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.

Glossary

Behavioral Biometrics: The use of a learned or acquired (as opposed to a biological) characteristic to identify a user. Examples include how an individual types, moves a mouse, or uses gestures on a smartphone.

Biological Biometrics: The use of an anatomical or physiological (as opposed to a behavioral) characteristic to identify a user. Examples include an individual's fingerprint, iris or retinal pattern, or heartbeat.

Biometrics: Broadly, the use of a biological or behavioral characteristic to identify a user.

Cookie: A file stored by a website on a user's computer, typically containing information about the user (e.g., username, preferences regarding the website, registration information), the user's computer (e.g., information about the computer's browser, location, or configuration), and/or information about the user's interaction with the website (e.g., information regarding previous transactions, such as login times or pages viewed).

Device Fingerprinting: The creation of a profile of a user's computer, smartphone, or other device, based on information compiled about the device. Examples include a device's location, IP address, screen resolution, operating system, installed software, attached hardware, or other information about the device's configuration.

Enhanced Authentication: The use of multiple measures relying on what a user knows (e.g., a password plus a "shared secret," such as the user's mother's maiden name).

Equal Error Rate: The rate at which the false acceptance rate and the false rejection rate are equal.

Error-Rate Tradeoff: The proposition that, as the false acceptance rate rises, the false rejection rates tends to fall, and vice versa.

False Acceptance Rate: The rate at which an authentication mechanism incorrectly permits an *unauthorized* person to gain access to a protected system.

False Rejection Rate: The rate at which an authentication mechanism incorrectly prevents an *authorized* person from gaining access to a protected system.

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.

Geolocation: The determination of a user's geographical location (e.g., based on information provided by the user's mobile phone or other device).

Hardware Token: A small electronic device that, at regular intervals (e.g., every 30 seconds), generates a number or a code that a user must enter to complete the authentication process.

Internet Protocol (IP) Address: A set of numbers or hexadecimal values assigned to each device connected to the Internet or other network.

Knowledge-Based Authentication: A form of single-factor authentication in which a user is asked to answer questions to which he or she is particularly likely to know the answers, such as financial questions about the user's monthly mortgage payment or credit card account, or "shared secrets" about a user's personal life (e.g., the user's first car, childhood pet, or mother's maiden name) that are provided in advance by the user. Sometimes referred to as "challenge-response" authentication.

Malware: **Mal**icious soft**ware** that is harmful to a computer, smartphone, or other device. Malware include computer viruses, worms, spyware, and Trojans.

Man-in-the-Middle Attack: An attack in which a fraudster intercepts—and alters—communications between two parties who believe that they are communicating directly and only with each other.

Multi-Factor Authentication: The use of a combination of what a user *knows* and any additional authentication factor (whether it pertains to what a user *has* or what a user *is*).

Mutual Authentication: In this context, the steps taken by fund groups to ensure that shareholders and/or their devices are able to confirm the identity and validity of the shareholders' online connections to the fund groups. These steps may include the use of digital certificates or the use of security images.

Negative Authentication: The use of measures chiefly intended to establish the identity of the person seeking to effect a transaction *as somebody other than the shareholder*.

Out-of-Band Communication: The use of an additional channel of communication to verify a user's identity. Examples include contacting an online user by telephone, e-mail, or text message to verify the user's identity and intent to engage in the online transaction at issue.

Phishing: A form of e-mail fraud in which a fraudster posing as a legitimate company requests confidential information from a broad range of individuals. Compare with "spear phishing."

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.

Positive Authentication: The use of measures chiefly intended to establish identity of the person seeking to effect a transaction *as the shareholder*.

Salting and Hashing: The process of adding complexity and uniqueness to a user's password, which is accomplished by adding characters to, or "salting," the password, then using a "hashing" algorithm (e.g., SHA-512 or bcrypt) that generates a long, unique string of characters and that is designed to be irreversible.

Sidejacking Attack: An attack in which a fraudster copies a cookie that has been placed on a user's computer by a website, and subsequently uses that cookie to impersonate the user (and to fool the website into treating the fraudster as the user). If the cookie indicates that the user's identity has been properly authenticated by the website, the fraudster may be able to circumvent the website's authentication procedures.

Single-Factor Authentication: The use of what a user *knows* (e.g., a password).

Software Token: A mobile phone app or similar program that performs the function of a hardware token—i.e., generates, at regular intervals (e.g., every 30 seconds), a number or code that a user must enter to complete the authentication process.

Spear Phishing: A form of phishing e-mail fraud in which the fraudster specifically targets particular individuals. Compare with "phishing."

Spoofing: In this context, "spoofing" refers to a fraudster's falsification of device characteristics in order to fool a fund group. Examples include "spoofing" the Caller ID of a legitimate shareholder, or the IP address of a legitimate shareholder's computer or other device.

Trojan (or Trojan Horses): A type of malware that appears to the user to be benign or useful.

Two-Factor Authentication: The use of a combination of what a user *knows* and what a user *has* (e.g., a hardware token).

Information current as of September 2015