Authentication of Devices

To reduce the risk of transactional fraud, some fund groups consulted for this study seek to ascertain whether a device—e.g., a telephone, computer, or mobile device—that is being used by a shareholder to effect a given transaction has been previously used by the same shareholder. For *telephone* transactions, for example, a fund group might use caller ID to determine the originating telephone number and compare it to numbers used by a shareholder in prior transactions.

For *online* transactions, there are a variety of means by which a fund group might authenticate the device being used. Many fund groups, for example, place a cookie on a shareholder's device when the shareholder logs in to his or her account. At the next login, the fund group can readily establish that the shareholder has previously used the device in question. While cookies may be helpful for certain purposes, it is important to recognize that if not implemented securely, they may also introduce vulnerabilities with respect to shareholder authentication.[1]

A few fund groups consulted for this study have begun to incorporate device fingerprinting into their authentication processes—i.e., compiling information about a shareholder's device to create a profile or "fingerprint" of the device, to be used to assist in authenticating the shareholder in subsequent transactions.[2] For example, a smartphone or other mobile device might provide its location, its Internet protocol (IP) address, screen resolution, and details about the device itself (e.g., model number and its operating system). Similarly, laptops and desktop computers might be queried for their IP addresses, operating system, overall configuration (which may include information about the presence of firewalls or antivirus/antimalware software, the browser and browser plugins used, screen resolution, the presence of other software installed on the computer, and/or the hardware components connected to the computer).

Device Fingerprinting

Devices used by shareholders to engage in transactions may provide identifying information to the fund group. Taken collectively, this information may provide a "device fingerprint" that may not be truly unique, but that is likely to be difficult to spoof. Such identifying information may include:

- Location
- IP address
- Operating system
- Browser
- Other software
- Attached hardware (such as printers or hard drives)

The relative uniqueness—and therefore the relative usefulness—of this "fingerprint" for authentication purposes may vary, depending on the number and type of device characteristics tracked. A device fingerprint that is based on more detailed information about the device's configuration may provide a fund group with a

significantly higher degree of confidence about whether the shareholder has used that particular device in prior transactions.

At some point in the future, it may be that the devices themselves will assist in the authentication process. One mobile device manufacturer is reportedly developing technology that would vary the level of security needed to unlock smartphones and tablets based on the user's location. For example, a user might need to enter a complex password (or a fingerprint) if he or she happens to be in a foreign country, or in a less routinely frequented area domestically, or on public transportation, but may be required to enter only a four-digit passcode if the user is located at home or in his or her office.[3]

Endnotes

[1] *See* Joanne Furtsch, *Best Practices for Using Cookies*, TRUSTe Blog (Dec. 2, 2011), http://www.truste.com/blog/2011/12/02/best-practices-for-using-cookies/; The Fishbowl (2004), http://fishbowl.pastiche.org/2004/01/19/persistent_login_cookie_best_practice/.

[2] *See* Dan Goodin, *Top sites (and maybe the NSA) track users with "device fingerprinting"*, ARS TECHNICA (Oct. 11, 2013), http://arstechnica.com/security/2013/10/top-sites-and-maybe-the-nsa-track-users-with-device-fingerprinting/.

[3] *See* Jasper Hamill, *Future Apple gumble could lock fanbois out of their own devices*, THE REGISTER (Jul. 3, 2014), http://www.theregister.co.uk/2014/07/03/apple_location_security_tech_could_auto_lock_your_istuff/.