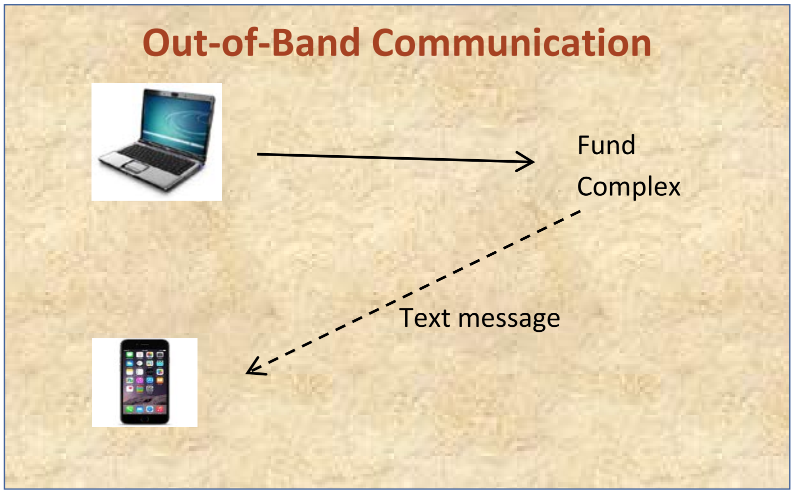
The text below is an excerpt from the ICI Mutual Study risk management study *Shareholder Authentication: Managing the Risk of Fraudulent Transactions.* The full study may be accessed at www.icimutual.com/ShareholderAuthentication.

The Second Authentication Factor: What You Have

Transactional security can be enhanced by employment of a second authentication factor, “what you have.” This authentication factor is typically deployed in conjunction with the first authentication factor (i.e., two-factor authentication), such that a user must typically establish his or her identity both by using a username/password (what the user knows) and by confirming his or her identity through use of an object (what the user has). This second authentication factor may be implemented through a variety of measures, including use of hardware tokens (small electronic devices) that generate a number that a user must enter to complete the authentication process. As typically implemented, the number provided by a hardware token expires after a given period (e.g., 30 seconds or a minute) and is replaced by a new number. Even if a fraudster has obtained a user’s username and password, the fraudster will generally be unable to access the user’s account without also having obtained the user’s hardware token. More recently, software tokens (e.g., apps for smartphones and other mobile devices that generate a number for the user to enter) may take the place of dedicated hardware tokens.

Mobile devices may also be used to implement two-factor authentication over separate communication channels, or out-of-band communications. For example, because most mobile phones permit text messaging, financial institutions can utilize out-of-band communications—such as text messages containing numbers, one-time passwords, or details of a transaction—to their online customers, either as part of the initial authentication process or as confirmation of a particular transaction request. Customers, in turn, may be required to enter these numbers or one-time passwords, or to confirm the texted details of the transaction.[1]


Out-of-Band Communication

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.

© 2015 ICI Mutual Insurance Company, RRG

Information current as of September 2015

ICIMutual
The safest decision you can make.

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

Experts believe that the use of two separate channels of communication provides significant additional security over the use of a single channel.[2]

Endnotes

[1] *See* Scott Perry, *Addressing Advanced Fraud Threats in Today's Mobile Environment*, Entrust (Apr. 2011), *available at* http://docs.media.bitpipe.com/io_10x/io_105707/item_558837/WP_MobileSecurity_June2012.pdf.

[2] *See id.*; *see also* FFIEC, Supplement to Authentication in an Internet Banking Environment (June 29, 2011), http://www.ffiec.gov/pdf/authentication_guidance.pdf (describing “the use of dual customer authorization through different access devices” and “the use of out-of-band verification for transactions” as effective controls in a layered security program).

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.

© 2015 ICI Mutual Insurance Company, RRG

Information current as of September 2015