



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](http://www.icimutual.com/ShareholderAuthentication).

### Multi-Factor Authentication

Recent hacking incidents and data breaches have fueled increased concerns over security, and it has become increasingly common for non-financial organizations (such as e-mail providers and social media sites) to provide users with the option of using multi-factor authentication (i.e., the use of a combination of the first factor and one or both of the other two factors).<sup>1</sup> Multi-factor authentication is not foolproof, but can significantly enhance security.<sup>2</sup> As often implemented, multi-factor authentication requires a user to provide a username/password and a separate code (which may be provided by text message or by a hardware token or software token). Some financial institutions, including some banks,<sup>3</sup> broker-dealers,<sup>4</sup> and fund groups, now offer multi-factor authentication to at least some of their retail customers.

The use of multi-factor authentication measures by financial institutions and other organizations is likely to become more prevalent in the coming years. Adoption of multi-factor authentication has been slowed by, among other things, concerns over the costs of implementation and customer acceptance. These concerns may diminish over time, as implementation costs continue to fall and as the general public becomes more willing to accept the inherent tradeoffs between added inconvenience and greater security.

---

#### Endnotes

<sup>1</sup> The website, <https://twofactorauth.org/>, provides an updated list of websites and online services that support two-factor authentication. As of early 2015, sites and services offering two-factor authentication included Google (<http://www.google.com/landing/2step/>), Microsoft (<http://windows.microsoft.com/en-us/windows/two-step-verification-faq>), Apple ID (<http://support.apple.com/kb/ht5570>), Facebook ([https://www.facebook.com/note.php?note\\_id=10150172618258920](https://www.facebook.com/note.php?note_id=10150172618258920)), LinkedIn (<http://blog.linkedin.com/2013/05/31/protecting-your-linkedin-account-with-two-step-verification/>), Twitter (<https://blog.twitter.com/2013/getting-started-with-login-verification>), PayPal ([https://www.paypal.com/us/cgi-bin?cmd=xpt/Marketing\\_CommandDriven/securitycenter/PayPalSecurityKey-outside&bn\\_r=o](https://www.paypal.com/us/cgi-bin?cmd=xpt/Marketing_CommandDriven/securitycenter/PayPalSecurityKey-outside&bn_r=o)), and Evernote (<http://blog.evernote.com/blog/2013/10/04/two-step-verification-available-to-all-users/>).

<sup>2</sup> See NIST, Electronic Authentication: Guidance For Selecting Secure Techniques, <http://www.itl.nist.gov/lab/bulletns/bltnaug04.htm>.

<sup>3</sup> See Stephen Northcutt, SANS Inst. Security Laboratory, *Two factor authentication for online banking* (2014), <http://www.sans.edu/research/security-laboratory/article/2factor-banks>.

<sup>4</sup> See Schwab website, <http://workplace.schwab.com/public/workplace/nn/legal-compliance/schwabsafe/we-guard-your-account> (last visited September 28, 2014); E-trade website, <https://us.etrade.com/e/t/user/secureid-enter> (last visited July 7, 2014).

---

**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.