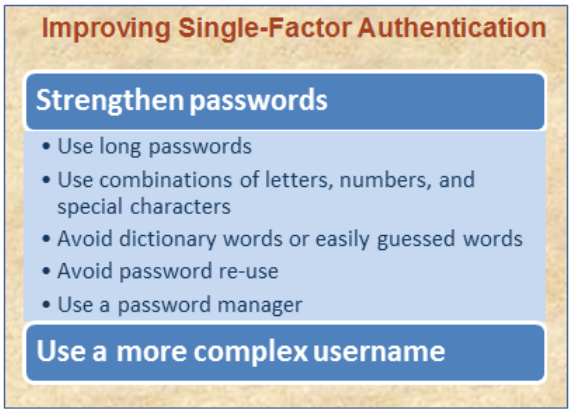
The text below is an excerpt from the ICI Mutual risk management study *Shareholder Authentication: Managing the Risk of Fraudulent Transactions.* The full study may be accessed at www.icimutual.com/ShareholderAuthentication.

Shareholder Knowledge

In authenticating the individual involved in a shareholder transaction, fund groups have typically employed single-factor authentication measures (i.e., measures based on what the shareholder *knows*). The "knowledge" requested by fund groups from shareholders may differ depending on whether transactions are being conducted over the telephone or online.

For *telephone transactions*, most fund groups consulted for this study often authenticate shareholders based on their knowledge of multiple items of information. The information requested typically includes some combination of the following: the name(s) of the shareholder(s), the shareholder's account number at the fund group, the shareholder's bank account number, and/or other personal information (e.g., address, mother's maiden name, Social Security number, or personal identification number (PIN)). Under some circumstances (based, for example, on recent fund activity or the amount of a transaction), a fund group might require a shareholder to provide additional documentation (e.g., a signature guarantee or a notarized signature) before processing a telephone transaction.

For *online transactions*, requiring users to enter usernames and passwords appears to be near-universal in the fund industry. Fund groups typically impose password complexity requirements (e.g., mandating minimum password lengths and/or the use of a combination of uppercase and lowercase letters, numbers, and special characters). At least one fund group consulted for this study also subjects the *username* to similar complexity requirements on the theory that shareholder usernames might be easily guessed, particularly if used on multiple sites. As one security expert has observed, with an obvious username, "you're giving hackers half the battle."[1]

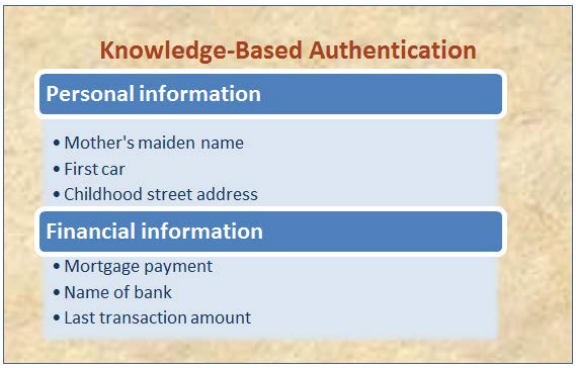


Other password-related requirements (such as those relating to the frequency of password changes or the re-use of old passwords) are commonly employed for internal computer systems *within* fund groups, but, perhaps to minimize shareholder inconvenience, do not appear to be as commonly required of shareholders. In any event, as some experts have suggested, requiring customers of financial institutions to periodically change their passwords arguably serves little purpose because fraudsters who gain access to account passwords are likely to use them very shortly thereafter.[2]

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.

Fund groups typically lock shareholders out of 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.

In addition to the username/password combination, a number of fund groups use forms of KBA (or knowledge-based authentication) under designated circumstances, such as if a shareholder attempts to log in from a different device (or even through a different browser on the same device). The requisite KBA may take the form of "shared secrets" (i.e., shareholder responses to pre-determined questions) or financial questions (e.g., about the shareholder's mortgage payment). Fund groups may verify the accuracy of shareholder answers to the latter type of questions with third-party service providers that have access to various sources of information (e.g., credit bureaus) about shareholders.



Endnotes

[1] *See* Paul Sullivan, Keeping Swindlers Out of Your Bank and Brokerage Accounts, NEW YORK TIMES (Feb. 7, 2014), http://www.nytimes.com/2014/02/08/your-money/keeping-swindlers-out-of-your-bank-and-brokerage-accounts.html.

[2] *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 ("A hacker who steals your password is going to use it right away; he won't wait two months."); Bruce Schneier, Changing Passwords, Schneier on Security (Nov. 2010), https://www.schneier.com/blog/archives/2010/11/changing_passwo.html.