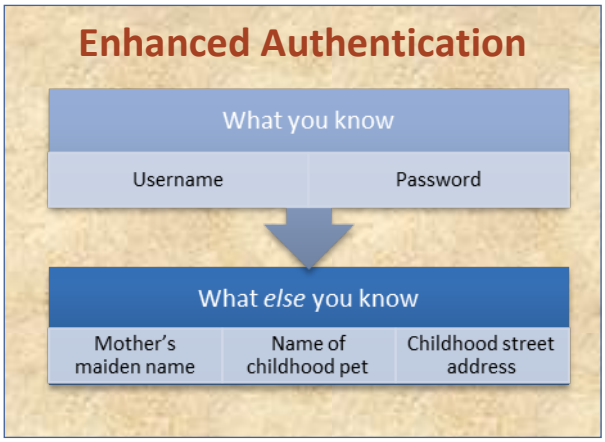
The text below is an excerpt from the ICI Mutual risk management study *Shareholder Authentication: Managing the Risk of Fraudulent Transactions.* The full study may be accessed at www.icimutual.com/ShareholderAuthentication.

The First Authentication Factor: What You Know

Reliance solely on the first traditional authentication factor, "what you know," is often referred to as single-factor authentication, and most commonly requires the user to provide a username and password. In and of itself, the username has limited value in authenticating a user; rather, it serves to identify which user is being presented to a company for authentication. The password is then used to authenticate that user's identity.

To enhance the effectiveness of the username/password combination, account lockout requirements (i.e., locking out a user from an account after a given number of failed login attempts) and/or password complexity requirements (e.g., minimum password lengths or the use of a combination of uppercase and lowercase letters, numbers, and special characters) are frequently employed and enforced. Such requirements seek to strike a balance between password strength and user convenience. In the absence of complexity requirements, users employing self-selected passwords may gravitate toward weak passwords (with "password" and "123456" being among the most common in 2014[1]). In contrast to user-selected passwords, automatically generated passwords are likely to have significantly greater "entropy" (i.e., the password is more random) and therefore afford stronger protection.[2] Even so, requiring more complex passwords can sometimes be counterproductive—if passwords are too complex and/or are not self-selected by users, users tend to have difficulty remembering them, and, as a result, may resort to writing their passwords down and leaving them in plain sight.

Single-factor authentication is not limited to the username/password combination. Enhanced authentication still relies on what a user knows, but includes other measures requiring the user to demonstrate additional knowledge, beyond the username/password, personal to that shareholder. Such additional measures, sometimes referred to as knowledge-based authentication (or "challenge-response") often require a user to answer additional questions,



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.

which may include financial questions (such as the user's monthly mortgage payment, credit card issuer, or the like) or "shared secrets" about a user's personal life (e.g., the model of the user's first car, name of childhood pet, mother's maiden name) that are provided in advance by the user.

Strictly speaking, the use of more than one single-factor authentication measure may be viewed as enhanced authentication, but not as true multi-factor authentication.[3]

Endnotes

[1] *See* Jordan Crook, This List Of 2014's Worst Passwords, Including '123456,' Is Embarrassing, TECHCRUNCH (Jan. 20, 2015), http://techcrunch.com/2015/01/20/this-list-of-2014s-worst-passwords-including-123456-is-embarrassing/; *see also* Chenda Ngak, The 25 most common passwords of 2013, CBSNews.com (Jan. 21, 2014), http://www.cbsnews.com/news/the-25-most-common-passwords-of-2013/.

[2] *See, e.g.*, NIST, DEP'T OF COMMERCE, SPECIAL PUBL'N NO. 800-63-2, GUIDE TO ENTERPRISE PASSWORD MANAGEMENT (DRAFT) 3-8 (Aug. 2009), http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf [hereinafter NIST Password Management] ("It is generally unrealistic to expect users to memorize [long, automatically generated] passwords. For passwords that are intended to be memorized, organizations should consider security needs and expected user behavior when deciding which password generation method should be used.").

[3] *See* Internal Revenue Service, Dep't of the Treasury, Safeguards Technical Assistance Memorandum: Multi-factor Authentication Implementation (June 2013), http://www.irs.gov/file_source/pub/irs-utl/safeguards-multi-factor-auth-alert.doc ("One type of authentication may not be repeated in attempting to satisfy multi-factor authentication. For example, authenticating using two passwords does not constitute multi-factor. They are both part of 'Something you know' and can both only satisfy this category.").