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.

Overall Threat Environment

Financial institutions (including fund groups) are potentially subject to an array of cyber-related threats from a variety of actors, including hackers, identity thieves, state-sponsored actors, and organized crime groups. But not all of these actors present the same threat level with respect to authentication issues. For fund groups concerned with the potential for transactional fraud, one significant threat is from identity thieves who, acting alone or with the assistance of larger groups, may target fund shareholders. For financial institutions more generally, concerns have also been voiced about other actors, including organized crime groups, who may mount broader attacks that exploit vulnerabilities in authentication systems.[1]

The threat environment for fund groups has changed not only as a result of the emergence of malevolent external actors, but also for more benign reasons. The continued evolution in the nature and scope of shareholder services, and in the channels of communication used by shareholders, may increase or otherwise alter fund groups' risk exposures with respect to authentication issues. For example, some fund groups have expanded the range of shareholder services that they provide online or over the phone and/or have expanded available channels of communication (e.g., through the development of mobile apps). Meanwhile, shareholder behavior continues to shift, as shareholders increasingly adopt online access, use mobile apps, and move toward omnibus accounts.

Changes in the Threat Environment

- Fraudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication mechanisms and to gain unauthorized access to customers' online accounts.
- Rapidly growing organized criminal groups have become more specialized in financial fraud and have been successful in compromising an increasing array of controls.
- Malware can compromise some of the most robust online authentication techniques, including some forms of multi-factor authentication.

FFIEC, Supplement to Authentication in an Internet Banking Environment (June 29, 2011), http://www.ffiec.gov/pdf/authentication_guidance.pdf.

These general changes in the threat environment highlight the need for fund groups to engage in periodic re-assessments of the risks they face with regard to shareholder authentication. Periodic re-assessments may also be warranted by specific events. For example, a vulnerability exposed in 2014—the "Heartbleed" flaw in Internet encryption—caused some fund groups to focus immediate attention on designated authentication issues. According to press reports and fund group websites, at least one fund group at that time advised its customers to change their

About ICI Mutual: ICI Mutual is the predominant provider of D&O/E&O liability insurance and fidelity bonding for the U.S. mutual fund industry. Its insureds represent more than 60% of the industry's managed assets. As the mutual fund industry's dedicated insurance company, ICI Mutual is owned and operated by and for its insureds.

© 2015 ICI Mutual Insurance Company, RRG

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.

potentially compromised passwords and to take other steps to protect their accounts,[2] while a number of fund groups thought it appropriate to advise that their websites and services were not affected by Heartbleed.[3]

Endnotes

[1] *See, e.g.,* FFIEC, Supplement to Authentication in an Internet Banking Environment (June 22, 2011), https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20%28FFIEC%20Formated%29.pdf (describing changes in the threat landscape since 2005).

[2] *See* American Funds urges password change to counter 'Heartbleed' bug, Reuters.com (Apr. 16, 2014), http://www.reuters.com/article/2014/04/16/cybersecurity-heartbleed-funds-idUSL2N0N81DC20140416 (reporting that one fund group was advising shareholders to change their passwords and security questions and to delete their browsing history and cookies in the wake of the disclosure of the Heartbleed bug); Joe Morris, American Funds Warns of Heartbleed Risk, Ignites.com (Apr. 17, 2014), http://ignites.com/c/860784/77724.

[3] *See, e.g.*, Fidelity: Sites Safe from Heartbleed Bug, Ignites.com (Apr. 10, 2014), http://ignites.com/c/857834/77314.

About ICI Mutual: ICI Mutual is the predominant provider of D&O/E&O liability insurance and fidelity bonding for the U.S. mutual fund industry. Its insureds represent more than 60% of the industry's managed assets. As the mutual fund industry's dedicated insurance company, ICI Mutual is owned and operated by and for its insureds.

© 2015 ICI Mutual Insurance Company, RRG Information current as of September 2015