Shareholder Authentication

Managing the Risk of Fraudulent Transactions

ICI Mutual
The safest decision you can make

Table of Contents

Additional Information and Resources Available Online

Please visit ICI Mutual's website (www.icimutual.com) for an interactive online version of this document. The online version provides links to more detailed discussions of particular topics, as well as an online glossary of key terms utilized in the document. The underlined, colored text in this document indicates where additional information may be found online.

Introduction

Recent large-scale data breaches have heightened concerns among regulators, businesses, and the public over the risk of identity theft and the resulting potential for fraudulent financial transactions. Other developments associated with the digital age—i.e., advances in computing power, the rise of social media, and growth in online commerce—have also fueled these concerns. The concerns are well founded. Fraudulent customer transactions reportedly cost financial institutions and their customers billions of dollars each year. To date, most fraudulent transactions have occurred outside the mutual fund context. Yet the fund industry has not been immune, and the ongoing risk to the industry and to fund shareholders cannot be discounted.

Fund groups have long sought to protect the integrity of transactions effected by fund shareholders, whether effected by traditional means (e.g., in writing, by telephone) or by newer means (e.g., online, via mobile apps). But the digital age has added to the challenges, and for many fund groups, these challenges have underscored the importance of "shareholder authentication"—that is, of having appropriate mechanisms and processes in place (1) to confirm the identities of shareholders who seek to conduct redemptions or other transactions involving fund shares, and (2) to ensure the integrity of the transactions that are effected by those fund shareholders.

Key Aims of Shareholder Authentication

- Confirm shareholder identity
- Ensure transactional integrity

The fund industry's interest in effective authentication techniques reflects a recognition that even a low incidence of transactional fraud can have significant consequences for affected fund groups and their shareholders, in terms of (1) financial damage (i.e., direct financial loss for fund groups and/or fund shareholders); (2) legal damage (to the extent that transactional fraud gives rise to regulatory scrutiny and/or private litigation); and/or (3) reputational harm. Indeed, for fund groups, where maintaining the trust of shareholders and business partners is central to successful operations, the reputational harm that can be associated with fraudulent transactions may ultimately be the most significant of the three.

This study explores mechanisms and processes implemented by fund groups to confirm shareholders' identities and to ensure the integrity of transactions. This study is divided into two parts:

- **Shareholder Authentication in Theory:** Part I describes (1) general principles of authentication, and (2) limitations of authentication, both with respect to particular authentication measures and with respect to authentication generally.

- **Shareholder Authentication in Practice:** Part II reviews practical considerations for fund complexes when addressing authentication issues, focusing on (1) technological solutions, (2) operational initiatives, and (3) educational efforts.

This study focuses primarily on redemptions and other fund share transactions effected by retail shareholders directly with fund groups over the telephone or online. But the contents of

this study may also be relevant to the broader universe of transactions involving fund shares, including those effected by institutional shareholders, by retail shareholders transacting through financial intermediaries, and by retail shareholders who are requesting transactions by letter or facsimile.

Part I: Shareholder Authentication in Theory

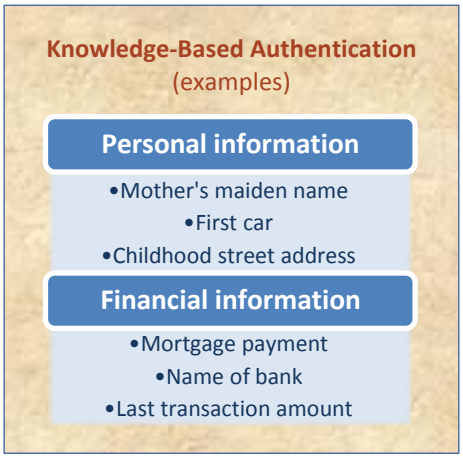
The fund industry relies on shareholder authentication as a fundamental means of protecting transactional integrity. This part of the study reviews general authentication principles, and outlines some of the inherent limitations of particular authentication measures and of authentication generally.

Principles of Authentication

Shareholder authentication involves testing the identity of a user through the use of one or more "factors," each of which may be implemented through one or more specific means, or "measures."

There are three "traditional" factors for testing user identities:

- The first traditional authentication factor, *what you know*, involves testing the identity of a user on the basis of something the user knows which is unique to that user. Reliance solely on this first authentication factor is generally referred to as single-factor authentication. One very common measure to implement this factor is to require a user to enter a username and password. Sometimes this factor may be implemented through use of additional measures, as well (e.g., asking knowledge-based questions about a user's personal life). The use of multiple measures (e.g., a username/password *and* knowledge-based questions) to implement this first factor is often referred to as enhanced authentication.

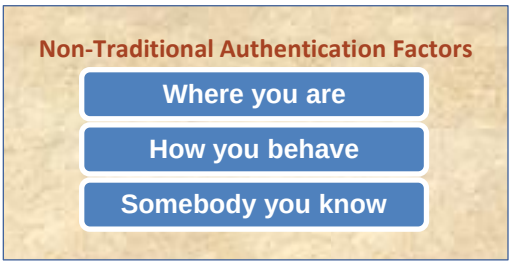


- The second traditional authentication factor, *what you have*, involves testing the identity of a user on the basis of something unique that the user has in his or her possession (often a particular device). Measures used to implement this second factor may include issuing and requiring the use of a hardware identification token or smartphone. Reliance on both what a user has *and* what a user knows is often referred to as two-factor authentication.

- The third authentication factor, *what you are*, involves testing the identity of a user using "biometrics" (i.e., a biological characteristic or attribute unique to the user). Measures used to implement this third factor may include establishing the identity of a user based on his or her voice, fingerprint, retinal or iris pattern, artery pattern, or DNA.

All else being equal, authentication systems relying on multi-factor authentication (i.e., the use of a combination of the first factor and one or both of the other two factors) are viewed as offering stronger protection than those relying on a single factor. Systems relying on all three of the factors are viewed as offering stronger protection than those relying on just two factors.

Certain current and/or proposed authentication measures may not always fit neatly within the framework of the three traditional factors. In order to categorize such measures, some experts have articulated additional, non-"traditional" authentication factors. These include: (1) *where you are* (e.g., assessing where a user is located based on information provided by the user's computer or mobile device); (2) *how you behave* (or *what you do*) (e.g., analyzing patterns of behavior with respect to logging in, navigating the website, or engaging in transactions); and (3) *somebody you know* (e.g., having your identity verified by one or more financial or other institutions).



Authentication is often viewed as primarily a one-way process, which focuses on testing the identity of a user. But authentication can also be a two-way process (i.e., mutual authentication). Mutual authentication addresses concerns of users who may wish to have greater confidence that they are dealing with their financial institutions, and not with fraudsters. Examples of measures used in mutual authentication include the use of digital certificates and/or the use of images while logging into certain financial institution websites, with a caution to users not to proceed unless the images displayed are those that are pre-selected by users.

Authentication measures also may be referred to as "positive" or "negative." Many authentication measures, including those relating to the three traditional authentication factors discussed above, are "positive" measures, in the sense that they are intended to positively identify a person seeking to effect a transaction *as the shareholder* (or other authorized person). Other authentication measures may be viewed as "negative," in the sense that they are chiefly intended to screen out probable impostors. These negative authentication measures (or "de-authentication" measures) may be used to establish the identity of the person seeking to effect a transaction *as somebody other than the shareholder*. For example, a person's *ability* to provide a shareholder's Social Security number or address of record may not positively identify the person as the shareholder, but the *inability* to provide such basic information suggests that the person is an impostor.

Limitations of Authentication

Authentication measures have their limitations. Some of the authentication measures in common use by fund groups have become less effective over time. In particular, the single-factor username/password combination historically (and still commonly) used by fund groups to authenticate shareholders may, for various reasons, offer less absolute protection against fraud than it has in the past. A username/password combination (as well as other personal information) can be at risk of being lost or misappropriated (e.g., in the event of large-scale data breaches). Even absent misappropriation, fraudsters have become quicker and more sophisticated at cracking ever stronger passwords (including those with numbers, special characters, and a mix of capitalization).

Similarly, the information underlying knowledge-based authentication questions (e.g., a user's mother's maiden name or the name of a childhood pet) may be lost or misappropriated in large-scale data breaches. Even in the absence of loss or misappropriation, such questions may offer less absolute protection than in the past; with the rise of social media, such underlying knowledge-based information has tended to become more broadly available and accessible to fraudsters.

Authentication measures are subject to more general limitations as well. For example, the strength of a password—or, indeed, of stronger authentication measures—may be irrelevant if a fraudster *compromises* the systems of a financial institution and then causes such systems to transfer money or initiate transactions. Password strength is likewise irrelevant if a fraudster is otherwise able to *circumvent* the need for the password. For example, in a man-in-the-middle attack, a fraudster may "hijack" a session in which a user has already been authenticated by an organization. Because the fraudster is impersonating both the user (to the organization) and the organization (to the user), neither party may be aware that the session has been hijacked.

Part II: Shareholder Authentication in Practice

Fund groups have adopted a variety of approaches to shareholder authentication. A robust approach to shareholder authentication tends to rely on "defense in depth." In this context, "defense in depth" implies multiple layers of protection that tend to incorporate one or more of the following three elements: (1) technological solutions that provide greater confidence in establishing the identity of a shareholder; (2) operational initiatives, which may include risk assessments and the implementation of targeted policies and procedures; and (3) educational efforts designed to reduce the risk of human error on the part of both employees and shareholders.

Technological Solutions

Fund groups may adopt a variety of technological measures, both positive and negative, to authenticate each of the various elements of a shareholder transaction: (1) the person (i.e., the shareholder); (2) the device that he or she is using to effect the transaction; (3) the details of the transaction at issue; and (4) the fund group itself.

Fund groups have tended to focus primarily on the first of these elements—i.e., authenticating the person. This has typically been accomplished through single-factor authentication measures based on shareholder knowledge. Less commonly, fund groups have begun to employ other types of authentication measures, such as those based on hardware or software tokens or on biometrics or behavioral patterns. Moreover, once fund groups have authenticated the person, they often take steps designed to protect the integrity of a properly authenticated session so as to provide assurance that the person on the other side of the transaction continues to be the properly authenticated person. In this regard, fund groups may, for example, terminate a session after some period of inactivity.

Separate and apart from authenticating the person, some fund groups also seek to authenticate the device (e.g., a telephone, computer, or mobile device) that is being used to effect a given transaction. Here, the focus is on whether the particular device has previously been used by the shareholder. Thus, for example, in telephone transactions, a fund group might use caller ID to determine the originating telephone number and compare that number to numbers used by the shareholder in prior transactions. In online transactions, there are a variety of means (e.g., through the use of "cookies" or by examining the configuration of the device used) by which a fund group might ascertain that the device being used is the same device previously used by the shareholder.

Fund groups may also seek to authenticate the transaction itself (i.e., the details of the transaction), by seeking to establish that a given transaction is consistent with previous transactions made by the same shareholder, and therefore more likely to be a legitimate transaction. Authentication of transactions, whether after the fact or in real time, tends to help reduce the incidence of fraudulent transactions, without having a significant adverse impact on ease of use or shareholder convenience.

Many fund groups also take steps to ensure that shareholders are able to authenticate the fund groups themselves (i.e., to confirm the identity and validity of the shareholders' online connections to the fund groups). Often, this form of "mutual authentication" is accomplished through digital certificates signed by a trusted certifying authority or through the use of security images.

Operational Initiatives

While technology plays a critical role in effective approaches to shareholder authentication, operational initiatives can be equally important. Operational initiatives include (1) assessments of relevant risks to transactional integrity, and (2) development of appropriate policies and procedures to mitigate those risks.

> *"The implementation of appropriate authentication methodologies should start with an assessment of the risk posed…."*
>
> — FFIEC, Supplement to Authentication in an Internet Banking Environment (June 29, 2011), http://www.ffiec.gov/pdf/authentication_guidance.pdf

In conducting risk assessments, fund groups tend to consider the following:

(1) overall threat environment (e.g., the growing threat from external actors, the evolution in the provision of services to shareholders, and the emergence and/or discovery of new vulnerabilities);

(2) risks associated with authentication systems generally (e.g., the ongoing effectiveness of existing authentication systems, and the consideration of new technologies and techniques);

(3) risks associated with particular transactions or groups of transactions (e.g., whether certain transactions may facilitate fraud in the future, or may, in combination with other transactions, be viewed as potentially suspicious); and

(4) potential legal consequences of transactional fraud (e.g., whether transactional fraud, or a fund group's approach to preventing such fraud, might lead to regulatory scrutiny and/or private litigation).

The potential for damage from fraudulent transactions is already limited, to some extent, by the "closed" nature of most fund shareholder transactions—redemptions in fund shares tend to be made to the shareholder of record at the address of record, or to pre-designated persons or bank accounts. But fund groups may utilize additional measures to further limit the potential for damage from fraudulent transactions. For example, fund groups may adopt restrictions on shareholder redemptions that are

NIST Checklist for Risk Assessment

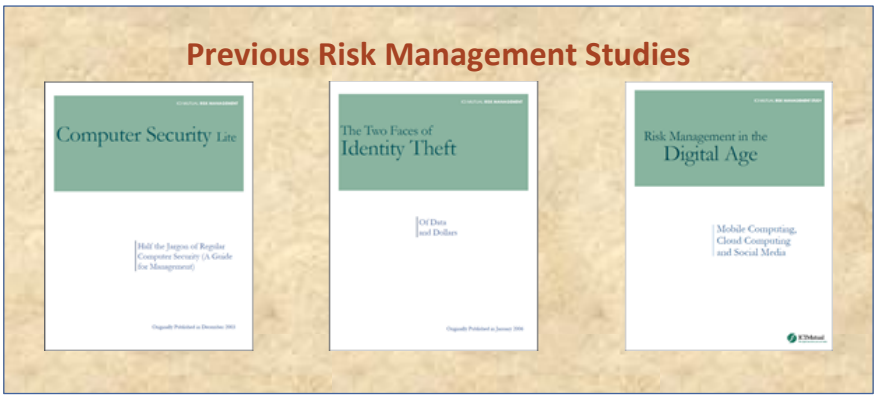
In 2014, the National Institute for Standards and Technology ("NIST") released a "Framework for Improving Critical Infrastructure Cybersecurity," which is viewed by some observers as "fast becoming the *de facto* standard for private sector cybersecurity." Under this "Cybersecurity Framework," a company should consider the following:

- Asset vulnerabilities are identified and documented
- Threat and vulnerability information is received from information sharing forums and sources
- Threats, both internal and external, are identified and documented
- Potential business impacts and likelihoods are identified
- Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
- Risk responses are identified and prioritized

NIST, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

See Richard Raysman and Francesca Morris, *CIOs Ignore the NIST Cybersecurity Framework at Their Own Peril*, WALL ST. J. (Dec. 18, 2014), http://blogs.wsj.com/cio/2014/12/18/cios-ignore-the-nist-cybersecurity-framework-at-their-own-peril/tab/print/.

made to other persons, addresses, or bank accounts. Fund groups may also impose transaction thresholds on purchases, sales, or exchanges and/or by placing restrictions on the types of transactions that may be effected through certain channels (e.g., via fund group websites or mobile apps).



Fund groups also take steps to appropriately safeguard authentication-related information and to protect online transaction systems—and the authentication-related information on those systems (which may include usernames and passwords, as well as the responses to security questions)—from both external and internal threats. With respect to authentication-related information, merely encrypting passwords can be viewed as insufficient because encryption is designed to be a reversible operation. To address this vulnerability, fund groups tend—in a process referred to as salting and hashing—to add characters to passwords and then run them through an algorithm designed to be irreversible. As for protection of the online transactions systems themselves, a full discussion of relevant network security measures is beyond the scope of this study, but has been described in greater detail in ICI Mutual's previous risk management studies on computer security, identity theft, and digital age risks.

Educational Efforts

As with many risk management initiatives, people are often the weakest link in the authentication chain (i.e., process). Greater awareness by employees and shareholders alike may provide an important defense against fraudulent transactions and against identity theft (which may lead to fraudulent transactions).

Some fund groups provide fraud training to some or all of their employees and seek to raise employee awareness of risks associated with fraudulent shareholder transactions. Such employee training and awareness, often conducted at regular (e.g., annual) intervals, may be specifically focused on customer service representatives who are directly interacting with shareholders, or may extend more broadly to fostering company-wide awareness with respect to fraud issues (e.g., by training employees to identify fraudulent e-mails).

Fund groups often take a variety of steps to raise shareholder awareness about potential threats to their personal information and assets. While not requiring financial institutions to provide such information, regulators have encouraged these efforts as a defense against fraud and identity theft. The U.S. Securities and Exchange Commission's recent cybersecurity initiative, for example, specifically focused on information that may be given to customers about steps that they may take to reduce cybersecurity risks in conducting transactions.

Insurance Considerations

Financial institution bonds utilized by fund groups (sometimes known as investment company blanket bonds) often provide at least some degree of coverage against losses resulting from third-party frauds in requests for redemptions and other designated transactions in fund shares. Bonds may differ with respect to the scope of coverages afforded, as well as in the specific terms and conditions to which these coverages are subject. Coverage terms aside, the insurers themselves may also differ in their experience in the bond market, their claims-handling reputations, their responsiveness to administrative and coverage needs of insureds, and the client services they make available.

Note to Readers

This study—which is directed primarily towards senior management and towards those fund group personnel with responsibility for assessing and managing risks associated with fraudulent share transactions—is designed to serve as a resource for fund groups as they continue to develop and refine their own risk management approaches and techniques in this regard. The contents of this study reflect ICI Mutual's interviews with selected fund groups, consultation with industry and technical experts with specialized knowledge of shareholder authentication issues, and review of available literature.

This study is intended to assist fund group personnel in evaluating risks associated with shareholder authentication, and in developing risk management approaches tailored to the risks and needs of their own organizations. This study is not intended to, and does not, recommend any single approach or set of "best practices" for shareholder authentication. One-size-fits-all standards are generally not practical or advisable, given the diversity of the industry, the range of risk management techniques that may be utilized by fund groups, and the pace of technological developments. Moreover, nothing in this study should be considered legal advice; rather, readers should look to their counsel for such advice.