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.

Protection of Online Transaction Systems

Fund groups typically take strong steps to ensure that online transaction systems are protected, both from external and internal threats, through appropriate network security measures. Moreover, these online transaction systems are generally segregated from other computer systems through the use of firewalls and/or DMZs (i.e., firewall-protected servers that are set up in the "demilitarized zone" outside the perimeter of a corporate network). A full discussion of relevant network security measures for online transaction systems is beyond the scope of this study, but has been described in greater detail in ICI Mutual's prior risk management studies on computer security, identity theft, and digital age risks.

Fund groups also take steps to protect authentication-related information that is stored on online transaction systems. While storing passwords in plain text creates an obvious vulnerability, merely encrypting them, as was the case in Adobe's 2013 data breach (in which over 150 million records were breached), still leaves a significant vulnerability.[1] (Because encryption is designed to be a reversible operation, a fraudster obtaining a list of encrypted passwords would likely be able to recover at least some of those passwords.) To address this vulnerability, fund groups tend to store passwords that have been "salted" (i.e., additional characters are added to the passwords) and then "hashed" with an algorithm that is designed to be irreversible. Salting and hashing passwords (preferably with a *slow* hashing algorithm, thus increasing the amount of

Encrypting, Hashing, and Salting Passwords

Encryption: Because encryption is a reversible process, a fraudster would likely be able to recover at least some, and potentially a large number, of encrypted passwords.

Username	Password	Encrypted with 128-Bit AES Algorithm
User1	123456	Tx60TU3mrn6X04AO5TcPHw==
User2	123455	S3ii5cHwxVhjoVGQgXaAog==

Hashing (without salt): Because hashing is designed to be irreversible, it is extremely difficult to compute a password from the hashed value. However, if multiple users have the same password, the hashed result will be the same, as is the case for User1 and User2 in the chart below. Despite the computational hurdle, a fraudster is likely to be able to recover a number of hashed passwords by various means (e.g., brute force attacks, dictionary attacks, use of rainbow tables).

Username	Password	Hashed with SHA-256
User1	123456	8d969eef6ecad3c29a3a629280e686cf0c3f5d5a 86aff3ca12020c923adc6c92
User2	123456	8d969eef6ecad3c29a3a629280e686cf0c3f5d5a 86aff3ca12020c923adc6c92
User3	123455	fc1f09ab08ebdd072ea6da53a5691abcc18c916 3b1be1f0921a5adb50e3f5077

Hashing (with salt): "Salting" each user's password, preferably with randomly generated characters for each user, ensures that, even if multiple users have the same password, the hashed results of the salted passwords will be different. A fraudster will have a very difficult time recovering salted and hashed passwords.

Username	Password + Salt	Hashed with SHA-256
User1	123456 + Xk35@!	2d24fa96930a634ca0cda021c6db29d1423b68b30fe 3a75fc265cf62fb95ab78
User2	123456 + Jy12%$	89b8d3e8e1ea8c62b23f609cc139ccc64236cc4b633 515d58c3a4225f56e4ce1
User3	123455 + Xz52!#	d148610398d1dbd831ae8d87ea44f6f028a00a44c79 708b0811d31a3849436a3

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.

time needed for a successful brute force attack) makes it significantly more difficult for a fraudster to recover passwords.[2]

Endnotes

[1] *See* Steve Ragan, *Adobe confirms stolen passwords were encrypted, not hashed*, CSOONLINE.COM (Nov. 4, 2013), http://www.csoonline.com/article/2134124/network-security/adobe-confirms-stolen-passwords-were-encrypted-not-hashed.html; Alex Hern, *Did your Adobe password leak? Now you and 150m others can check*, THE GUARDIAN (Nov. 7, 2013), http://www.theguardian.com/technology/2013/nov/07/adobe-password-leak-can-check.

[2] *Storing Passwords - The Wrong, Better and Even Better Way*, WEBLINKS (June 21, 2009), https://wblinks.com/notes/storing-passwords-the-wrong-better-and-even-better-way/.