The text below is an excerpt from the ICI Mutual risk management study *Shareholder Authentication: Managing the Risk of Fraudulent Transactions.* The full study may be accessed at www.icimutual.com/ShareholderAuthentication.

Potential Legal Consequences of Transactional Fraud

Transactional fraud may have significant adverse consequences for affected fund groups, including legal damage in the form of regulatory scrutiny and/or private litigation.

Over the years, regulators have focused increased attention on authentication, among other cyber issues. As early as 2005, the Federal Financial Institutions Examination Council issued its *Guidance on Authentication in Internet Banking Environment*, (later supplemented in 2011).[1]

Securities regulators have also become more active in this area.[2] In April 2014, the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued a risk alert describing its cybersecurity examination initiative, which included a cybersecurity questionnaire for broker-dealers and registered investment advisers. One section of this questionnaire specifically focused on the authentication of customers.[3] While OCIE's questionnaire was not specifically directed at the fund industry, fund groups may find it helpful to consider the authentication-related questions both as guidance in this area and as an indication of OCIE's examination priorities.

The SEC's Cybersecurity Sweep

In April 2014, the SEC's Office of Compliance Inspections and Examinations issued, as part of a risk alert describing its cybersecurity examination initiative, a questionnaire seeking information from broker-dealers and registered investment advisers about various practices. With respect to online transactions, the questionnaire inquired about the following:

- Are customers provided with online account access? If so, the OCIE questionnaire sought additional information, including:
  - The name of any third party or parties that manage the service.
  - The functionality for customers on the platform (e.g., balance inquiries, address and contact information changes, beneficiary changes, transfers among the customer's accounts, withdrawals or other external transfers of funds).
  - How customers are authenticated for online account access and transactions.
  - Any software or other practice employed for detecting anomalous transaction requests that may be the result of compromised customer account access.
  - A description of any security measures used to protect customer PINs stored on the sites.
  - Any information given to customers about reducing cybersecurity risks in conducting transactions/business.
- How is the authenticity of email requests seeking to transfer customer funds verified?
- Are there policies for addressing responsibility for losses associated with attacks or intrusions impacting customers?
- Are customers offered a security guarantee to protect them against hacking of their accounts?

SEC, OCIE, National Exam Program Risk Alert: OCIE Cybersecurity Initiative (Apr. 15, 2014), http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

In February 2015, OCIE provided summary observations from its cybersecurity examination initiative. With respect to authentication issues, OCIE found that approximately half of the firms examined had received fraudulent e-mails seeking to transfer funds, and that some of those e-mails resulted in losses.[4]

In September 2015, OCIE issued a risk alert announcing a second round of cybersecurity examinations of investment advisers and broker-dealers. OCIE enumerates six areas of focus, including access rights and controls.[5] The risk alert includes a sample document request list, which requests, among other things, information on the use of multi-factor authentication for customer access, and on policies and procedures related to verifying the authentication of customer requests to transfer funds.[6]

In a proceeding outside the fund industry, the SEC sanctioned an investment adviser for failure to properly authenticate transfer requests that were sent by e-mail. In this proceeding, a fraudster had hacked into an advisory client's e-mail account and had sent e-mails requesting fund transfers to a foreign bank. Because the fraudster purportedly needed the funds immediately but had no access to a telephone, the investment adviser sent transfer instructions to its clearing firm, using a photocopy of the client's signature on file. The SEC found, among other things, that the investment adviser had no "procedures in place to confirm the authenticity of transfer requests made by e-mail."[7]

In discussing shareholder authentication, this study chiefly focuses on the steps taken by fund groups to confirm the identity of *existing* shareholders who seek to access and transact in their accounts. It should be noted, however, that in initial account openings, fund groups take steps—and indeed are required to take steps—to verify the identity of persons seeking to open accounts. In this regard, the SEC (together with the Treasury Department through the Financial Crimes Enforcement Network) has issued rules regarding customer identification programs for mutual funds, and has specified the information that should be collected to verify identities. This information includes, at a minimum, a customer's name, date of birth, address, and identification number (e.g., a Social Security number).[8]

Endnotes

[1] *See* FFIEC, Authentication in an Internet Banking Environment (Oct. 12, 2005), http://www.ffiec.gov/pdf/authentication_guidance.pdf; FFIEC, Supplement to Authentication in an Internet Banking Environment, note 1 (June 22, 2011), https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20%28FFIEC%20Formated%29.pdf.

[2] FINRA has focused on customer authentication issues. *See, e.g.*, FINRA, Customer Account Protection: Verification of Emailed Instructions to Transmit or Withdraw Assets from Customer Accounts (Jan. 2012), http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p125462.pdf; Comment Letter from Marcia E. Asquith, SVP and Corp. Sec'y, FINRA, to Nancy M. Morris, Sec'y, SEC (May 12, 2008), http://www.sec.gov/comments/s7-06-08/s70608-54.pdf (expressing FINRA's support for using risk-based standards for safeguarding customer information).

[3] *See* SEC, OCIE, National Exam Program Risk Alert: OCIE Cybersecurity Initiative (Apr. 15, 2014), http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.

[4] SEC, OCIE, National Exam Program Risk Alert: Cybersecurity Examination Sweep Summary (Feb. 3, 2015), http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

[5] *See* SEC, OCIE, National Exam Program Risk Alert: OCIE's 2015 Cybersecurity Examination Initiative (Sept. 15, 2015), www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf. OCIE advised that it would also focus on the following areas in addition to access rights and controls: (1) governance and risk assessment, (2) data loss prevention, (3) vendor management, (4) training, and (5) incident response. *Id.* at pp. 2-3.

[6] *See id.*, Appendix, p. 3.

[7] *See* In the Matter of GW & Wade, LLC, Advisers Act Rel. No. 3706 (Oct. 28, 2013), https://www.sec.gov/litigation/admin/2013/ia-3706.pdf.

[8] *See* SEC, Dep't of the Treasury, and Financial Crimes Enforcement Network, Joint Final Rule: Customer Identification Programs for Mutual Funds, 40 Act Rel. No. 26031 (Apr. 29, 2003), https://www.sec.gov/rules/final/ic-26031.htm.