Regulatory Notice 12-05

Customer Account Protection

Verification of Emailed Instructions to Transmit or Withdraw Assets From Customer Accounts

January 2012

Notice Type
- Special Alert

Suggested Routing
- Operations
- Senior Management
- Systems

Key Topics
- Customer Account Protection

Referenced Rules & Notices
- FINRA Rule 4311
- FTC FACT Act
- NASD Rule 3012
- NYSE Rule 401
- Regulatory Notice 08-69
- Regulatory Notice 09-64

Executive Summary

FINRA has received an increasing number of reports of incidents of customer funds stolen as a result of instructions emailed to firms from customer email accounts that have been compromised. These incidents highlight some of the risks associated with accepting instructions to transmit or withdraw funds via email. FINRA recommends that firms reassess their policies and procedures to ensure they are adequate to protect customer assets from such risks. The Federal Bureau of Investigation (FBI), Financial Services Information Sharing and Analysis Center (FS-ISAC) and Internet Crime Complaint Center (I3C) recently released a joint fraud alert describing a similar trend.[1]

Questions concerning this *Notice* should be addressed to:

- Patricia Albrecht, Associate General Counsel, Office of General Counsel, at (202) 728-8026; or
- Terry H. Miller, Lead Sr. Regulatory Specialist, Member Regulation Department, at (202) 728-8159.

Background and Discussion

FINRA has received an increasing number of reports of incidents in which firms have wired customer funds to third-party accounts based on instructions received from customers' email accounts that had been compromised by third parties. In some instances, the perpetrators appear to have obtained customers' brokerage information by accessing customers' email accounts and searching contact lists or emails sent from the account. Typically, the perpetrators of these fraudulent schemes email brokerage firms from customers' personal email accounts with instructions to wire funds to an account, often overseas, controlled by the perpetrator. The instructions may be accompanied or followed by fraudulent letters of authorization also emailed from compromised email accounts. In some instances, firms have released funds after unsuccessfully attempting to verify emailed instructions by phone. In at least one case, the fraudulent email stressed the urgency of the requested transfer, pressuring the firm to release the funds before verifying the authenticity of the emailed instructions.

FINRA
Financial Industry Regulatory Authority

Policies and Procedures

NASD Rule 3012 (Supervisory Control System)[2] and Incorporated NYSE Rule 401 (Business Conduct) require all firms to establish, maintain and enforce written supervisory control policies and procedures that, among other things, include procedures that are reasonably designed to review and monitor the transmittal of funds (*e.g.*, wires or checks) or securities:

- from customer accounts to third-party accounts (*i.e.*, a transmittal that would result in a change of beneficial ownership);
- from customer accounts to outside entities (*e.g.*, banks, investment companies);
- from customer accounts to locations other than a customer's primary residence (*e.g.*, post office box, "in care of" accounts, alternate address); and
- between customers and registered representatives (including the hand-delivery of checks).

The policies and procedures a firm establishes under these rules must include "a means or method of customer confirmation, notification or follow up that can be documented."[3] NASD Rule 3012 further provides that a firm must identify in its written supervisory control procedures any of these activities in which it does not engage, and document that additional supervisory policies and procedures for such activities must be in place before the firm can engage in them.[4]

FINRA addressed the scope of these obligations in *Regulatory Notice 09-64*, which highlighted a number of questions firms should consider in assessing the adequacy of their policies and procedures for verifying the validity of requests to withdraw or transfer customer funds. Among other things, FINRA noted that firms should ensure that their procedures adequately address the specific risks associated with each method the firm allows for transmitting instructions.

One of the risks associated with accepting instructions to withdraw or transfer funds by email and other electronic means is that customers' email accounts are susceptible to being breached by hackers or other intruders who may use the email accounts to commit fraud. Therefore, FINRA recommends that firms reassess their policies and procedures for accepting instructions to withdraw or transfer funds via electronic means to ensure that they are adequately designed to protect customer accounts from the risk that customers' email accounts may be compromised and used to send fraudulent transmittal or withdrawal instructions. Among other things, FINRA recommends that such policies and procedures should:

- include a method for verifying that the email was in fact sent by the customer; and
- be designed to identify and respond to "red flags," including transfer requests that are out of the ordinary, requests that funds be transferred to an unfamiliar third party account,[5] or requests that indicate urgency or otherwise appear designed to deter verification of the transfer instructions.

As FINRA noted in *Regulatory Notice 09-64*, firms must train their employees to follow all applicable policies and procedures rigorously. Firms' policies and procedures should also include random sampling and testing of transfers and withdrawals to monitor for compliance.[6]

As noted in *Regulatory Notice 09-64*, the requirement that firms have supervisory procedures for reviewing and monitoring transfers of customer assets applies to both clearing and introducing firms. Further, FINRA Rule 4311(c) requires that when customer accounts are to be carried on a fully disclosed basis, the carrying agreement must specify the responsibilities of each party to the agreement, and while the rule permits firms to allocate responsibility for the performance of certain functions between the carrying and introducing firms, it expressly requires that the carrying firm be allocated the responsibility for the safeguarding of customer funds and securities. Both firms must have policies and procedures in place to ensure that their respective regulatory and contractual responsibilities are met. For example, the firms may agree that the introducing firm is responsible for verifying a customer's identity and that the instructions originated with the customer, in which case the introducing firm must have adequate policies and procedures to ensure that it effectively carries out this function.

However, the carrying firm must still have adequate policies and procedures to review and monitor all disbursements it makes from customers' accounts, including but not limited to third-party accounts, outside entities or an address other than the customer's primary address. A firm's procedures should also specify how instructions to withdraw or transmit assets may be conveyed, including which employees of the introducing firm are authorized to transmit instructions to the clearing firm on the customer's behalf, and both firms are responsible for ensuring that their employees follow their respective procedures.

Firms should also consider advising customers to notify the firm if a customer discovers that his or her email account has been compromised. Firms receiving such notification should have a method for ensuring that the information is communicated and used effectively within the firm to protect both the customer accounts and the firm.

Conclusion

Given the rise in incidents reported to FINRA involving fraud perpetrated through compromised customer email accounts, FINRA recommends that firms reassess their specific policies and procedures for accepting and verifying instructions to withdraw or transfer customer funds that are transmitted via email or other electronic means, as well as firms' overall policies and procedures in this area.

1. Fraud Alert Involving E-mail Intrusions to Facilitate Wire Transfers Overseas, January 20, 2012, at http://www.ic3.gov/media/2012/EmailFraudWireTransferAlert.pdf.

2. The current FINRA rulebook consists of (1) FINRA Rules; (2) NASD Rules; and (3) rules incorporated from NYSE (Incorporated NYSE Rules). While the NASD Rules generally apply to all FINRA member firms, the Incorporated NYSE Rules apply only to those member firms of FINRA that are also members of the NYSE (Dual Members). The FINRA Rules apply to all FINRA member firms, unless such rules have a more limited application by their terms. For more information about the rulebook consolidation process, *see Information Notice 3/12/08* (Rulebook Consolidation Process).

3. *See* NASD Rule 3012(a)(2(B) and Incorporated NYSE Rule 401(b) (requiring procedures as part of a firm's internal control requirements prescribed under Incorporated NYSE Rule 342.23).

4. *See* NASD Rule 3012(a)(2)(B). Incorporated NYSE Rule 401 does not have a comparable provision.

5. In this regard, firms might consider having customers indicate in writing parties to whom they might make transfers as a check against unfamiliar third party transfers.

6. Firms are also reminded that the Federal Trade Commission (FTC) and the federal banking regulators have issued joint regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). Among other things, the FTC's regulations, which apply to most member firms, require that financial institutions develop and implement a written program to detect, prevent and mitigate identity theft in connection with the opening of certain accounts or the maintenance of certain existing accounts (referred to as the Red Flags Rule). See Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 FR 63718 (November 9, 2007) (Joint Final Rules and Guidelines of the FTC, Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and National Credit Union Administration (NCUA)).See Pub. L. 108-159 (amending Section 615 of the Fair Credit Reporting Act of 1970 (FCRA) and adding new Section 605(h)(2)). For more information on the applicability of the FTC Red Flags Rule to FINRA member firms, see *Regulatory Notice 08-69* (November 2008).