WINSTEAD

Cybersecurity: Don't Become a Different Kind of Victim

01.15.19

A former broker at a national brokerage firm was recently sanctioned by FINRA after accepting instructions to transfer assets out of a client account. The problem? The instructions were actually sent by an imposter who had obtained access to the client's account, presumably through some form of cyber-crime. Unfortunately, the broker unwittingly contributed to the imposter's malfeasance by not only accepting the instructions but by also taking pro-active steps to circumvent his brokerage firm's controls.

This action joins a list of actions taken by FINRA and state securities regulators on similar issues, which we suspect will continue to grow as regulators continue to increase their scrutiny of cybersecurity controls and practices at financial service firms. Thus, broker-dealers and investment advisers would be wise to review and enhance, if needed, their systemic controls and incorporate training elements to reinforce their representatives' ability to identify suspicious conduct and act appropriately to avoid becoming victims themselves.

In the recent matter, the broker received e-mailed requests for wire transfers from a customer account. The individual posing as the customer had gained access to the customer's e-mail account. Of course, access to the e-mail account allowed the imposter to learn where the customer maintained a brokerage account. The imposter then used the e-mail account to submit instructions for transfers totaling almost $800,000.

It is not uncommon for brokerage firms to accept e-mail instructions from customers. However, it is essential that the firm require verbal verification of the instruction with the client even if the e-mail address is known to belong to the customer. In this case, the brokerage firm had implemented such a requirement. Just as important, the brokerage firm required that its brokers attest in writing that they have verbally verified wire requests with the relevant customer. This additional control mechanism is designed to minimize the chances that brokers simply forget to obtain verbal verification. Unfortunately, the broker in this matter falsely attested that he had obtained verbal verification and even took other steps to bypass active monitoring by other personnel at the brokerage firm.

The brokerage firm ended up reimbursing the customer and stepped into the customer's shoes as a victim. Notably, in this case, FINRA does not appear to have sanctioned the brokerage firm for any supervisory lapses associated with the transfers. This contrasts with other examples where brokerage firms have been held accountable even when they have already fully compensated their customers.[i] Thus, while the firm incurred a significant expense, it avoided additional cost and reputational harm by maintaining a well-designed system and because other personnel at the firm were clearly doing a good job of monitoring activity and supporting the firm's controls.

We expect that regulators will only be heightening their scrutiny of practices that can be affected by cyber-threats – both within a firm and at third-parties (such as customers). Towards that end, here are some reminders and ideas for brokerage firms and their representatives:

- Greatly limit (if not reject entirely) the ability to accept customer instructions via e-mail.
  - While it is common to require verbal verification for transfers to third-parties, such confirmations are not always required for transfers to accounts in the customer's name. Firms should carefully weigh the benefits of customer convenience with the associated risk as to all fund transfer requests.
- Require representatives and other personnel to pro-actively represent or acknowledge client contact.
  - Such documentation could serve the firm in any actions to sanction or terminate the relevant representative. But more importantly, the requirement is likely to be viewed by regulators as an important – if not essential – component of a reasonably-designed supervisory system.

- Training, training, training
  - Strong controls should go a long way to preventing damage in these cases. However, it is important that personnel understand that the controls are not simply technical requirements. Broker-dealers and investment advisers should incorporate examples such as the recent FINRA action into trainings on the subject. Moreover, the trainings should focus on identification of common red flags, such as the uncommon requests or pattern of requests, incorrect or little detail about accounts in e-mail request, and new or recently amended client contact

information.

- Empower customer contact throughout the organization.
  - Even the best designed supervision systems and training components are only as strong as the weakest member of the team. On these issues, a useful way to mitigate the risk of a "bad" team member is to permit, and even empower, direct customer contact by persons other than the primary representative and supervisor. In that way, the firm would avoid simply doubling-down on the bad team member's word if other personnel notice risks associated with customer transfers.

[i] *For example,* FINRA AWC No. 20130350000501 (June 19, 2015); Texas State Securities Board Order No. IC15-CAF-01 (July 27, 2015); Texas State Securities Board Order No. IC16-CAF-04 (March 7, 2016).

Contacts:

Ronak V. Patel
512.370.2892
rvpatel@winstead.com

Toby Galloway
817.420.8262
tgalloway@winstead.com