Regulatory Notice 22-18

Digital Signatures

FINRA Reminds Firms of Their Obligation to Supervise for Digital Signature Forgery and Falsification

Summary

FINRA has received an increasing number of reports regarding registered representatives and associated persons (representatives) forging or falsifying customer signatures, and in some cases signatures of colleagues or supervisors, through third-party digital signature platforms. Firms have, for example, identified signature issues involving a wide range of forms, including account opening documents and updates, account activity letters, discretionary trading authorizations, wire instructions and internal firm documents related to the review of customer transactions.

These types of incidents underscore the need for member firms that allow digital signatures to have adequate controls to detect possible instances of signature forgery or falsification.

To help firms address the risks these signature forgeries and falsifications present, FINRA is sharing information in this *Notice* about:

- relevant regulatory obligations;
- forgery and falsification scenarios firms have reported to FINRA; and
- methods firms have used to identify those scenarios.

Questions concerning this *Notice* should be addressed to Steve Price, Senior Vice President, National Cause Program, at (303) 446-3125 or steven.price@finra.org.

Questions concerning rule requirements should be addressed to the Office of General Counsel at (202) 728-8071.

Background & Discussion

Regulatory Obligations

Signing someone else's name to a document violates FINRA rules when it is a forgery or falsification. Forgery occurs when one person signs or affixes, or causes to be signed or affixed, another person's name or initials on a document without the other person's prior permission.

August 3, 2022

Notice Type

- Special Alert

Suggested Routing

- Back Office
- Branch Inspections
- Branch Office Personnel
- Compliance
- Conduct
- Fraud Prevention
- Internal Investigations
- Legal
- Operations
- Risk
- Senior Management

Key Topics

- Books and Records
- Conduct
- Correspondence
- Customer Signature Forgery and Falsification
- Supervisory Systems and Controls

Referenced Rules & Notices

- FINRA Rule 2010
- FINRA Rule 3110
- FINRA Rule 4511
- Information Notice 10/15/20
- Regulatory Notice 09-64
- Regulatory Notice 14-10

Falsification occurs when a person creates a document or entry in a firm's system that creates a false appearance by including altered or untrue information. Forgery and falsification are violations of FINRA Rule 2010, which requires associated persons to observe high standards of commercial honor and just and equitable principles of trade in the conduct of their business.[1]

Where the forged or falsified document is a book or record the member firm maintains, the associated person also separately violates FINRA Rule 4511. FINRA Rule 4511 requires members to "make and preserve books and records as required under the FINRA rules, the Exchange Act and the applicable Exchange Act rules."[2] Inherent in the obligation to make and preserve books and records is the requirement that they be accurate.

In addition, FINRA Rule 3110(a) requires each member to establish and maintain a system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules. As noted above, FINRA Rule 2010 prohibits associated persons from forging or falsifying documents, and FINRA Rule 4511 requires members to make and preserve accurate books and records. A firm's duty of supervision also includes the responsibility to identify and respond to "red flags" or suspicious activity that suggest misconduct may be occurring.[3]

In *Regulatory Notice 09-64* (Verification of Instructions to Transmit or Withdraw Assets from Customer Accounts), FINRA reminded members that as part of their duty to safeguard customer assets and meet their supervisory obligations, member firms should periodically review and assess the adequacy of their supervisory systems and procedures, "which can become outdated or ineffective for a variety of reasons, including . . . new technologies[.]"[4]

Methods to Identify Digital Signature Forgery or Falsification

Below, we describe five scenarios member firms reported to FINRA in which representatives forged or falsified customer signatures, including the methods firms used to identify the forgeries or falsifications.

- **Customer Inquiries or Complaint Investigations**—In their investigations of customer inquiries or complaints, firms identified situations in which representatives forged or falsified customer signatures. For example, customers raised questions or complained about:
  - account transfers where firm investigations revealed that representatives facilitated the transfer process by digitally signing forms on behalf of customers; and

- securities transactions where firm investigations revealed that disclosure forms executed in connection with the transaction acknowledging a product's alignment with the customer's investment objective and risk tolerance had been forged.

Firms have identified similar signature issues involving a wide range of forms, including account opening documents and updates, account activity letters, discretionary trading authorizations, wire instructions and internal firm documents related to reviewing customer transactions.

- **Digital Signature Audit Trail Reviews**—Digital signature platforms generally store identifying information for each signatory on a document, including email address and Internet Protocol (IP) addresses from which the document was signed, as well as other information, in an audit trail or completion certificate. Firms reviewing this information identified red flags indicating that representatives may have been engaged in forgery or falsification. For example, firms identified instances where:
  - customer signatures originated from email addresses associated with their representative or other email addresses that were inconsistent with customer email addresses the firm maintained;
  - there was a discrepancy between the location of the user (*e.g.,* the individual affixing the customer's digital signature) and the customer's residence; or
  - the IP addresses for the representative and customer signatures on a document were the same.
- **Email Correspondence Reviews**—Firms' email reviews also identified situations where representatives had forged or falsified signatures. These reviews identified instances where correspondence showed that documents were sent to non-customer emails, including the representative's personal email address or that of their assistant, to a representative's firm-assigned email address, or an address associated with a representative's approved outside business activity. Such reviews may also enable a firm to identify instances where a customer's email address has been changed in ways that are indicative of attempts to conceal information from a customer. These instances may include, for example, a customer's email address that is changed to the representative's email address, or unrelated customers having the same email address.
- **Administrative Staff Inquiries**—In some cases, administrative staff raised questions to management or compliance after representatives directed them to manipulate the digital signature process in what the representatives claimed were acceptable accommodations to the customer. FINRA notes that training for administrative staff can help encourage them to resist pressure to manipulate signature processes and report concerns to appropriate firm staff.

- **Customer Authentication Supervision**—Firms sometimes use an authentication process when obtaining digital signatures that asks customers to answer one or more questions with personal information to verify their signature. In some instances, representatives have been able to circumvent the authentication process because the verification questions were based on personal information contained in customer files accessible to the representative. Because representatives often have access to customer information, firms relying solely on this verification process may miss red flags of potential forgery or falsification by representatives. Additionally, firms should ensure their procedures address safeguards around the authentication process and clearly indicate any restrictions on employee access to, for example, customer passwords and answers to verification questions.

Conclusion

The increasing use of digital documentation can significantly improve the ease and efficiency of customer interactions, but digital documentation also creates risks for customers and firms. The recent increase in reports to FINRA of digital forgery and falsification is one of those risks. The information provided in this *Notice* can help firms mitigate that risk and meet their regulatory obligations.

Endnotes

1. *See, e.g., Department of Enforcement v. Claggett,* Complaint No. 2005000631501, 2007 FINRA Discip. LEXIS 2 (NAC Sept. 28, 2007).
2. *See also* Rules 17a-3 and 17a-4 under the Securities Exchange Act of 1934.
3. *See, e.g., Regulatory Notice 09-64* (Verification of Instructions to Transmit or Withdraw Assets from Customer Accounts) (stating that a firm's policies and procedures should include procedures that are reasonably designed to, among other things, identify and respond to red flags or suspicious activity).
4. *Regulatory Notice 09-64*, at 1–3. When FINRA issued *Regulatory Notice 09-64*, NASD Rule 3012 was the relevant operative rule. Effective December 1, 2014, NASD Rule 3012's requirements regarding the review and monitoring of transmittals of funds and securities, among other things, were relocated to FINRA Rule 3110(c)(2). *See Regulatory Notice 14-10* (SEC Approves New Supervision Rules). *See also Information Notice 10/15/20* (Cybersecurity Background: Authentication Methods) for additional information about authentication.