BITS Multifactor Authentication

FEBRUARY 2023

Member Contributors

Matt Darlage, Citizens Bank

Todd Dufour, Citizens Bank

Dana Ingraham, KeyBank

Stephen Locke, Northern Trust

Sean Hollingsead, State Farm

Richard Jones, TD Bank

Steve Harrington, Truist Financial Corporation

Andrew Strear, Truist Financial Corporation

Ann Hines, USAA

Jeremy Stevens, USAA

Charlie Kandiko, U.S. Bank

BITS Staff

Andrew Kennedy

Table of Contents

About This Document

TRADEMARK INFO

Names, products and services referenced within this document may be the trade names, trademarks or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our readers, and do not constitute or imply endorsement by the Financial Institutions, Bank Policy Institute or the Authors' employers of any entity, event, product, service or enterprise.

ABOUT THE AUTHORS

BITS, the Bank Policy Institute's technology policy division, promotes current and emerging technology and fosters innovation to reduce fraud and improve cybersecurity, resilience and risk management practices for the nation's financial sector. BITS members include banks, insurance firms, asset managers, card companies, financial market utilities and technology providers. BITS also provides forums for board of directors, CEOs, CIOs, CISOs and senior executives of these organizations to have in-depth, informed and insightful discussions on the use of technology in financial services. Multifactor authentication has been identified by BITS members as an important technology and security area for their firms. As a result, subject matter experts from participating financial services organizations have joined efforts to create this paper.

Executive Summary

The purpose of authentication is to provide a high level of assurance that the entity logging on to a system or application is who they say they are. In the digital world, username and password has been traditionally accepted as an appropriate authentication control; however, with widespread data breaches, phishing and other nefarious criminal activities being prevalent, this "single-factor" authentication has been challenged as a reliable authentication control in high-risk use cases and is often insufficient. Multifactor authentication (MFA), the use of more than one authentication input, has become the minimum industry standard for stronger authentication assurance. These authenticators can include biometrics, one-time passcodes or a physical token like a smartcard.

Authentication controls are intended to ensure access to assets are granted to the authorized user at the appropriate entitlement level. Foundationally, access controls are organized into three categories:

- Something you know;
- Something you have; and
- Something you are.

In the physical world, the reliance has been on something you have (ID, badge, etc.). In the digital world, there has been an historical reliance on something you know (e.g., username and password). Advancements in technology have made it possible to enhance digital access by replacing or supplementing knowledge-based access with alternatives. Notable changes over the past few decades include:

- Proliferation of data breaches that have put personal credentials in the wrong hands;
- Considerable growth of mobile device use leading to more significant 'footprint' to protect; and
- Migration from physical interaction to digital.

These changes are challenging historical authentication norms requiring firms to revisit the effectiveness of legacy access controls. The use of two or more authenticators in at least two different categories, also known as multifactor authentication, significantly increases authorized user confidence levels. The use of MFA, however, may not be applicable in all use cases. The guidance of when and how to use MFA varies. The purpose of this paper is to provide an industry perspective on the use of MFA in context of risk mitigation, user impact, alternatives and operational considerations.

Given the proliferation of authentication guidance from state, federal and international regulators and private sector bodies such as PCI and SWIFT, the scope of this BITS paper is to develop an industry consensus on MFA requirements to achieve effective identity assurance for both a firm's workforce and customers.

Section I – Need for MFA

The most common authentication method in use today is still a username and password combination. A 2022 study of password use found weaknesses in this approach including the following:

- The most common password in the United States is 123456.
- 42% of seasonal passwords contained the word "summer."
- 54% of organizations do not have a tool to manage passwords.
- 93% of brute forced passwords had eight or more characters (long passwords alone are not sufficient).
- 41% of passwords used in real attacks are 12 characters or longer.
- 68% of passwords used in real attacks include at least two character types (e.g., letters, numbers or symbols).

Source: SpecOps Weak Password Report, 2022

These metrics underscore the fact that traditional password methods offer an easily managed "user friendly" way of user identification and authorization, but fall short of serving their main purpose of safeguarding access to digital resources that they are meant to protect.

Challenges with password-based authentication include[1]:

1) Password-Based Methods Do Not Accurately Determine Identity – User ID and password combinations are easily exploited because once an attacker knows the legitimate user's ID code and captures their password, they can gain access by masquerading as the legitimate user.
2) Passwords Are Easily Compromised – End-user behaviors are the source of most password weaknesses. These include succumbing to phishing attacks and the selection of easily guessed passwords. Users frequently select credentials comprised of the user's ID, the word "password," personal names of family members, names of pets or words commonly found in dictionaries. Users also record passwords directly on their computer system, which can be extracted and exfiltrated by malware attacks. Users also face the challenge of remembering multiple passwords, leading users to leverage the same password across multiple platforms. In addition, some applications allow "non-expiring" passwords, compounding the issue. Attackers are aware of these insecure behaviors and exploit them. Once credentials are acquired (typically on a low-risk platform), they often allow access to other platforms with a single compromise (possibly higher-risk platforms such as banking or payment platforms).
3) Password Administration Challenges – To mitigate security issues associated with passwords, application owners tighten security controls to require more complex passwords – for example, through longer password lengths, the use of special characters and requiring capital letters or numbers. Application owners also require

[1] SpecOps Weak Password Report, 2022

more frequent password changes, leaving users back in the quandary of not being able to remember passwords, recording the password somewhere for future reference and forgetting the passwords, leading to the frequent need for password resets.

For financial institutions, this scenario represents a "single control" failure resulting in several undesirable outcomes:

- Client Dissatisfaction – Clients are frequently frustrated and dissatisfied with having to remember more complex passwords.
- Costly Password Reset Support – Organizations must dedicate call center resources to password reset support which increases overall support wait times, which can negatively affect client satisfaction.
- Auditor & Regulatory Challenges – Financial services oversight groups (FDIC, OCC, FSB, etc.) have raised concerns with the financial services sector's use of single-factor authentication and have increased examination of this area.
- Prevalent Password Based Attacker Exploits – Automated and social attacks such as phishing (by email), smishing (by SMS) and vishing (by phone) have become prominent cyber attacker exploits resulting in financial services organizations having to put extensive cybersecurity defenses and programs in place to deal with these attack methods, often with limited effectiveness.

Given the risks associated with single-factor authentication (e.g., password-based authentication) there is a growing need for organizations to migrate to stronger authentication methods that provide enhanced security against increasingly complex cyberattacks. The decline in assurance for traditional authentication methods has been documented by independent authorities, government agencies and many others, including:

- The National Institutes of Standards & Technology (NIST) – Password Guidance
- The Information Security Institute's 2022 Worst Passwords of the Decade Article – Worst Passwords of the Decade: A Historical Analysis
- The Verizon Data Breach Investigations Report (DBIR) points out that 81% of hacking related breaches are the result of compromised passwords in its 2022 Data Breach Investigations Report
- Federal Financial Institutions Examination Council (FFIEC) guidance – Authentication and Access to Financial Institution Services and Systems

Note that financial institutions are held to a high standard because they are a prominent target due to the accessibility of sensitive data and the ability to monetize attacks.

Section II – MFA Defined

Secure authentication is required when legitimate system users attempt to access (i.e., "log on" to) a computer resource, such as, a network, device, web site or other application, especially if those resources contain valuable assets. Single-factor authentication requires only one such piece of evidence – typically credentials. Implicit in authentication is that the selected protection scheme, whether single-factor, multifactor or something else, effectively prevents unauthorized sources from gaining access to those assets. It is not that passwords do not work but, alone, they are not as effective as other methods at positively authenticating the identity of those attempting access.

Access to the resource may require more than one authentication element where additional identity assurance is needed. That may include two factor authentication, or multifactor authentication where two or more

authentication elements are required to be in place. These authentication "factors" typically include two or more of the following elements:

- Something the User Has - Any physical object in the possession of the user, such as a security token or smartphone-based application with a frequently changing synchronized access code display, Universal Serial Bus (USB) stick, a bank card, a key, a smartphone, the user's web browser, etc.
- Something the User Knows - Certain value only known to the user, such as a password or Personal Identification Number (PIN).
- Something the User Is - Some physical characteristic of the user commonly referred to as "physical biometrics", such as a fingerprint, eye (iris), voice or face that is read through a device and matched against a stored characteristic value called a "print". If proven reliable[2], behavioral biometrics that measure user specific patterns (e.g., keystroke or mouse patterns) could be considered something the user is.

  Note: While behavioral biometrics rely on semi-unique patterns like typing cadence and mouse movement, human behavior can be mechanically inconsistent or imitated and complicated by real world operations that can serve to reduce the assurance levels of these authentication techniques by themselves.

It is important to note that use of MFA typically increases access and authentication complexity and may reduce the "user friendliness" of systems and applications. Secondarily, using a combination of MFA factors significantly raises the security bar but doesn't eliminate authentication risk. Advanced cyberattacks can still be effective in exploiting MFA methods warranting a risk-based implementation approach.

Despite these known limitations and risks, MFA is strongly and widely endorsed by authoritative sources including:

- Cybersecurity & Infrastructure Security Agency (CISA) - Multifactor Authentication | CISA
- NIST MFA Page - Multifactor Authentication | NIST

Section III - A Risk-Based Approach to the Application of MFA

LEVERAGING A RISK-BASED APPROACH

The UK's Financial Services Authority (FSA) originally defined a risk-based approach in the context of Anti-Money Laundering Controls[3] by laying out a three-step methodology:

- Recognize Existence of a Risk – Multifactor authentication is commonly used as a control against the use of compromised credentials. Compromised credentials are harvested, used or sold regularly. Since credential reuse across unrelated sites is high, data breaches or credentials compromised from other sites become problematic across industries.

- Assess the Risk – The decision to leverage single-factor vs. multifactor authentication should be based on risk to the business, customers and the sector including impacts ranging from business disruption to customer and privacy protection. Firms should identify and prioritize use cases to mitigate these challenges appropriately. The risk/impact of compromise should be evaluated in context of the access the credentials grant. Given there are a range of potential impacts, the totality of the risk should be evaluated when determining if, and where, to deploy MFA.

[2] https://www.csoonline.com/article/3330695/6-reasons-biometrics-are-bad-authenticators-and-1-acceptable-use.html
[3] "A new regulator for the new millennium", FSA, 2000

- Develop and Deploy Strategies – Strategies should be developed to reduce risk to a level that fits within the financial institution's (FI) risk tolerance. NIST Special Publication 800-63-3 (Digital Authentication Guidelines)[4] contains a framework and approach to consistently applying authentication assurance levels based on risk.

WHEN SHOULD A FINANCIAL INSTITUTION EMPLOY MFA?

When determining whether MFA should be employed, there are a few primary considerations / drivers:

- The sensitivity of the data or service needing protection;
- The entitlement and level of access provided by the user ID and the role in the firm the user ID holder has, aligned with providing access limited what the user someone needs to perform;
- The likelihood of a compromise, based upon a risk analysis of the user, of the role they have, and the value of the service they provide; and
- Compliance with regulatory guidelines.

REGULATORY GUIDELINES

Aside from risk factors, MFA deployment can be driven by regulatory requirements. As an example, the New York Department of Financial Services (NYDFS) has levied very large fines against corporations that failed to implement MFA consistent with their regulations.[5][6] The SEC has also fined financial services companies for failing to protect email accounts with sufficient controls, that subsequently allowed breaches even after the organizations were initially warned of the vulnerabilities.[7]

The FFIEC has issued several iterations of guidance requiring banks to perform risk assessments and implement stronger authentication for high-risk transactions, the most recent being 2021.[8] SWIFT in 2021, revised Customer Security Programme (CSP) mandatory control 4.2 which lays out requirements for MFA in money transfer.[9] Additionally, Europe's General Data Protection Regulation (GDPR) requires that data considered a high risk must be protected by MFA[10]. Organizations will need to determine in all of these cases how, or if, these are required. Organizations may face a gray area regarding the applicability of these requirements due to ambiguity in the language. Bearing that in mind, best practices dictate that MFA should be considered for use cases that provide access to sensitive data, and where increased friction (anything that impedes customers from finalizing a transaction) is acceptable to prevent the risk of data loss/exposure. Be aware that some regulations require specific controls when customer data is involved, including strong authentication. This must always be a primary consideration when planning when and where to enforce MFA in a system.
Additionally, private sector regulators such as PCI DSS guidance have requirements for the use of MFA[11]

LEVEL OF PRIVILEGES AND ROLES

Level of access (or entitlement) should be a driving force in a risk-based approach to enforcing MFA for authentication. While each firm needs to define what it means to have privileged access, there are a few broad categories to consider in a risk-based MFA deployment:

[4] https://pages.nist.gov/800-63-3/sp800-63-3.html
[5] https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202105131
[6] https://www.jdsupra.com/legalnews/nydfs-imposes-heavy-fine-and-adopts-7165817/
[7] https://therecord.media/sec-fines-three-companies-over-hacked-employee-email-accounts/
[8] FIL-55-2021, *Authentication and Access to Financial Institution Services and Systems*, August 11, 2021http://www.fdic.gov/news/financial-institution-letters/2021/fil21055.html
[9] Standards Releases | SWIFT - The global provider of secure financial messaging services
[10] https://www.irisclasson.com/2017/10/06/not-so-stupid-question-303does-the-gdpr-require-two-factor-authentication-from-companies-processing-personal-data/
[11] Understanding New PCI Guidance on MFA (pcisecuritystandards.org)

- Systems Administration – While their business function may be related to applications, servers, network, or some other infrastructure; and their role can be related to development, operations, or second/third level support – those accounts that can modify configurations, code or data are privileged.
- Accounts that can peer into data – The typical example is a database administrator who can "dump out" unencrypted/non-obfuscated data; or a server administrator with read-only access that can peer into scripts and see credentials.
- Business Users who can modify the entitlements – Users who can change the authorizations of other users of an application (pursuant to the overall risk of the application itself).

In addition to technical users, FIs should consider the accounts that can execute certain transactions — such as money movement — or employees in positions that are prone to spear phishing attacks — such as employees with access to a privileged account. FIs should look within their cyber teams and ensure that individuals who perform credentials management, for example, require MFA to access their Identity Governance and Administration (IGA) application.

In cases where the access is privileged, the identity asserting that privilege should be proven via MFA. It is up to the organization to develop standards and regularly define what privileged access means, what level of access is afforded and under what conditions access should be revoked. For most, it could be defined as an administrator or individuals who can change configurations that could expose sensitive data.

WHEN USERS TRAVERSE NETWORK ZONES

MFA should be used when users are traversing zones. If your users are connecting remotely into your network from outside the network, that user should be required to assert their identity and MFA. If a user is communicating, connecting to, or utilizing information resources from one network zone to the next within the network, that user should re-assert their identity and re-authenticate via MFA.

In cases where users are connecting to a remote cloud solution, they should also consider leveraging MFA. See Figure 3. The New York Department of Financial Services has set the precedent for the cloud-based MFA requirement with its decision to fine First Unum Life Insurance Company of America ("First Unum") and Paul Revere Life Insurance Company ("Paul Revere") $1.8 million combined for MFA.

"The investigation uncovered, among other things, that First Unum and Paul Revere violated the DFS Cybersecurity Regulation by failing to implement Multifactor Authentication without implementing reasonably equivalent or more secure access controls approved in writing by the Company's Chief Information Security Officer."[12]

[12] https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202105131

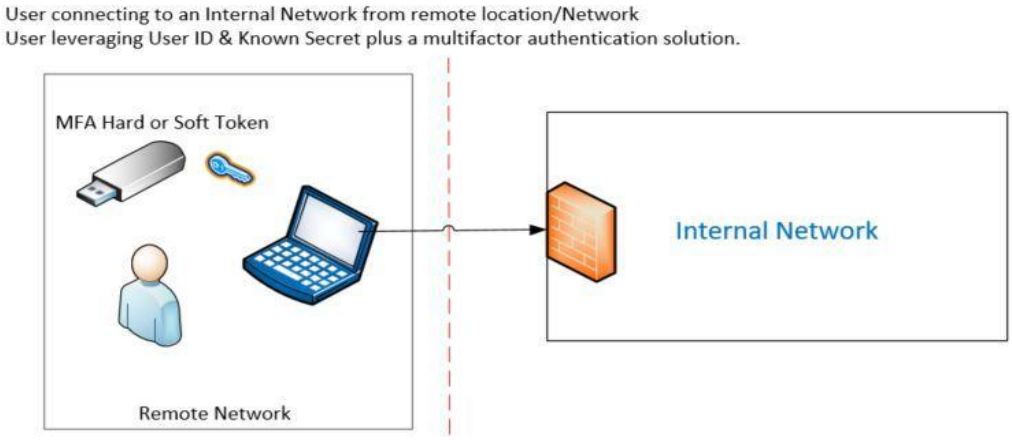

Figure 1

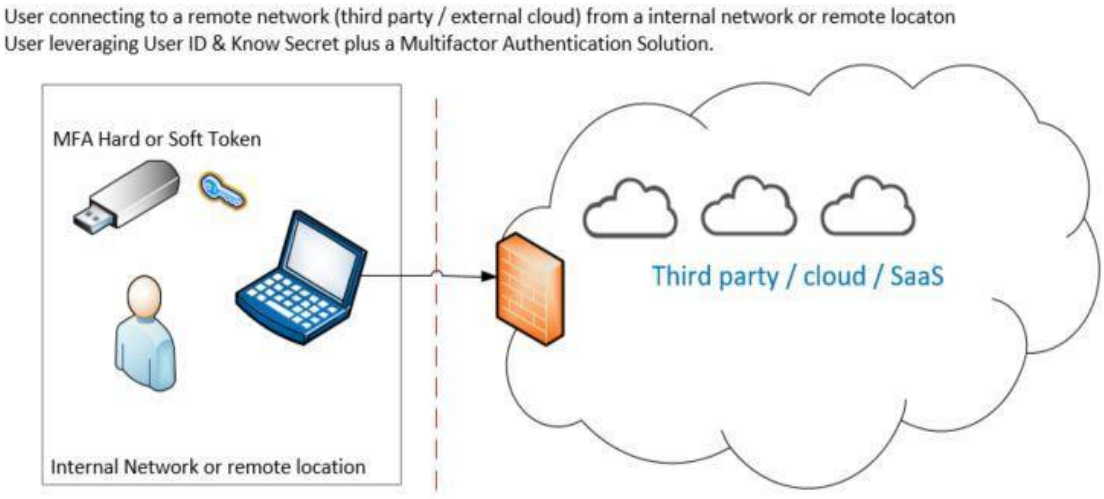

Figure 2

ADDITIONAL USE CASES AND CONSIDERATIONS

- Protecting access to sensitive data – Privileged access can also mean the type of data the identity is authorized to access. If a particular application holds highly sensitive data, an organization may require a user to use MFA to authenticate with the application. Contrast this to an application holding non-sensitive data that is accessible through either single sign-on or single-factor authentication.

  FIs should use MFA when protecting access to sensitive data or other high value applications. Many FIs will leverage MFA, and other conditional access and data loss prevention controls, to lessen the likelihood of a security breach. MFA reduces the likelihood by better preventing unauthorized access to the data because a bad actor is unable to use stolen credentials by themselves.

- Reducing Third-Party Risk – Protecting against malware installed at a third party. Most FIs leverage third parties for technical support or business process outsourcing. While most third parties must comply to cybersecurity standards prescribed by the FI, the controls are not infallible and sometimes malware is placed on the managed third-party device; or an individual at the third party is compromised via social engineering into giving up their third-party credentials.

MFA IS NOT A ONE SIZE FITS ALL

There will be scenarios where using MFA is not possible as a solution. In these cases, a risk-based approach should be employed to determine how to enhance authentication assurance in the absence of MFA. Below are some situations where MFA may not be possible.

SITUATIONS WHERE MFA CANNOT OR MAY NOT BE APPLIED

- Non-interactive credentials such as system accounts, automated service bots and one time or ephemeral passwords
- Shared accounts
- American Disabilities Act (ADA) and accessibility considerations
- Lack of end-user availability to hardware or services (mobile devices, network availability, etc.)

In these cases, the firm should consider whether to accept or mitigate the risks through other controls (e.g., time or location-based access), or to provide alternative methods for achieving the same levels of assurance (e.g., offering more than one additional factor as a choice in a multifactor implementation).

Section IV – Third-Party Authenticators

Third-party authenticators can be leveraged but the firm accepting the authentication needs to understand the controls employed to ensure they provide a high enough level of identity assurance (does the authentication being asserted by the individual confirm who they claim to be). Firms should assess the effectiveness of the control and security end-to-end and determine what level of assurance the authentication provides.

MFA solutions offered by third-party services such as Google, Microsoft, or Okta can be considered reliable and acceptable provided their offering conforms to industry standards (e.g., FIDO2[13], RFC 6238) and in combination with a satisfactory review of the third parties' security practices and policies for how they manage identities. An example of a review could be evaluating how the given provider uses information collected on the individual throughout the data lifecycle (such as brokering the data for non-security purposes). This conflict can challenge the level of trust institutions have with the authenticator. If a third party has been repeatedly breached or has been shown to be indifferent to privacy issues, this should raise additional questions.

Not all MFA use cases will demand the same level of assurance across all business use cases and populations. Customers may decide to secure their own accounts with a preferred third-party authenticator, and this may be considered acceptable to the FI. However, that same authenticator may not meet the trustworthiness standard required by an enterprise to authenticate its workforce. Administrators may need to have even more stringent requirements on what authenticators are appropriate.

The process for first verifying the identity of the individual becomes potentially more important than the provider. Identity Proofing remains the critical process for assuring the first factor, and likely the second factor, are tied to a specific human.

[13] The FIDO Alliance (Fast IDentity Online) has created a standard to enable a more seamless "passwordless" user experience that securely stores authentication information (e.g., biometric data) on the user device rather than a centralized database.

IDENTITY PROOFING

Adequate identity proofing prior to the issuance of an MFA Authenticators is a key component to establishing the level of trust necessary for any assertions of the identity going forward. The level of assurance should be implemented that will describe the highest level of assurance that authenticator can deliver. Usage of authenticators should describe how strong the tie between an actual user's claim and the authenticator must be to perform a given function. Of the four primary approaches for identity proofing (knowledge-based, identity document verification, biometric, out-of-band), knowledge-based authentication is considered the least reliable.

IDENTITY ASSURANCE

Authentication methods vary and should be assigned an assurance level. Higher assurance level authenticators can be used in lower assurance instances but not the inverse. NIST Special Publication 800-63-3 describes the requirements for the three Identity Assurance Levels (IAL)[14]. Enterprises should identify the level of IAL required for specific use cases and ensure they fit within their risk thresholds.

BRING YOUR OWN ID (BYOID)

Firms should look to reduce the friction for customers as much as possible while still providing the institution with the level of assurance it needs to meet its KYC requirements. It should be expected that customers may want to consolidate their various e-commerce accounts into a single identity that they maintain and monitor. In the broader security context, this would provide better security for both the end user as well as the institution. The assumption would be that an individual will pay more attention to anomalies to one set of credentials than they would trying to manage multiple credentials across multiple relationships.

A workforce user could also take advantage of BYOID; however, the adoption of this approach should be evaluated on security or legal requirements for the specific use case. Some parts of an organization may be less of a security concern when leveraging BYOID than others. Back-office workers, such as administrative support staff, marketing or public relations staff, who do not work with privacy, privilege access management data and processes may be able to consume BYOID. Highly sensitive areas may need additional controls and oversight in place prior to enabling BYOID.

Section V - Authentication Attribute Role In MFA

Additional attributes can strengthen the assurance of authentication requests, but are not a replacement. The use of additional attributes, including user location, behaviors and intelligence driven data are recommended but do not typically contribute to identity assurance (assurance the individual is who they say they are)

- Somewhere the User Is – Determination of the user's connection to a specific computing network, Internet Protocol (IP) address or Global Positioning System (GPS) signal to identify the user's location.
- Something the User Does – Referred to as "behavioral biometrics" which observes a user's actions or activities, such as, keystrokes, timing of access, etc. If proven to provide a high level of identity assurance, something the user does can be considered "something you are."

[14] https://pages.nist.gov/800-63-3-Implementation-Resources/63B/AAL/

- Intelligence-driven assurance – Typically consists of analysis of data to determine the likelihood of the user being authentic (e.g., impossible login – user logs in from multiple geolocations which are physically impossible to achieve). The general concept of zero trust is also an example of intelligence driven assurance. [15]

Section VI: Operational Considerations

CHALLENGES WITH MFA

The use of MFA can provide a significant amount of risk mitigation when applied appropriately. Given the potential risk reduction, it can be tempting to apply MFA wherever possible. With the proliferation of mobile services over the last decade, the use of a frictionless digital experience has expanded and become an expectation of users (ex. single sign-on (SSO), one-click checkouts and NFC/Tap&Go). When MFA is employed, due consideration must be given as to how to balance risk reduction and the friction of MFA.
This section will describe some of the challenges that need to be considered when deciding to use MFA.

ACCESSIBILITY OF DEVICES USED FOR MFA

Whether by choice or socioeconomic circumstances some users may not have access to digital resources that would allow them to leverage MFA. This includes convenient or reliable access to the internet, mobile device or documentation to enable registration for MFA.

LEGAL

Some states or jurisdictions restrict what you can mandate (e.g., use of personal devices, downloading software to personal devices, etc.) so the use of enhanced authentication, such as MFA, must ensure conformance with laws that may restrict the ability to operationalize them.

In use cases where firms are storing biometrics as an authenticator, it may introduce complexity where the right to be forgotten[16] is required or use conflicts with state or local law.[17]

INTERNAL POLICY

Other operational considerations include internal policies impacting the use of MFA. As an example, clean rooms restrict the use of personal devices, including cell phones.

USER IMPACT

User experience must also be considered when leveraging MFA. Areas that cause a high level of user friction include:

- Prompting users multiple times within a session may lead to frustration and lack of engagement from consumers;
- Lost or broken tokens or cards may lead to a delay or lack of access;
- Environmental considerations (lighting, climate, etc.); and
- People with disabilities may not be able to leverage certain types of MFA situationally (this may also have legal and compliance implications).

Optionality becomes a significant influence in the decision to deploy MFA. Any authentication deployment will impact some population of users in some way so single solution MFA deployments are likely to be problematic. Firms should consider offering more than one additional factor to reduce the likelihood of disenfranchising customers while providing higher levels of assurance.

[15] https://bpi.com/adaptive-trust-zero-trust-architecture-in-a-financial-services-environment/
[16] https://gdpr-info.eu/art-17-gdpr/
[17] https://news.bloomberglaw.com/privacy-and-data-security/first-illinois-biometric-privacy-jury-trial-ends-in-bnsf-loss

GENERAL GUIDELINES FOR ADDRESSING CHALLENGES

While these challenges may seem daunting, there are some general guidelines to help navigate them. This is not an exhaustive list but is meant to stimulate thought on how to begin to address these concerns.
Partner with the line of business to determine the relevance of U.S. export restrictions to international service provider and customer segments. This may be supported by internal policy, risk management or solution design standards. The earlier in the process these risks are captured, the easier and more cost effective it is to provide alternative solutions.

Do not revert to single-factor authentication if MFA fails or becomes unavailable. Having a single-factor authentication mechanism as a fallback negates the risk mitigation that MFA provides. To avoid having to revert to single-factor authentication be prepared to provide alternative MFA solutions for a variety of scenarios. This may include providing less preferred or higher friction MFA solutions when the preferred method is not available.
Ensure solution testing accounts for relevant use cases (e.g., people with disabilities). This is vital to ensure segments of users and consumers are not unintentionally excluded. A greater focus on this is needed from solution providers and regulators to account for instances where business may have to make decisions between compliance with security laws and regulations and inclusivity.

Consistent engagement with users of the MFA solution ensures a balance can be found between the reduction of risk and usability. Collecting data such as average time for MFA registration, dropout during authentication prompts, number of related service calls along with direct consumer feedback can help identify points of user friction.

Section VII – Conclusion

Authentication exists to ensure appropriate access to systems and assets. Historically, credentials have been relied upon to provide identity assurance; however, knowledge-based questions on their own have become less reliable. A sharp rise in data breaches, malware deployment and other criminal activity have rendered the use of single-factor, knowledge-based questions unreliable in high risk uses cases. The need for enhanced authentication in these circumstances is well supported by governing bodies and industry organizations.

However, the use of MFA should be evaluated in context of risk, legal and operational considerations and grounded in a risk-based approach rather than as a generic requirement. FI's must recognize the existence of authentication risk, assess the need for higher authentication in context of risk and employ solutions which balance the benefits of higher assurance authentication with end-user impact and operational support. Given increasing regulatory focus on authentication, FIs understand the need to document risk-based decisions, especially in for higher risk use cases where MFA cannot be implemented as a control, obliging firms to consider and employ compensating controls of an equivalent strength.

The growing existence of external authenticators and identities also provides FIs choice however the use of these identities and authenticators is critically dependent on the strength of the identity proofing process and overall cyber controls of the originating organization. Regardless of the authenticator leveraged, operational considerations become an important part of the decision equation. While these considerations do not supersede the need for risk mitigation, they play an important part in end-user impacts and should be evaluated as part of the overall decision of how and when to deploy MFA. In summary, MFA is an important part of protecting FIs and their customers against misuse of access; however, it is equally important to ground decisions in context of risk rather than a one-size fits all approach.