft.

Finally, FINRA also alleged that Smith impeded FINRA's investigation by providing false testimony during a FINRA on-the-record interview, and requesting that another firm employee provide false information to FINRA. FINRA's Complaint seeks all available relief for its causes of action in the Complaint.

FINRA's Complaint against Smith follows a December 2020 settlement (a FINRA "Letter of Acceptance, Waiver and Consent" or "AWC") with Supreme Alliance, in which the firm consented to findings that its ID Theft Program was inadequate because it lacked appropriate procedures to detect, prevent or mitigate identity theft in the opening or maintenance of customer accounts. The

Supreme Alliance AWC contains many of the same findings that serve as allegations in the Complaint against Smith. In particular, FINRA found that, after Supreme Alliance discovered a potential breach, it made no effort to determine how many of the CEO's e-mails had been potentially compromised, or whether customers' identifying information had actually been exposed. To the contrary, FINRA found that the firm did not even look into the matter until a May 2019 cycle examination, when FINRA staff began inquiring about the CEO's inability to deliver e-mails to the external e-mail address. Only then did Supreme Alliance commence an effort to understand the scope and nature of any potential breach or Identity Theft. Most troubling, though, was that as of the December 2020 AWC, Supreme Alliance still had not notified any potentially impacted customers. As a result, apart from the $65,000 fine imposed, the firm was required to certify in writing to FINRA that it: (1) notified potentially impacted customers of the breach, (2) revised its ID Theft Program to address the deficiencies identified in the settlement, and (3) enhanced its e-mail security systems to address the deficiencies identified in the settlement.

In light of the Supreme Alliance AWC and Smith Complaint, broker-dealers should carefully evaluate their ID Theft Programs. Among other things, firms should ensure that:

- The ID Theft Program contains written procedures regarding identifying and detecting red flags of Identity Theft;
- The written procedures specify, in the event of a breach, who is to take what steps, and a precise time frame in which the steps should be taken;
- The ID Theft Program should be tailored to the firm's particular business model, the electronic tools used, and the particular Identity Theft risks the firm may have; and
- The ID Theft Program is periodically updated (at a minimum annually, but ideally more frequently) to address evolving state and other laws that may require particular steps in the event of any breach.

Firms should also consider identifying and appointing outside counsel as a "breach coach," and identifying a forensic provider to be retained by outside counsel in the event of a data breach. In addition, firms should periodically address security obligations through risk assessments, third party audits, and "tabletop" sessions in which breach scenarios are rehearsed. Responding to breaches appropriately can be challenging, especially in exigent circumstances, but establishing organizational "muscle memory" in this area goes a long way toward achieving good execution when it counts.

Bryan Cave Leighton Paisner's Global Data Privacy and Security team has a world class incident response practice that has helped clients navigate major security incidents and data breaches. In that regard, our 24-hour hotline connects clients directly with experienced attorneys who will guide companies through all aspects of breach response. Our Broker-Dealer and Data Privacy and

Security teams have assisted numerous financial institutions with data breach issues, including an assessment of whether notification of regulators (i.e., FINRA) and state agencies is required.

RELATED CAPABILITIES

- Financial Regulation Compliance & Investigations
- Broker-Dealer and Investment Advisor Regulatory Enforcement, Disputes and Investigations
- Investigations
- Securities Litigation and Enforcement
- Data Privacy & Security

MEET THE TEAM

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144
