THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.

REMOTE AUTHENTICATION
FRAUD LANDSCAPE SERIES
AUGUST 2021

BRIEF #3:

Authentication Fraud Mitigation Approaches, Key Findings and Recommendations

OVERVIEW

This third research brief in the Remote Authentication Fraud Landscape series describes risks associated with authentication methods, as well as the benefits and challenges associated with several fraud mitigation approaches. Finally, this brief presents key findings and recommendations that the industry and the Federal Reserve should consider for mitigating remote authentication fraud.

RISKS ASSOCIATED with AUTHENTICATION METHODS

The intent of payment authentication is to protect the payment parties (e.g., customers, financial institutions or FIs, processors and merchants) and help mitigate fraud. However, all authentication methods have vulnerabilities that may create different levels of risk depending on the type of transaction, merchant and payment method. Here are some of the risks associated with different authentication methods.

Username and password

Passwords simplify the customer experience. They are easy to use, require no extra hardware, have no compatibility issues and are inexpensive to implement. However, they are also the most vulnerable authentication method, with high risk of compromise. Many passwords are changed infrequently – typically no less often than every 30 days – or not changed at all if this is not required by the provider. They are not encrypted when passed from the customer device to the FI or payment service provider (PSP), and are subject to man-in-the-middle (MiTM)[1] attacks. Additionally, traditional methods of entering a password or responding to additional security questions are not tamper-proof, as information is often misspelled, forgotten or stolen.

The increasing number of passwords used per person across multiple websites or apps creates further vulnerability. Almost every website or mobile app still requires a username and password. Because remembering so many passwords is difficult, many users repeat the same username and password across locations. This allows the fraudster to use a stolen or breached password to access multiple accounts.

While other methods, such as device biometrics (i.e., face or fingerprint verification), are replacing passwords, many FIs, payment providers and merchants still enable passwords as a backup authentication method. Biometrics do not replace passwords, which remain available as an authentication method, thus diluting the security provided by biometrics.

1 Man-in- the-middle (MiTM) attack: perpetrators position themselves in a conversation between users and an application – either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is under way. The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically users of financial applications, software as a service or SaaS businesses, e-commerce sites and other websites where logging in is required. Information obtained during an attack can be used for many purposes, including identity theft, unapproved fund transfers or illicit password changes. Man in the Middle (MITM) Attack

For example:

- Browser-based access to bank account: password is saved and auto-populated; source is a trusted device if customer opts in
- Mobile-based access to bank account: biometric and trusted device, password is a backup
- Pay wallets: biometric and trusted device, password is backup
- Third-party PSP: saved password or biometrics, trusted device if customer opts in
- Online merchants: varies. Some still accept username/email and password

A 2020 FICO authentication study[2,3] found that a large percentage of Americans do not take the necessary precautions to secure their information online. For example, 17% of U.S. respondents reuse between two and five passwords across multiple accounts and 4% use one password. The same FICO study found that just 23% of respondents use a password manager, which is a software application that stores and manages encrypted user passwords for multiple online accounts and provides secure access to all password information with a master password.[4] The study also reported that 30% still use high-risk practices, such as writing down their passwords. It's likely that non-users may not be aware of password managers and their benefits. Alternatively, 20% to 53% of survey respondents would consider using some type of one-time passcode (OTP) or biometric to secure their financial accounts. Statista[5] found similar results in its survey of 1,200 U.S. adults (age 18+) about their use of passwords in October 2018.

Finally, while various security solution providers offer their perspectives on best practices for passwords, there are no common standards or guidelines across the financial services industry. Each provider – issuers, networks, merchants and PSPs – establishes its own formats and requirements.[6]

Personal Identification Number (PIN)

Consumers and other payments stakeholders seem to use PINs to prioritize convenience over security. Typically, consumers use PINs for ATM, debit card and debit mobile transactions, for which some merchants may require a PIN after authenticating with a biometric fingerprint. The only universal requirement for a PIN is that it contains four to six numeric characters. FIs do not review new PINs to make sure they are not replicating the customer's Social Security number, date of birth or other personally

2 United States Identity Authentication and Your Customers – Survey Results

3 FICO Survey Reveals U.S. Consumers Need to Better Protect Themselves When Banking Online May 13, 2020

4 For more details, see Password Manager.

5 Use of same online passwords, Statista, Oct 2018 Survey of 1,200 US adults, 18+. Use same password for: all accounts (6%); most accounts (20%); some accounts (45%); none (20%); don't know (7%).

6 Organizations that list some best practices for strong passwords include: Digital Identity Guidelines and Small Merchant Guide to Safe Payments. 2018.

identifiable information (PII). Some non-bank payment and wallet providers do not edit PINs to prevent using repetitive (e.g., 0000) or sequential digits (e.g., 1 2 3 4). PINs that change infrequently or are too short, basic or easy to guess are more susceptible to fraud. Despite this, some payment providers allow customers to create weak PINs, and some mobile phone providers do not require a PIN to open the device, potentially enabling fraudsters to access payment apps on stolen devices.

Knowledge-based Authentication (KBA)

KBA is an authentication method used to confirm the customer's identity. The customer answers a series of questions that are verified using queries to credit bureaus and third-party databases. The customer selects some questions ahead of time or responds to personal questions based on public data. This can create friction because it requires customers to take extra time to remember and answer such questions (e.g., not everyone remembers the year, make and model of their first car). It has become relatively easy for fraudsters to obtain KBA data through publicly available channels, social media and the black market due to large-scale data breaches and oversharing on social media. Fraudsters may use this information to reconstruct customer identities, which they use to answer KBA questions posed by FI customer service representatives to gain access to legitimate bank or credit card accounts. However, the availability of stronger authentication methods that also minimize friction is enabling FIs to move away from KBA.

All authentication approaches have vulnerabilities – and strengths. Two-factor authentication can add friction but is very effective at blocking attacks by bots or hackers.

Two-factor authentication (2FA)

Two-factor authentication can add friction to the customer experience because it requires additional actions from users at sign-up and login. However, 2FA is very effective at blocking attacks by bots (an autonomous program on the internet or another network that can interact with systems or users), helping to verify identity and protecting customer accounts from hacking. Research found that an SMS code sent to a recovery phone number could block 66% of targeted attacks, 99% of bulk phishing attacks (a form of social engineering that uses email, phone or text to entice individuals into providing personal or sensitive information) and 100% of automated bots.[7]

There are risks associated with 2FA. For example, users receive a phishing email asking them to access and log in to their bank accounts, but the phishing email contains a link to an intermediary site that looks like the actual bank's website. Users click into

7 J. Wagner. "Balancing Fraud Prevention with Welcoming New Customers." CNP.com/Ekata, February 6, 2020.

the phishing site and enter their usernames and passwords, plus the 2FA code. The phishing site then uses the two data points to log into the FI website as the authorized customer. Because the legitimate user "trusted" the phishing site and entered his or her credentials, the second factor was rendered useless.[8]

One-Time Passcode (OTP) and Push Notifications

The proliferation of OTPs communicated via text messages as a confirmatory factor risks, creating a false sense of security in customers. While OTPs provide an additional layer of authentication to help prevent account takeovers, there are growing concerns that they are becoming increasingly vulnerable to compromise from MitM attacks.[9] Although OTPs are not reusable, they can be stolen, usually through social engineering via a phishing email, or by intercepting the communication sent to the mobile device.

Consumers are reluctant to adopt more secure app-based solutions, such as in-app push notifications, because they require more complex security processes. It is also important to note that in-app push notifications are vulnerable if the device is lost or stolen and the application is compromised.

Physical Biometrics

Biometrics link proof of identity to a person's physical characteristics and behavior patterns. Once obtained and mapped, the biometric data is stored for use in future access verifications. Most of the time, this data is encrypted and stored within the device or in a remote server. By definition, it is more difficult to steal or impersonate biometrics than a password or key, and biometrics cannot be lost or forgotten since they are always with the person. Any biometric (fingerprint, face, iris, voice) can be used to onboard and subsequently, authenticate customers, who also have become more familiar and comfortable with unlocking their mobile phones with either a fingerprint or face scan.

Organizations need to be careful about how they implement their biometric authentication systems to avoid infringing on customer privacy or improperly exposing sensitive information. False positives and false negatives can occur, which could affect a customer's experience and level of trust with the provider. For example, a facial recognition system might not recognize a user wearing makeup or glasses. An individual's voice may vary based on time of day, health, etc. A fingerprint or retinal scan, however, is immutable and the release of this or other biometric information could put users at permanent risk since they cannot change their fingerprints or faces.[10]

8 Two-Factor Authentication Is Not Secure: The Benefits and Risks of Various 2FA Schemes. September 2019.

9 NIST has stated that using SMS 2FA is risky.

10 What is biometrics? 10 physical and behavioral identifiers that can be used for authentication

Fraudsters could hack private or public databases containing PII and fingerprints. Stolen fingerprints create opportunities for identity theft. Because customers maintain control of their mobile devices, storing physical biometric data on devices, such as iPhone TouchID or Face ID, is more secure than storing it with a service provider, even when the data is encrypted.

A service provider or other third party may use biometric data captured during enrollment for purposes other than those agreed to by the customer. If fraudsters capture the data during transmission to the provider's central database, they can replicate it in other transactions and the biometric is no longer solely in the user's control. While the risk is similar to that of a password database, the ramifications are significantly different. A compromised password can be changed. Biometric data remains the same forever.[11]

Authentication strategies usually incorporate multiple approaches.

AUTHENTICATION FRAUD MITIGATION APPROACHES

Overview

Fraud mitigation approaches have evolved over time and continue to evolve as fraudsters develop new capabilities. Authentication strategies usually incorporate multiple approaches, but organizations choose approaches that fit their strategy, so they are not uniform across the industry. The 2017 National Institute of Standards and Technology (NIST) Digital Identity guidelines provide clear direction for identity proofing and authentication protocols, but these have not yet gained wide industry adoption. Most approaches can support multiple payment use cases but may have different levels of effectiveness to recognize fraudsters, reduce fraud rates or minimize customer friction, depending on how they integrate into an organization's fraud prevention strategy. Organizations' level of sophistication, preferences and tolerance for risk and trust, as well as magnitude of the fraud, help determine their fraud strategies. Beyond security considerations, organizations also must factor in the cost and complexity of implementing new fraud strategies, positive and negative impacts on customers and reputational risk.

11 What is Biometrics Security. October 7, 2020.

Mitigation approaches and enabling technologies support and/or enhance the authentication methods described earlier. They can be used as additional checks on the validity of the user or payment method through collection, analysis and review of additional data provided over time from previous activity, combined with other data sources about the customer, payment method, channel and location. Fraud mitigation approaches are progressing from transaction-centric – i.e., applying static rules based on historically observed fraudulent behavior – to user-centric, where authentication is a continuous and frictionless measurement of expected normal behavior on a user's device that does not rely on passwords and KBA. The present landscape is a patchwork of layered, multi-factor and risk-based authentication approaches, which require two or more factors from knowledge (something you know), ownership (something you have), and/or inherence (something you are: including fingerprints, facial scans, voice prints, retinal or iris scans, or similar biometric identification systems).[12]

Machine learning enables systems to automatically learn and improve from experience without explicit programming to "teach" the rules.

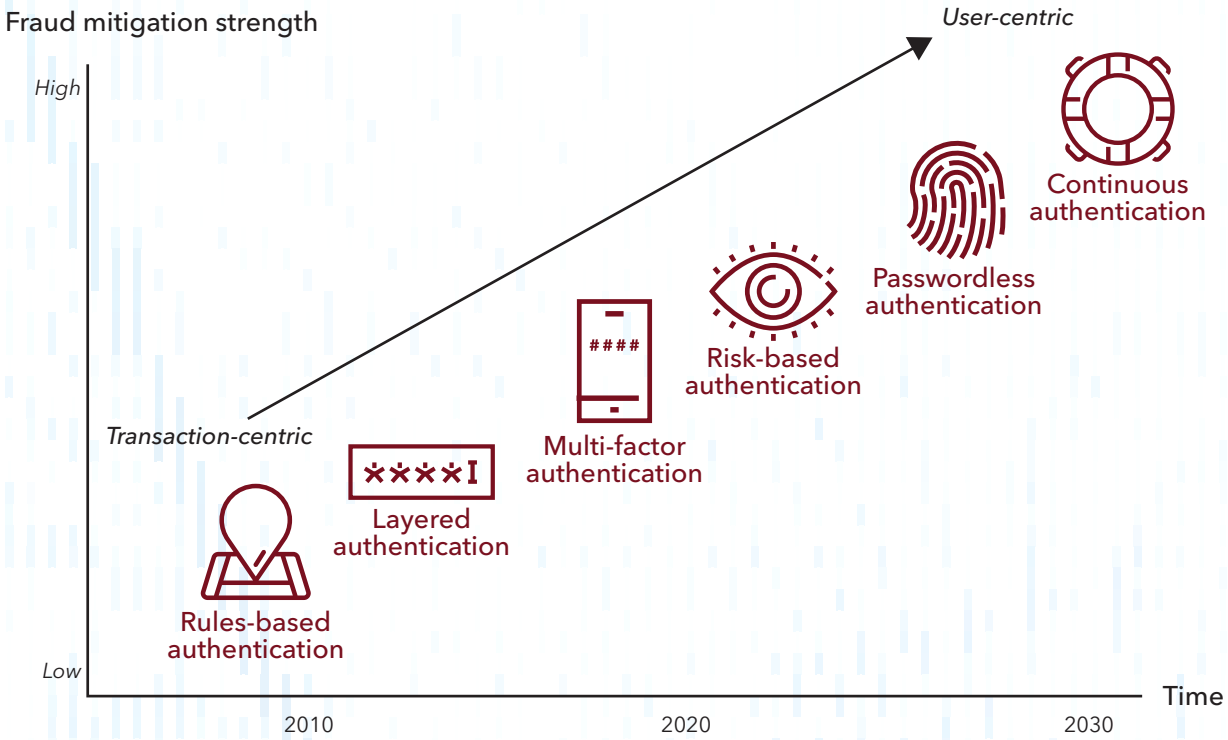
Authentication methods will continue to overlap, but the significance of each method in the overall authentication landscape will likely shift over the next several years. For example, rules-based authentication with manually coded rules may gradually move from being a dominant method to one that supports machine learning. Machine learning (ML) enables systems to automatically learn and improve from experience without explicit programming to "teach" the rules. It applies to all technologies and approaches, but how it is used can vary. Machine learning incorporates rules and Know Your Customer (KYC) protocols to automate manual processes (e.g., Suspicious Activity Reports or SARs) to increase efficiency and reduce costs. For fraud mitigation, ML takes a more predictive and preemptive approach by analyzing vast amounts of data from large user groups.

Until a decade ago, the payments industry's primary authentication approach emphasized the risk associated with the nature of the payment transaction itself. Rules were written to flag transactions that might, for example, take place at an unusual time of day, from an atypical location, or be an unusual amount. Since then, fraudsters' capabilities to circumvent rules have grown exponentially, increasing fraud risks. Moreover, fraudsters expanded their attack surface to account owners through impersonation, social engineering and use of stolen credentials.

12 Understanding Multi-Factor Authentication: 3 Ways It Can Benefit Your Business

Figure 4 represents the authors' view of how current authentication approaches and enabling technologies may evolve over time.

Figure 4: Possible evolution of current authentication approaches and enabling technologies

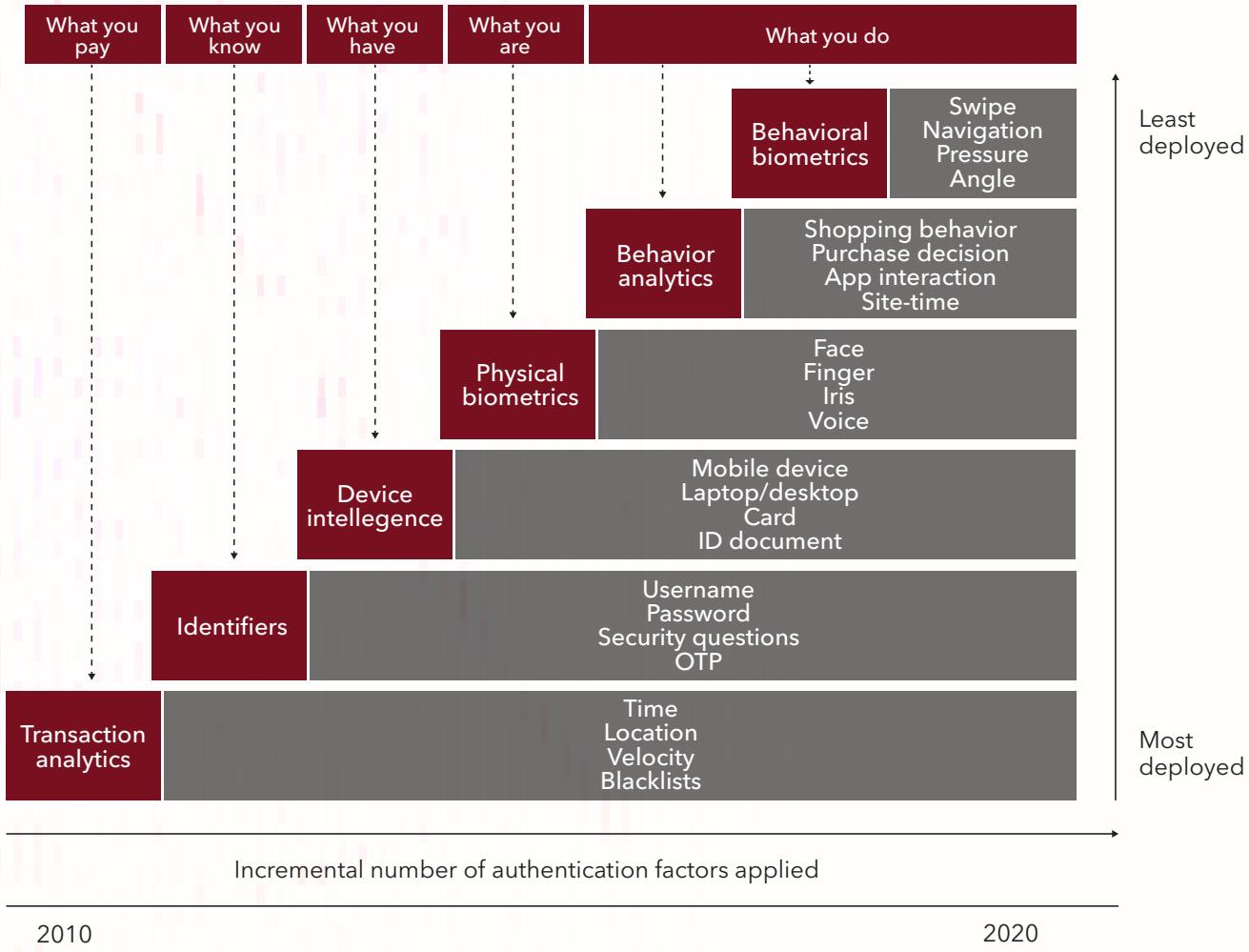


New authentication approaches have been launched in rapid succession. Each one is more focused on the identity of the user and the devices they use to conduct transactions. These approaches seek to minimize friction while maximizing security commensurate to the identified risk. In practice, however, organizations do not replace one approach with another, but tend to add a new approach to their existing capabilities.

The strongest defense against fraud is multi-factor authentication (MFA). However, each new approach can add incremental costs associated with purchase, integration, training, education and potential customer friction. This can slow down the adoption of successively more effective solutions. The result is a fragmented marketplace, which plays to the advantage of fraudsters.

Figure 5 breaks down technologies that can be associated with the approaches in Figure 4.

Figure 5: Stronger mitigation can create implementation complexity and market fragmentation



Rules-based authentication

Rules-based systems rely on pre-programmed rules to identify changes in user behavior or predict outcomes. FIs, payment providers, merchants and other payments stakeholders manually create a pre-defined set of options or static binary rules to assess whether or not to approve payment transactions. The rules are based on analysis of the customer's historical fraud patterns and other environmental factors. Rules may be set for dollar amounts, currency, date/time of transaction, card type, transaction location and other factors. For example, a spike in fraud attempts originating from an IP address in a foreign country may result in a rule to flag all transactions from that country for further review.

Fraud rules leverage knowledge gained over time about the characteristics of both fraudulent and legitimate transactions to automate the authentication processes. These rules are static in nature and therefore, only effective in detecting known frauds. The effectiveness of the system can increase as it adds more rules. However, the system's effectiveness also depends on the expertise of people who analyze, create and update rules, as well as the availability of data needed for analysis. If the data is not available, tweaking or adding new rules is challenging.

Minimize false positives by looking at transactions in a broader context.

To minimize false positives, it is necessary to look at transactions in a broader context, not just based on the outcome of a rule. In some cases, the decision to accept or decline the transaction may depend on the percentage of good transactions captured with the rules versus false positives, or if suspicious transactions are sent to a "yellow path" for review before being rejected. However, organizations have different risk levels, and some may reject every transaction above a certain risk threshold because it is less costly to lose a sale than have a fraudulent transaction. For example, high-value orders and orders from high-risk locations are more likely to be fraudulent. But if the rule blocks all transactions over $500 or every payment from a risky region, it can cause good customers to abandon their purchases. Because false positives also affect longer-term customer relationships, rules-based manual reviews are most effective as a last line of defense in a fraud detection strategy.

Finally, rules-based systems are not adaptable to an evolving and highly disrupted industry such as financial services, which requires a more agile, flexible platform to overcome fraud challenges.

Benefits

- Rules-based authentication is very specific, as it provides a straightforward binary (yes/no) response.[13]
- The organization developing the rules has full control over the logic behind the rules and how and when to apply them.
- When combined with machine learning, a rules-based system can cover a wide attack space.[14]

13 Rules-based payer authentication is a type of rules-based authentication. Instead of providing a yes/no decision whether to accept a transaction, it provides a set of configurable rules to provide merchants with the option to invoke RBA/3DS or not.

14 What is Continuous Authentication? 2021.

Challenges[15]

- Traditionally, businesses have relied on rules to block fraudulent payments, and rules are still an important part of the anti-fraud toolkit. Rules must keep up with frequently changing fraud patterns, which is a manual, resource-driven and costly process. They are not very scalable and can become more expensive to maintain as the customer base and number of rules increase to keep up with fraud. This can further increase maintenance and the number of manual reviews performed by the fraud analyst team.
- As fraudsters become more sophisticated, it is harder for the organization to react quickly to create new rules, which require changes, testing and implementation. If rules are not updated, added or deleted in a timely way, they can become less effective and let more fraud into the system, making organizations more vulnerable.
- Merchants and FIs can only implement rules based on the data they have, because rules cannot self-learn or react in real time to detect and react to subtle changes in fraud patterns. This limits the organization's ability to proactively predict industry fraud patterns and adjust to mitigate unknown or evolving fraud trends.
- As more detected fraud schemes translate into rules, it may become more difficult for rules-based systems to keep up with analyzing the data. Fraud thresholds for a financial service or payment business can change over time as organizations adapt to new products and services or shifts in customer mix, which can make the rules invalid and require more frequent updates.
- Writing rules is an internal process customized to the threats an organization faces. FIs may share threat intelligence, but not rules. The ability of internal fraud teams and data scientists to devise mitigating rules can translate into a competitive advantage (i.e., the organization is more trusted by its customers) but does not contribute to systemic industrywide mitigation. We recognize that organizations develop their own rules, but this constitutes a potential industry weakness. Fraudsters constantly test authentication practices at individual organizations through automated attacks to find the weakest targets by determining which organizations have not yet implemented a rule that prevents a particular form of fraud.

Risk-based authentication enables issuers to analyze and separate good transactions from those suspected of fraud.

15 Rule-Based vs. Machine Learning: Effective Fraud Prevention. November 2019.

Risk-based authentication (RBA)

Risk-based authentication enables issuers to analyze and separate good transactions from those suspected of fraud. Issuers can then limit their challenges to transactions suspected of fraud. RBA measures risk associated with user login and post-login activities based on a pre-defined set of rules and data about a user's location, device, IP address, login patterns and other risk indicators. These are fed into a model to calculate a real-time risk score for any access attempt. The risk score determines the risk level at which a login attempt appears to be legitimate or fraudulent.

Based on the probability that the transaction is fraudulent, RBA dynamically adapts to the circumstances and presents the issuer with authentication options appropriate to that risk level. If the risk score exceeds the risk level that the issuing bank (or merchant) is willing to accept, it triggers step-up authentication. If the model does not register a threat, the transaction will be approved automatically without additional (i.e., step-up) authentication. RBA's adaptive and contextual nature lends itself to a layered or multi-factor authentication (MFA) approach.

Benefits

- Providing FIs with the ability to proactively detect signs of ATO before it impacts the customer.
- Creating a risk score to enhance MFA enables FIs and merchants to find a balance between security and the customer experience by limiting step-up authentication to high-risk situations or use cases.
- Applying predictive learning helps the risk score become more accurate as RBA accepts more inputs.
- Examining a wide variety of inputs across channels enables providers to make real-time decisions about the precise level of authentication security required for each transaction.

Challenges

- Through targeted testing and attacks, sophisticated fraudsters can detect and understand how fraud prevention systems calculate risk scores. If they know which data elements influence the score more than others, they may attempt to manipulate particular data elements to keep the score low.
- It is not an exact science to determine whether to approve or decline an order or other financial transaction through manual review or based on a risk score. For example, if the rule is to decline every transaction with a score below 12, how should a transaction with a slightly higher score (e.g., 12.14)

be treated? The threshold constantly needs adjusting, and some transactions will inevitably fall close to the set threshold. The response to scores slightly above or below the threshold will vary by merchant or payment provider based on how well they know their customers.

- Since risk scores only provide recommendations, manual teams must review them to decide whether to accept, decline or require step-up authentication for a transaction. Using a manual team to review only the high risk or "gray area" transactions can magnify human error or bias.[16]

Passwordless authentication

Passwordless authentication verifies users' identities without passwords or any other memorized secret information. Instead of passwords, identity is verified based on an object that uniquely identifies the user: e.g., OTP, registered mobile device, mobile app (such as OneLogin Protect[17]), a hardware token (such as YubiKey[18]) or an "inherent factor" (such as a person's biometric signature via fingerprint, face or retina).[19] The mobile app or e-commerce website to which the user is authenticating is agnostic about the verification path.

Passwordless authentication removes password vulnerability by using a more secure authentication factor stored securely in the device and not shared with anyone but the user. If the passwordless authentication is device-based, it matches consumers' mobile devices to the device information registered with their wireless carriers, which helps to secure logins and transactions. If a fraudster gains access to a customer's mobile phone, they cannot gain access to PII and financial or account data because the data is protected by the customer's locally stored biometric.

Passwordless authentication relies on the FIDO2[20] standard. FIDO2 is an open authentication standard designed around public key cryptography. It enables passwordless single-factor authentication, where the login is backed solely by local authentication and biometrics. It encompasses W3C's WebAuthn[21] and FIDO's CTAP[22] standards.

FIDO2 is a considerable departure from incremental authentication approaches, such as rules-based, multi-layered, MFA or RBA, to counter the vulnerability of the

16 Riskified, What You Can Gain by Partnering with a Fraud Prevention Vendor. April 2020.

17 OneLogin Protect is an OTP mobile app generator. Single sign-on (SSO) with OpenID Connect allows customers to sign into applications without a password. SSO strengthens security and reduces friction during the sign-in and registration process. Once authenticated, customers can seamlessly sign into any application that has a trust relationship with OneLogin.

18 YubiKey is a hardware authenticator for strong single-factor authentication, MFA and touch/tap (i.e., biometrics). Protect your digital world with YubiKey

19 Zenkey is a new mobile device-based passwordless authentication method developed by ATT, Verizon and Sprint/T-Mobile to enable login to apps without creating a new account or password. The mobile phone authenticates an identity, using Customer Proprietary Network Information (CPNI) data elements, such as mobile phone number, account tenure, phone account type, SIM card details and IP address. Zenkey replaces SMS when consumers use their mobile phones to verify their identities. It is unclear whether any FIs or businesses have implemented Zenkey.

20 The FIDO (Fast Identity Online) Alliance is an industry association that provides open and free authentication standards to help reduce reliance on passwords, using the universal authentication framework (UAF), universal second factor (U2F) and FIDO2 protocols. The association has about 300 members representing vendors, big tech, FIs, government, telecom, insurance and others. FIDO is addressing the "trust in authentication" issue. Other organizations and associations – including NIST, ISO, FATF, W3C and ToIP (Trust over IP foundation) – are approaching the issue from their vantage points.

21 W3C WebAuthn is an API that enables servers to register and authenticate users with public key cryptography instead of a password in web-based applications and services.

22 CTAP (client to authenticator protocol) is a communication protocol to connect to FIDO authenticators.

password, although it uses elements of each. In a way, the "username + biometric + device" concept can be viewed as the password for remote authentication. However, broad industry support for this standard needs to occur to gain traction in adoption and synchronize the many mitigation approaches.[23]

Benefits

- Addresses consumer negligence: Some consumers may be unwilling or incapable of taking security measures to protect themselves from identity and password theft. Passwordless authentication removes the password as a fraud vector by eliminating the need for the consumer to remember it.
- User control: The consumer chooses the authenticator tool to create the keys and authenticate identity.
- Stronger security than user-controlled passwords because it removes the vulnerability that large data breaches present for passwords by storing payment credentials locally instead of in merchant databases. It also eliminates a fraudster's ability to obtain passwords on a massive scale through a single attack.
- Biometrics render social engineering and phishing useless because consumers register their biometrically enabled devices at enrollment and establish a key "handshake" for any purchase.
- Passwordless authenticators protect users from MiTM, MiTB and other "replay attacks" that target passwords.
- Data protection: authentication data is never stored in the provider's file.
- Better user experience (UX): Passwordless authentication eliminates the need for customers to create and remember passwords for all their accounts or enter them for every login. The process is more secure, logins are easier and data can be accessed from anywhere on the web.

Challenges

- The FIDO2 standard addresses authentication for an initiated transaction but does not cover credential enrollment and account recovery.
- Not all devices support biometrics and FIDO capabilities.
- Unless the industry can eliminate passwords on the back end, passwordless authentication will not achieve the efficiency and cost savings associated with the reduction of password management or eliminate all related security threats.

23 For example, while Apple's February 2020 endorsement showed the company's desire to coalesce around the FIDO2 standard, full consumer adoption may take several years.

Continuous authentication

Continuous authentication provides ongoing identity confirmation and cybersecurity protection. By constantly measuring the probability that individual users are who they claim to be, continuous authentication validates the user not just once, but nonstop throughout an entire session. Continuous authentication applies machine learning and other factors, including behavioral patterns and biometrics, to furnish smart, secure identity verification without causing friction in the banking/payment transaction process. It verifies a consumer's identity at every touchpoint by using multiple, diverse sources of PII to identify potential fraud before a transaction starts or a payment is sent.

Behavioral biometrics are the strongest component of continuous authentication because this method assesses how an individual interacts with the device. This pattern of interaction is unique to the user and cannot be replicated (as opposed to physical biometrics, e.g., fingerprint or facial recognition, which can be copied and replayed).

An application with continuous authentication functionality can continually compute and modify an "authentication score" to determine how certain it is that the account owner is using the device. Depending on the score, the user might need to input additional information, such as a password, card or fingerprint.

Continuous authentication signals a fundamental change from authentication as an event to authentication as a process. However, stakeholders should view it as a supplement to – and not a substitute for – MFA. MFA confirms that the person trying to access a remote banking or merchant app, or website is who he or she claims to be, but an MFA solution does not re-verify a user's identity once a session begins.

Benefits

- Continuously authenticates the user to prevent ATO through malware, bots, aggregators, remote access Trojans and some social engineering schemes
- Limits the impact and likelihood of payment credential compromise, data breach and sabotage using proven behavioral biometric algorithms
- Provides a smooth and uninterrupted mobile/digital user experience, reducing customer friction and session abandonment
- Provides a more accurate RBA risk score that reduces friction-related costs caused by false positives and step-up authentication
- Supported by several existing technologies, including Face ID and fingerprint readers in smartphones

Challenges

- Low awareness and adoption of continuous authentication approach
- Potential privacy and compliance concerns related to behavioral analytics and biometrics
- Risk of potential harvesting of behavioral biometric data by social media applications
- Absence of interoperability standards complicates exchange of authentication score(s)

Enabling technologies

Enabling technologies can increase the performance and effectiveness of the mitigation authentication approaches previously described. Organizations need to recognize that full or partial integration will benefit their overall security posture, but costs associated with design, implementation and training can be significant.

Behavioral analytics

Organizations study available data from payment processors and credit card networks to gain insights on the purchasing behaviors of large groups of consumers to build individual profiles. When suspicious or non-typical behavior occurs, the system flags it as a potentially fraudulent transaction.

Behavioral analytics focus on understanding how and why consumers act to enable accurate predictions about how they are likely to act in the future. It also can uncover patterns in behavior to identity what is normal, and what might be evidence of intruder compromise, insider threats or risky behavior on a network. Analytics focus on transactional behavior, which detects when a consumer completes a transaction out of pattern compared to normal behavior; and navigational behavior, which detects if the way a consumer navigates the website is inconsistent with his or her usual behavior or could indicate bot navigational patterns. The latter is also known as behavioral biometrics, covered below.

Behavioral analytics use machine learning (ML) to understand and anticipate behaviors at a granular level across each aspect of a transaction. Profiles track information that represents the behaviors of each individual, merchant, account and device. The profiles are updated in real time for each transaction to compute analytic characteristics that provide informed predictions of future behavior. Profiles contain financial and non-financial transaction details. Non-financial actions may include change of address, request for a duplicate card or a recent password reset. Financial transaction details show patterns that may represent an individual's typical spend velocity, when he or she tends to transact, and the time period between

geographically dispersed payment locations. Profiles are very powerful as they provide an up-to-date view of activity that can prevent transaction abandonment otherwise caused by false positives.

Benefits

- Differentiates between actual fraud and activities that appear suspicious but are ultimately legitimate, which minimizes false positives and reduces customer friction
- Automatically monitors all activity in real time for every account holder
- Detects early stages of a fraud attack, i.e., before a transaction is initiated, which makes prevention easier and less costly
- Supported by FIs and specialized fraud vendors with years of experience developing highly effective tools and algorithms to detect transactional fraud and anomalies
- Does not require prior knowledge of the specific fraud that the perpetrator is attempting

Challenges

- Ability to distinguish good behavior that typically precedes authorized access from bad behavior and therefore, unauthorized access to avoid false positives.

Behavioral biometrics

Behavioral biometrics analyze the way users interact with their mobile or computer devices for remote purchases and digital banking. It works behind the scenes continuously, to identify potential automated actions or fraudulent activity by an imposter, to ensure that only the legitimate person is using the device. It compares the information to a previously developed user profile, or "behavior fingerprint," to authenticate the customer continuously throughout the entire digital banking or payment session. It recognizes, measures and analyzes behaviors and physical patterns of an individual that uniquely determine their identity, from the way he or she holds the mobile device, to finger pressure, swipe patterns, keystroke dynamics and more. Examples based on pattern recognition include vein flow,[24] gestures, keystroke analysis, heartbeat and motion analysis. It also can look at the user's navigation behavior in the application and on the device, examining their typical speed of browsing and accuracy of movement. Behavioral biometric data can also combine with server-side analytics, enabling the financial institution to draw insights from data collected from different sources, including consumer groups, events and third-party partners.

24 Vascular biometrics capture vein patterns inside the skin to identify a person. Individuals present themselves for identification by inserting a finger or palm into a device that shines near-infrared light on their hands. Vascular biometrics for enhanced identification and security

Behavioral biometrics work behind the scenes by continuously comparing user behavior to a previously developed user profile.

All payment stakeholders – financial institutions, card networks, processors and merchants – can add behavioral biometrics to their fraud controls, but the rationale for each is different. For example, a major retailer[25] recently added typing authentication logic to point-of-sale employee login screens, where it captured the typing pattern, confirmed the consumer and consumer group, and validated and authenticated the consumer. If the first attempt fails, the consumer must re-authenticate. This second attempt prevents a consumer from pasting a response and using a plug-in that may pre-populate the desired fields. While this example represents a cashier logging in, the concept of preventing automated account access could apply to customer situations where the intent is to screen out bots and impersonators prior to submitting the transaction to 3DS risk-based authentication.

Benefits

- Self-learning algorithms increase confidence in the accuracy of predicting expected behavior
- Process is non-intrusive and frictionless because it works in the background
- User behavior is monitored from login to logout to detect suspicious activity
- Behavioral data is protected because it is converted to a mathematical representation within the customer profile, which is meaningless to criminals
- Existing hardware collects behavioral biometric data, needing only software for analysis, unlike some types of physical biometrics. This capacity simplifies the behavioral biometrics process and reduces implementation costs

Challenges

- Fraudsters have the ability to harvest biometric behavior data through non-payment apps, e.g., gaming apps. When combined with PII obtained through data breaches or social engineering, they can mimic a legitimate user's behavior and nullify biometric behavior tools implemented in financial apps.
- Behavioral biometrics currently monitor and analyze a consumer's behavioral patterns without their knowledge or consent. Recent regulations, such as the

25 Case study - Sears Hometown and Outlet Stores

General Data Protection Regulation (GDPR) in the European Union (EU), have recognized the potential privacy risks. Organizations contemplating behavioral biometrics should be aware of the developing rules for the technology under GDPR, as well as emerging regulations in the United States.

Artificial Intelligence/Machine learning (AI/ML)

Artificial intelligence (AI) and machine learning (ML) can help FIs dramatically reduce payment fraud. They can better detect the number of new accounts opened with stolen identities and protect consumers against synthetic identity fraud or ATO. Machine learning refers to analytic techniques that learn patterns in datasets without human support. Artificial intelligence refers to the broader application of specific kinds of analytics to accomplish tasks.[26]

Machine learning gathers information about standard behavior or practices and builds models that use sophisticated algorithms to check the integrity of the payment instrument (account, card) and transaction (amount, origination, timing, frequency). Sophisticated algorithms create a risk score that provides fraud reviewers with context for each transaction. The risk score enables them to approve a higher number of legitimate orders with fewer false positives and recognize fraudulent behavior. If the model detects anomalies, it may invoke other tools to validate the identity of the account owner.

Advanced systems are not limited to finding anomalies but, in many cases, can recognize existing patterns that signal specific fraud scenarios. There are two types of machine learning approaches commonly used in anti-fraud systems: *supervised* and *unsupervised*. Both ML approaches function independently or can combine to build more sophisticated anomaly detection algorithms.

Supervised learning uses labeled historical data to train an algorithm. In this case, existing datasets already have target variables marked, and the goal of training is to make the system predict these variables in future data. Unsupervised learning models process unlabeled data and classify it into different clusters to detect hidden relationships between variables in data items.

Choosing the right machine learning method depends on the problem set, size of a dataset and resources. Often, multiple models work together to streamline assessment and achieve higher accuracy. For example, PayPal[27] used multiple models as early as 2015. The company separated suspect transactions from ordinary transactions, then processed suspicious transactions through three models comprising a linear model, a neural network and a deep neural network. The three models then "voted" to arrive at a result with higher accuracy.

26 Mastercard Brighterion survey, 2020.

27 How PayPal beats the bad guys with machine learning

Benefits

- Detects fraud in real time and automatically creates mitigation rules
- Uncovers hidden correlations
- Automates manual tasks, i.e., coding fraud rules, which may accelerate reduction of false positives and associated costs
- Provides data to predict acceptance, decline and manual review rates, as well as to reduce fraud costs. For example, if an FI understands the decline rates, it can better control the number of fraudulent transactions identified
- Centralizes how acquiring banks track their merchants' customer activity in real time and continuously assess compliance risk and exposure

Challenges

- Quality of the data that ML uses to detect fraud is critical and requires data science expertise. It also depends on the effectiveness of the data curation process – how well the data is organized and integrated. Data tagging and labeling is time-consuming, costly and inconsistent due to the lack of common fraud definitions.
- To train the models, machine learning needs large and carefully prepared trained datasets, as well as some features of rule-based engines, e.g., checking legal limitations for cash transactions
- Machine learning models require continuous updating through testing and evaluation to detect evolving fraud patterns. This can result in a decrease in the model's performance and efficiency
- Fraudsters can leverage ML to deflect fraud defense mechanisms

Link analysis

Link analysis is a technique used to assess and evaluate connections between data. It creates a graph of all available consumer data points, such as emails, phone numbers, device IDs or payment methods and how they are connected in a network. With the help of AI/ML, suspicious connections can be detected in real time. It can be a powerful tool to identify patterns and trends and drastically reduce the time and effort required to expose patterns indicative of synthetic identities, ATO, money laundering and many other criminal activities by identifying hidden connections and relationships in a dataset that are otherwise hard to spot.

In one example, criminal investigators are able to draw more precise conclusions through the visual analysis of connections. Investigators can use link analysis tools to analyze immense volumes of data by rapidly filtering and examining data streams and databases and uncovering connections between entities and accounts, then visually displaying the resulting networks to uncover suspicious or fraudulent activity and accelerate arrest and capture.[28] In another example, Ravelin has seen fraud networks showing account takeovers where more than 10,000 customers appear to be sharing one single device.[29]

Mitigation summary

Each organization has to develop a mitigation strategy that meets its business needs, but there are common practices for all organizations to consider. For example, using MFA with tools such as machine learning, rules engines and cutting-edge mitigation technologies can detect a wide range of fraud by looking for anomalies in customer behavior and other suspicious payment activity. However, fraud mitigation strategies should also take into account fraudsters' speed of progress and the organization's changing customer experience goals, compliance requirements, regulatory obligations and investment decisions.

KEY FINDINGS

As the volume of mobile and digital payments grows, FIs and merchants are trying to improve the increasingly fragmented components of the authentication process without major disruption to their customers. They must analyze thousands of data points and make the correct decisions to verify the customer and secure the payment process.

Efforts to improve authentication should not occur in silos because fraud is moving too fast and affects every point in the payment lifecycle.

Efforts to improve authentication should not occur in silos because fraud is moving too fast and affects every point in the payment lifecycle. There are many authentication methods, yet no one by itself can prevent fraud. There are numerous ways authentication approaches can combine – ostensibly offering a higher degree of protection. This makes it very difficult for FIs and merchants to assess which

28 Link analysis: The lynchpin to better investigations

29 Link analysis for fraud detection

combinations (layered or MFA) are most effective. Also, while any combination may be effective at a particular point in time, its effectiveness may decrease if a real-time fraud attack occurs. Therefore, even though many FIs still rely on KBA and may use MFA (e.g., OTP, push notifications and other device security) to strengthen it, others are advancing to device fingerprinting (65%), behavioral biometrics (65%), mobile network operator phone verification, authentication hubs and end-point detection.[30]

Our analysis has shown that many organizations use traditional rules-based and layered authentication. Passwordless authentication is gaining initial traction in identity management systems within organizations, but its use with payment applications lags. Continuous authentication is still emerging and not well understood. Machine learning is applicable to all authentication methods and approaches, but stakeholders should carefully review the benefits, capabilities and use models claimed in marketing messages.

Deployment of MFA is highly fragmented

Feedback from industry experts[31] noted that about 50% of U.S. FIs have adopted MFA, with higher adoption by FIs in the top asset tier. These large FIs tend to offer MFA to select high-value user segments with higher risk-type transactions. Wider deployment is not gaining a lot of traction because some FIs, when faced with the trade-off between fraud reduction that catches bad actors and higher friction that may turn away good customers, may lean towards limiting friction. Implementing MFA also may be cost-prohibitive to some FIs.

Because Federal Financial Institutions Examination Council (FFIEC) guidance for MFA is imprecise, there is little incentive for FIs of all sizes to encourage customers to accept MFA voluntarily. In addition, financial liability protection for consumers provides a disincentive for consumers to adopt strong security measures. Furthermore, different departments within an organization (e.g., AML, risk management, fraud prevention and account opening) may not agree on whether or how to incorporate MFA.

Data availability to conduct fraud analysis varies between enrollment and transaction

- When a customer opens a new bank account or credit card, or enrolls with a PSP or merchant, it is usually the first time the provider sees the customer. As noted earlier, there are techniques that verify new accounts, but they do not include a history of payment activity. An organization that has a previous relationship with the customer will have more data and may share it with other participants to the transaction.
- Because account opening assumes no previous relationship, and no historical/behavioral data to apply, some techniques used to authenticate transactions do not work for mitigating account opening authentication fraud.

30 Aite, May 2020, based on survey of FIs in September 2019.

31 Observations from subject matter expert interviews conducted between June and August 2020.

Weaknesses in current authentication methods

- Passwords are insecure authenticators and can be widely duplicated, yet payment stakeholders continue to offer passwords and customers continue to use them.
- KBA, also considered a weak authentication method, continues to be the primary or backup authentication method for account access and resets.
- MFA still relies heavily on the knowledge factor, which is subject to a high risk of compromise and effectively reduces MFA to 2FA, or single-factor if no biometrics are used.

No best practices or common lexicon to describe different authentication fraud detection and prevention techniques:[32]

- Creating a seamless customer process becomes a challenge when applying several authentication solutions for each step. In addition, the fragmented fraud mitigation landscape makes it difficult for many stakeholders to understand how different tools compare and which are most effective when part of a multi-layered approach. Many techniques can interact with one another (e.g., RBA, ML and AI, biometrics, MFA, 2FA), but information is lacking on how to most effectively combine or layer the techniques for different situations. One objective of these briefs is to encourage dialogue about potential industry collaboration to develop a common lexicon and best practices for mitigating remote authentication fraud.

Use of more sophisticated mitigation tools is growing inconsistently across the payment system

- This gap occurs within stakeholder segments, and by business asset size. Smaller FIs and e-merchants are more dependent on the tools their processors offer to manage authentication fraud, and may be at risk compared to large, more sophisticated organizations that have more resources and control over the authentication tools they implement.
- Because many organizations do not apply fraud mitigation tools uniformly or as part of a multi-layered approach, fraudsters are able to exploit vulnerabilities across the broader payment ecosystem.
- FIs and other industry stakeholders want to give customers streamlined experiences. However, to address potential ATO, they often have to interrupt the user with additional authentication requirements, e.g., 2FA, MFA, biometrics and/or passwords, etc., all of which fraudsters constantly try to break. The industry is starting to add smarter authentication tools. This process needs to be accelerated and become more coordinated among financial providers.

32 NIST 800-63-2 identifies four levels of assurance and the associated authentication methods. Most are focused on identity and access management (IAM), but the trajectory is toward payments.

Industry developments in the payment system are accelerating the need for stronger authentication fraud mitigation:

- COVID-19 has become a catalyst for wider, faster changes in how people pay across channels, e.g., using contactless cards at POS and ATMs, while shifting to digital channels (mobile/online) for card not present (CNP) purchases, P2P transactions and other banking services. The resulting acceleration of digital commerce has increased merchant volume, including smaller merchants that added online sales for the first time. This growth could be a potential tipping point for widespread adoption of strong authentication options in U.S. if consumers and businesses recognize the need for more effective authentication methods.
- Similar to legitimate customers, fraudsters are using more digital payment methods, such as digital wallets (e.g., PayPal, Apple Pay, Google Pay and Samsung Pay), which are more likely to be used fraudulently than regular credit card payments.[33]
- Fraudsters are constantly changing their focus of attacks more frequently and faster than fraud detection and mitigation tools can change.
- Merchants and FIs want fraud solutions to decrease their data security burdens and enable a faster and seamless user experience. They need more education on how to apply fraud techniques appropriately, e.g., when authentication tools should be layered.
- Faster payments – including the Federal Reserve's FedNow℠ Service and other forms – carry the risk of faster and irrevocable fraud. Real-time fraud mitigation will become a necessity.

Continuous authentication holds the promise of elevating trust in authentication mechanisms that preempt and mitigate fraud in real time.

- To function properly and effectively, continuous authentication would be embedded in a framework that defines design, infrastructure and governance of digital identity to unlock stakeholder value and address industry risk. Monitoring international (ISO, FATF) and national (NIST, FFIEC) digital identity standardization efforts and guidelines would help payments stakeholders to assess the potential impact of continuous authentication on the U.S. payment system.

Without more coordinated financial industry collaboration to address these challenges, fraudsters will continue to leverage opportunities to use automated methods, sophisticated machine learning algorithms and organized infrastructures to access and use customer financial data.

33 MPT: Battling fraud amid COVID-19, May 5, 2020, Brittany Allen.

RECOMMENDATIONS

These recommendations are intended to create discussion with stakeholders about the challenges of remote authentication fraud, help the Federal Reserve develop a strategy for next steps, and engage with the payments industry.

Recommendations for Federal Reserve/Secure Payments

1. Lead an industry initiative to enhance the MFA process and increase payment stakeholder adoption of effective MFA techniques.[34]

Research the current MFA landscape to analyze the effectiveness of different MFA approaches and techniques for financial services and identify examples where MFA has been successfully implemented.

Convene a group of stakeholders (including large and small FIs, merchants, payment service and solution providers) to build on these research findings to improve the MFA process. Develop a toolkit that:

(1) explains benefits and addresses potential barriers to adoption, particularly for smaller FIs and merchants that may have limited expertise and/or resources, and

(2) provides guidelines on how to apply appropriate authentication tools that comply with MFA and match the needs of individual FIs or businesses.

2. Lead an industry initiative to develop a framework for a common lexicon of authentication fraud detection and prevention techniques, including how the techniques interact.

Convene a few key industry experts to determine if there is interest to collaborate and develop a plan to educate payment stakeholders to make more informed remote authentication choices. Work with them to develop a statement of work for the framework before reaching out to broader group to solicit participation in a full project.

34 In May 2021, the White House issued an executive order on improving the nation's cybersecurity. Sec. 3. (d) states that within 180 days of the date of this order, [FECB] agencies shall adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent consistent with Federal records laws and other applicable laws. Executive Order on Improving the Nation's Cybersecurity. While directed at government agencies, this EO highlights the importance of MFA for non-government organizations, as well.

3. *Explore the industry's sentiment on eliminating passwords and the need for a more secure replacement, such as passwordless authentication. Convene an industry work group to discuss how to migrate from password to passwordless authentication, and address challenges.*

   Passwordless authentication (evolving to continuous), supported by behavioral analytics, behavioral biometrics, physical biometrics and machine learning, sets the stage for digital identity. Discuss the feasibility of password-less authentication with several industry stakeholders. If they agree that a more secure replacement for passwords is necessary, convene an industry work group to develop an industry strategy for migrating from password to passwordless authentication that supports the FIDO2 open standard.

   This initiative can include or coordinate with other industry associations. For example, FIDO2 and other FIDO initiatives apply to all the use cases covered in our analysis. The FIDO Alliance has broad cross-industry support of all major vendor, financial and big-tech players, but regulatory agencies are missing. And while FIDO is well-known in certain industry segments, it lacks recognition in others.

4. *Coordinate potential industry analysis and research on authentication fraud related to faster payments and open banking with the Federal Reserve's Reserve Bank Operations and Payment Systems and its FedNow Service under development.*[35]

   Identify existing authentication methods that support faster payments and open banking/application programming interfaces (APIs), as well as gaps and new issues that may arise with open banking. Many customers want access to convenient, digital financial solutions from fintechs that integrate with FIs to provide robust services. FIs must ensure protection of customer data accessed by third parties. FIs must be able to authenticate customers' identities and make it difficult for cybercriminals that steal customer information to represent themselves as legitimate customers.

35 May depend on what the U.S. Faster Payments Council is doing related to authentication fraud, and if this recommendation is duplicative.

Considerations for Payments Industry

1. Develop and refine authentication fraud mitigation strategies

Issuers and merchants need to stay abreast of new authentication methods and prepare to implement available solutions. They need to understand that there is no single authentication solution across payment types or channels to strengthen bank or card account authentication or reduce remote/CNP fraud. The optimal approach is to support a combination of tools and solutions that balance the costs of implementation with the expected benefits of managing remote fraud.

For example, as cybercriminals increasingly turn to stealing or hacking into mobile devices, analyzing mobile signals (such as IP addresses, phone numbers and other forms of passive information collected by apps) has become more important than ever to defend against fraud. More FIs and processors are implementing ML to leverage vast amounts of data to detect anomalies and identify fraudsters in real time. Leveraging ML to distinguish the common behaviors of trusted customers from those of fraudsters enables businesses to implement large-scale fraud prevention and mitigation strategies. This option may not be affordable for smaller stakeholders, but core processors and other industry providers have solutions that they can explore.

If stakeholders understand the attack vectors exploited, they can adjust their strategies, rules and models to address different types of fraud. Also, while mitigation is key, it is important to implement controls up front during the enrollment or transaction process that ensure preventative measures such as manual review and verification occur, even if this adds some friction.

2. Improve the customer authentication experience

Engaging customers in stronger authentication requires an improved and trusted user experience. It needs to be simple and quick, especially due to the increasing number of online banking and payment accounts used by consumers. Conducting analysis and applying techniques that match authentication methods to the level of risk at the point of interaction can balance the tradeoff between security and the user experience by limiting high-friction and more costly authentication methods to high-risk requests. If customers understand how the protections perform, they may be supportive.[36] NIST SP 800-63-3 establishes risk-based processes for the assessment of risks for identity management activities and selection of appropriate assurance levels and controls. Organizations have the flexibility to choose the appropriate assurance level to meet their specific needs.[37]

36 Experian survey 2019: 66% of people like security protocols when interacting online. 86% said consumer value security over convenience in digital channels.

37 NIST Special Publication 800-63 Digital Identity Guidelines

Stakeholders might consider when and where they deploy versatile and flexible passwordless, risk-based and two-factor authentication methods (including biometrics and behavioral biometrics) to guard against ATO and other types of emerging online fraud. Push notifications, facial and fingerprint biometrics, and behavioral biometrics are the most *difficult-to-tamper-with* types of 2FA. Leveraging industry protocols, such as 3DS, to allow the exchange of additional customer data may enable a more secure online payment experience. A combination of behavioral analytics, physical biometrics and behavioral biometrics, plus passwordless authentication, could enlarge the pool of transactions that are approved automatically, with relatively less friction.

3. Provide consistent and frequent authentication messaging to customers.

Consider promoting active industry efforts to strengthen payment authentication through education on best practices for consumers that help to recognize key fraud threats, use common terminology and understand prevention techniques. Robust authentication measures make it harder for criminals to gain access to accounts using stolen details, but FIs also should take measures to reduce the likelihood that fraudsters get any customer information. Developing more coordinated and frequent education for account holders on how to recognize risks, threats and mitigation could help to reduce authentication fraud. For example, malicious actors have been ramping up phishing attempts during the pandemic as customers and businesses quickly transitioned to digital operations. The current environment has made customers more vulnerable because they are enrolling in digital services they have not used before, and lack experiences to help spot red flags.[38] Complementing the use of stronger mitigation approaches with customer education and engagement in mitigating fraud may be more effective.

For more information, visit FedPaymentsImprovement.org and submit or update your FedPayments Improvement Community profile and select "Remote Payments Fraud" as a topic of interest.

THE FEDERAL RESERVE
FedPayments Improvement
COLLABORATE. ENGAGE. TRANSFORM.

38 Google reported that the number of phishing attacks involving fake websites rose 350% between January and March 2020. PYMNTS.com, June 8, 2020. Open banking financial institution security fintech fraud authentication