Hardware and Software Tokens

To date, authentication measures based on the second authentication factor—i.e., what a user *has*—appear to be relatively uncommon in the fund industry (although some brokerage firms do offer two-factor authentication). Such measures include the use of hardware tokens (such as the widely-used RSA SecurID token) or software tokens (in the form of text messages or mobile apps, such as the Google Authenticator app), which take advantage of the widespread adoption of smartphones. In considering the use of hardware or software tokens, fund groups may wish to consider, among other things, implementation costs and/or the anticipated degree of shareholder acceptance. For hardware tokens, for example, the cost of purchasing the tokens and providing them to shareholders may be significant.

Software tokens may address the cost issue associated with hardware tokens, but may be less secure because they potentially represent a single point of failure.[1] For example, a fraudster who uses a stolen mobile device to effect a transaction would not be thwarted if the same mobile device receives a text message with the additional authenticating information.[2] By comparison, where hardware tokens are used instead of software tokens, the fraudster would need both the stolen phone *and* the hardware token to effect a fraudulent transaction.

Endnotes

[1] *See, e.g.*, Grant Le Brun, *Hard, Soft, or Smart? Evaluating the Two-Factor Authentication Options*, INFOSECURITY MAGAZINE (Sept. 20, 2012), http://www.infosecurity-magazine.com/view/28368/hard-soft-or-smart-evaluating-the-twofactor-authentication-options-/ (comparing the advantages and disadvantages of hardware and software tokens); Chester Wisniewski, *The power of two - All you need to know about two-factor authentication*, NAKED SECURITY (Jan. 31, 2014), https://nakedsecurity.sophos.com/2014/01/31/the-power-of-two-all-you-need-to-know-about-2fa/ (same).

[2] *See* Grant Le Brun, *Hard, Soft, or Smart? Evaluating the Two-Factor Authentication Options*, INFOSECURITY MAGAZINE (Sept. 20, 2012), http://www.infosecurity-magazine.com/view/28368/hard-soft-or-smart-evaluating-the-twofactor-authentication-options-/ (questioning whether the use of a smartphone both to access sensitive data and to serve as the "something you have" device qualifies as two-factor authentication).