Information Notice

Cybersecurity Background: Authentication Methods

October 15, 2020

Summary

A key element in any firm's cybersecurity program is a robust authentication process, *i.e.*, the method that confirms that an authorized user seeking access to a firm's information technology systems is who they say they are.[1] This process typically relies on one or more "factors," such as a password or personal identification number (PIN) code, to provide the authentication. The importance of sound authentication techniques to protect investors' and firms' confidential information has increased in light of 1) escalating threats to the most commonly used form of authentication (single factor or password-based authentication) and 2) firms responding to the COVID-19 pandemic with work arrangements that typically require registered representatives to log in to their networks from a remote location.

In the 2018 Report on Selected Cybersecurity Practices and *Information Notice 10/2/19* (Cybersecurity Alert: Cloud-Based Email Account Takeovers), FINRA identified implementation of multi-factor authentication (discussed in greater detail below) as an effective practice firms may consider as one element in a broader cybersecurity program. This *Notice* provides additional, non-exhaustive background on authentication techniques for firms to consider as they implement authentication programs.

This *Notice* is not intended to express any legal position, and does not create any new legal requirements or change existing regulatory obligations.

Questions concerning this *Information Notice* should be directed to:

- Dave Kelley, Director, Member Supervision Specialist Programs, at (816) 802-4729 or *david.kelley@finra.org*; or
- Alex Khachaturian, Director, Office of Financial Innovation, at (202) 728-8275 or *alex.khachaturian@finra.org*.

Suggested Routing

- Compliance
- Information Technology
- Legal
- Operations
- Registered Representatives
- Risk
- Senior Management

Key Topics

- Cybersecurity
- Authentication
- Access Control

“Factors” in Authentication

There are a variety of means—or factors—that firms’ information technology systems can use to verify or authenticate whether a user is who they say they are. When those systems use more than one factor, with the first factor normally being a password, the authentication technique is referred to as multi-factor authentication.

- **Something You Know:** This authentication technique consists of a series of memorized, secret characters, such as a PIN or password. Using passwords as a single layer of protection may pose risks given the ubiquity of methods for stealing these credentials.
- **Something You Have:** This authentication technique can be either static (*e.g.,* certificate) or dynamic (*e.g.,* temporary or time-based one-time password) secrets. Users may carry them around as a “hard,” physical token (such as key FOBs),[2] have them installed or delivered to their devices in the form of a “soft” token (such as mobile phone app),[3] or received via out-of-band electronic accounts (such as email).
- **Something You Are:** This authentication technique consists of the characteristics that are exclusive to a person’s genetic makeup (*e.g.,* biometrics), commonly known to include fingerprints, retina or iris scans, voice recognition and facial recognition. Biometric authentication’s ability to rely on human features may make the technique convenient and simple for users. However, because human features can be difficult or even impossible to alter, biometric authentication contains limitations on the ability to change login details, either periodically or in the event of a known compromise.
- **Somewhere You Are:** This authentication technique relates to a user’s geographical location and is usually determined by the internet protocol (IP) address, which may be useful in detecting account access attempts coming from anomalous locations, such as those outside of a user’s country of work or residence. For financial accounts and transactions, this approach may be considered a supplemental measure, to enhance primary or secondary factors for authentication.
- **Something You Do:** This authentication technique consists of attempts to provide authentication by observing actions, such as gestures or touches on a screen or picture. This may be a viable alternative to one-time passwords when secure push and tap confirmation notifications are delivered to a supporting app installed on a registered device.

Single-Factor Authentication

Single-factor authentication is typically based on a secret password known only to users, and is widely used by broker-dealers, especially with customers. However, attacks on password credentials, as well as their theft, represent a vast majority of the hacking tactics associated with reported breaches. There are a number of ways that bad actors may compromise passwords including:[4]

- **Shoulder Surfing:** where a bystander, in proximity, views a password entered by a user;
- **Brute Force Attacks:** where an attacker permutates through multiple possible password combinations;
- **Password Spraying:** a larger-scale brute-force attack that targets a number of accounts;
- **Phishing:** emails used to lure users to unwittingly hand over credentials;
- **Keylogging:** installing a malware program to steal user secrets when input;
- **Credential Stuffing:** where stolen lists of emails, usernames and passwords are used for large-scale automated logins hoping to find a situation where a person uses the same username and password combination on multiple sites;
- **Man-in-the-Middle Attacks:** where an attacker secretly intervenes between two communicating parties in order to observe and record credentials.

FINRA has observed firms implement technical measures—some of them recommended by the National Institute of Standards and Technology (NIST)—to try and mitigate at least some of these threats, for example by:

- requiring minimum password length;
- requiring that passwords include special characters (which helps mitigate the threat of brute force attacks);
- restricting sequential and repetitive characters;
- preventing context-specific passwords (*e.g.,* those that use the firm's name or one of their products);
- requiring users to change their passwords periodically;
- prohibiting the use of frequently used passwords and common dictionary words;
- not allowing the re-use of passwords;
- establishing lockout procedures in the event an account is subject to multiple unsuccessful log-in attempts; and
- defending against automated computer-based attacks from malicious bots, for example, by using tests to verify that an actor is human (*e.g.,* Completely Automated Public Turing Test (CAPTCHA) challenges).[5]

Some firms supplement their technical controls with measures to educate and empower investors—including with respect to the ever-present danger from phishing attacks—by, for example:

- making customer service contact information readily accessible; and
- providing users with information for how trusted copies of communications will and will not be provided to them (*e.g.,* mail, email, communication with customer service).

In addition, firms may train customer-facing staff to identify and avoid attempts to gain unauthorized access to user accounts, such as phishing attacks or fraudulent password reset attempts.[6]

Multi-factor Authentication

Unlike single-factor authentication, multi-factor authentication uses two or more different types of factors or secrets, which significantly reduces the likelihood that the exposure of a single credential, such as a password, will result in account compromise.

FINRA has observed a number of firms implement multifactor authentication techniques that they require associated persons or vendors to use. For example, some member firms:

- implement two-factor authentication (2FA) for all log-in activity outside of their networks or portals by general users (*e.g.,* registered representatives, internal administrators);
- require individuals with elevated privileges—such as systems or database administrators—to use multifactor authentication when they log in to sessions where they exercise these elevated privileges; and
- require individuals with elevated privileges who log in to highly sensitive data or systems to use a separate username and password combination, in addition to using multifactor authentication. This access is typically recorded in a log and reported on as an access-related control.

Although less common, FINRA has observed firms that provide customers with the option of implementing two-factor authentication on their brokerage account(s). In providing this option, firms have noted that they need to balance customer convenience and security considerations

In addition, to controlling access to proprietary firm systems, FINRA has observed firms implementing 2FA for access to third-party services that the firm uses. For example, some firms that use the Microsoft Office 365 cloud-based email platform implemented 2FA by incorporating the Microsoft Authenticator application on their users' mobile devices or by sending a dynamically generated PIN via SMS text. In addition, these firms carefully review the platform's available authentication and other access controls to understand those features the firm can configure to appropriately limit access.

Additional Resources

Resources firms may consider for information as they assess and develop their authentication systems include:[7]

Fast IDentity Online (FIDO) Alliance: an open industry association of global technology firms whose mission is to limit over-reliance on passwords for authentication.

NIST Strength of Function for Authenticators (SOFA): an initiative to develop a framework for evaluating the security strength of various authentication technologies.

In addition, FINRA discusses firms' use of multi-factor authentication in the 2018 Report on Selected Cybersecurity Practices, the 2019 Report on Examination Findings and Observations and *Information Notice 10/2/19*, *Cybersecurity Alert: Cloud-Based Email Account Takeovers.*

Endnotes

1. "Users" in this context refers to authorized individuals, processes or systems.

2. Hard tokens are secure, self-contained devices with the sole purpose of providing a periodic secret (usually rotated every 60 seconds) in sync with a secure timing server integrated with the authentication service. A potential downside of hard tokens is that they may be relatively more expensive than soft tokens, they may expire or need a new battery over time, and the setup and recovery time if lost, stolen or damaged is longer.

3. Soft tokens are generally less costly than hard tokens and are often recommended as event-based gestures delivered to an app installed on a registered device, rather than token values sent via text or Short Message Service (SMS), to avoid possible SMS-intercept issues.

4. FINRA *Information Notice 10/2/19*, *Cybersecurity Alert: Cloud-Based Email Account Takeovers.*

5. National Institute of Standards and Standards and Technology, Special Publication 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*, June 2017.

6. For more information *see* FINRA Investor Alert, *"Phishing" and Other Online Identity Theft Scams* (Feb. 29, 2012).

7. FINRA does not endorse the listed standards and firms are not obligated to use them. The use of these standards does not ensure compliance with FINRA rules or other regulations or laws.

Regulatory Notices attempt to present information to readers in a format that is easily understandable. However, please be aware that, in case of any misunderstanding, the rule language prevails.