By Thomas D. Giachetti

The SEC is Watching Closely How Advisors Protect Clients From Identity Theft

It's smart to go beyond a written program and implement multi-factor authentication.

Here's a warning: Protecting your clients from identity theft means don't rely solely on your written identity theft prevention program under regulation S-ID. Make sure you implement a multi-factor authentication where possible.

As we've told clients going through the Securities and Exchange Commission examination process, we've noticed an uptick in SEC staff inquiries related to identity theft prevention. Typically these questions are focused on whether registered investment advisors have adopted and are maintaining an effective written identity theft prevention program, especially if their money movement practices clearly subject them to Regulation S-ID. To address these important issues, I spoke with my partner, and our firm expert, Cary Kvitka.

WHICH RIAS ARE SUBJECT TO REGULATION S-ID?

Regulation S-ID applies to SEC-RIAs that maintain "Covered Accounts." While the exact definition of a Covered Account is complex, at its core it is an account: 1) designed to permit multiple payments to third parties, and 2) "there is a reasonably foreseeable risk" that someone could perpetrate an identity theft attack, and defraud or use the investment advisor as a conduit to steal client funds from that account.

Cary advised that if an advisor, or its representative, is deemed to have custody of any client funds or securities that it is required to report on Form ADV Part 1, Item 9, then the affected accounts should be treated as Covered Accounts for the purposes of Regulation S-ID. In that case, the RIA should adopt a written identity theft prevention program meeting the requirements of Regulation S-ID. At a minimum, the accounts reported on ADV Part 1 Item 9 would be subject to the written identity theft prevention program.

However, we also caution RIAs to look at all of their money movement practices at that time and decide if there is a reasonably foreseeable risk that someone could abuse that particular practice to abscond with its clients' funds from accounts that aren't reported on ADV Part 1, Item 9. While the term "reasonably foreseeable" is subjective, an advisor that chooses not to implement a written identity theft prevention program and later suffers an identity theft attack to the detriment of its client will be in an uncomfortable position — to say the least.

Therefore, it's wise to err on the side of caution and implement a written identity theft prevention program if the advisor maintains accounts which permit the advisor to direct transfers to third parties, for which there is even the slightest chance that an identity theft attack may result in the misappropriation of its clients' funds.

WHAT ABOUT MULTI-FACTOR AUTHENTICATION?

Cary noted that "multi-factor authentication" means going through verification of at least two of these types of authentication factors: 1) knowledge factors, such as a password, 2) possession factors, such as a token or text message on a mobile device or application, or 3) inherence factors, such as a biometric characteristic (like a fingerprint).

In practice, this usually means that when a client or advisor representative is logging into a site containing confidential or nonpublic personal information, the multi-factor authentication mechanism will require them to enter a code sent to their mobile phone or another email address after entering the username and password.

We encourage the use of multi-factor authentication whenever practical for two reasons. First, there is always the possibility that the SEC can bring an enforcement action against a RIA for a data breach affecting its clients that could have been avoided, especially if it could have been averted using relatively inexpensive and functional defenses like multi-factor authentication. Second, unfortunately, we've been privy to data breaches that simply would not have transpired if the RIA implemented the use of multi-factor authentication.

Beware, regulators are aggressively watching. Please don't be their next enforcement victim. **IA**

Thomas D. Giachetti is chairman of the Investment Management and Securities Practice Group of Stark & Stark. He can be reached at tgiachetti@stark-stark.com.

ADOBE STOCK