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.

Limitations of Authentication Measures in Common Use

For various reasons, some authentication measures in common use by fund groups may have become less effective over time. For example, the username/password combination commonly used to authenticate shareholders may not offer the same degree of protection against fraud as it has in the past. Usernames, in and of themselves, are of limited value in authenticating users, and, as algorithms have become more sophisticated and computers have become more powerful, fraudsters continue to make significant advancements in cracking passwords. Indeed, tools for cracking passwords are readily available to the public, and require relatively modest equipment and little, if any, expertise.[1] A recent report found that passwords as long as 55 characters could be cracked with relative ease.[2]

Account Lockout Requirements

Fund groups typically lock out shareholders from their shareholder accounts after a given number of failed login attempts. In order to reset locked accounts, shareholders generally are required to call their fund group and to provide sufficient identifying information. For some fund groups, online account resets may also be permitted.

While account lockout requirements offer some protection against a fraudster who is sitting at a computer trying to guess passwords for a small number of accounts, such lockout requirements can be less effective against "password crackers," who tend to work offline on a database of passwords.[3]

In any event, the strength of a password is irrelevant if the fraudster simply steals or otherwise obtains a user's password. Passwords may be obtained in a variety of ways, including through phishing attempts (e.g., e-mails that seek to trick users into entering personal information on fraudulent websites) and through malware that logs keystrokes (including passwords) and relays the information back to the fraudster.[4]

Each passing year brings new data breaches involving a range of businesses, often involving the loss of usernames and passwords, as well as of customer personal information and/or financial information. As a result of a series of data breaches, or even a single data breach, fraudsters may gain sufficient information about a particular user to compromise the user's accounts at other organizations that were *not* subject to the breaches. The fraudsters' task may be simplified by the common predilection of many users to re-use the same or similar passwords at multiple websites.[5]

The information underlying knowledge-based authentication questions (e.g., a user's mother's maiden name or the name of a childhood pet) may also be lost or misappropriated in large-scale data breaches or may be obtained through hacking.[6] Moreover, with respect to certain questions, a fraudster may, even in the absence of a data breach or a hacking incident, obtain

sufficient information to compromise a user's account. Indeed, the user himself or herself, perhaps with the assistance of family and friends, may voluntarily divulge much of this information. The ubiquity of social media tends to undermine the value of certain questions, such as the shareholder's mother's maiden name or the name of a childhood pet.[7]

Endnotes

[1] *See* Dan Goodin, *Anatomy of a hack: How crackers ransack passwords like "qeadzcwrsfxv1331"*, ArsTechnica.com (May 26, 2013), http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/ (describing how an editor of a technology website used a password cracking program to decipher nearly half of over 16,000 passwords in a few hours, while expert password cracker deciphered up to 90% of the same passwords in less than a day).

[2] *See* Somini Sengupta, Machines Made to Know You, by Touch, Voice, Even by Heart, Bits Blog, NEW YORK TIMES (Sept. 10, 2013), http://bits.blogs.nytimes.com/2013/09/10/beyond-passwords-new-tools-to-identify-humans/.

[3] *See, e.g.*, Bob Covello, Why the password hackers never trigger an account lockout, GrahamCluley (Aug. 3, 2015), https://grahamcluley.com/2015/08/password-account-lockout/.

[4] *See* Neil J. Rubenking, Microsoft: Changing Passwords Isn't Worth the Effort, PC MAGAZINE (Apr. 15, 2010), http://www.pcmag.com/article2/0,2817,2362692,00.asp.

[5] *See* Graham Cluley, *55% of net users use the same password for most, if not all, websites. When will they learn?*, NakedSecurity.Sophos.com (April 23, 2013), https://nakedsecurity.sophos.com/2013/04/23/users-same-password-most-websites/ (citing a poll showing that over half of Internet users use the same password for most, if not all, websites).

[6] *See* David Lott, *Is Knowledge-Based Authentication Still Effective?*, Retail Payments Risk Forum, Federal Reserve Bank of Atlanta (Oct. 21, 2013), http://portalsandrails.frbatlanta.org/2013/10/is-knowledge-based-authentication-still-effective.html (describing an identity theft service that had hacked into some of the country's largest aggregators of consumer and business information, and then sold the information online).

[7] *See, e.g.*, Gasan Awad, Move Past Secrets to Real Identity Verification (Nov. 12, 2014), http://insight.equifax.com/move-past-secrets/ ("Now, with the proliferation of social networks, genealogy sites, blogs, and other ways for people to disclose more personal information about themselves in more different contexts, there are many fewer secrets than there used to be.").