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.

Protection of Authenticated Sessions

Fund groups often protect the integrity of an authenticated session by terminating the session after some designated period (e.g., 15 minutes) of inactivity on the shareholder's side. This step is intended to guard against the possibility that the shareholder has left his or her computer, and that a fraudster may seek to continue the session.

Fund groups may also wish to consider whether to include additional means of verifying that, after the initial authentication, the person engaging in a transaction remains the properly authenticated shareholder. This could be accomplished, for example, by requiring a shareholder who has just requested a higher-risk transaction (e.g., a transaction of an unusually large dollar amount) to answer KBA questions before the transaction order is sent. Another potential means of performing ongoing or continuous authentication might rely on analyzing a user's behavioral patterns (e.g., analyzing how a shareholder types, uses a mouse, or uses a smartphone).[1]

Endnote

[1] *See, e.g.*, *Active authentication seeks to augment passwords*, INFOSECURITY MAGAZINE (Sept. 10, 2012), http://www.infosecurity-magazine.com/news/active-authentication-seeks-to-augment-passwords/ (describing a project by the U.S. Defense Advanced Research Projects Agency to strengthen the initial authentication of a user through continuous monitoring of the user's keystroke and mouse movements).

Information current as of September 2015