PRESERVING TRUST IN DIGITAL FINANCIAL SERVICES:
THE ROLE OF IDENTITY AND AUTHENTICATION

September 2018

Sponsored by:

IBM Security

Independently produced by:

JAVELIN

TABLE OF CONTENTS

TABLE OF FIGURES

FOREWORD

This original report, sponsored by IBM Security examines the role of identity verification and authentication in building trust in financial services, both in helping accountholders trust their financial institutions and in enabling financial institutions to expand their digital features and functionality.

This research report was independently produced by Javelin Strategy & Research. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

In Europe and the U.S., financial services organizations and their customers are enjoying the benefits of a digital revolution. Digital channels have transformed the way consumers interact with their financial service providers. Digital channels have bolstered the ability of banks and insurers not only to attract new customers but also to engage with existing customers at a lower cost and with a broader range of relationship-enhancing capabilities. At the same time, the introduction of new digital capabilities has drawn the attention of criminals. Their efforts are undermining the trust at the center of the relationship between financial service organizations and their customers. Maintaining this trust while maximizing the potential of digital channel investments requires a comprehensive approach to identifying and authenticating customers from day one.

EXECUTIVE SUMMARY

Key Findings

The future of financial services is digital. Not only do broader digital feature sets make it easier for customers to perform traditional financial activities such as bill payment and financial management, they also open up new avenues for companies to engage with their customers through personalized guidance, peer-to-peer payments, and more.

However, expanding digital capabilities brings significant fraud risks. Tools that make it easier for customers to manage their financial lives through digital channels often make it easier for fraudsters to target those accounts as well. Digital account opening, rapid money movement, and remote account access are all both crucial for serving customers and subject to sophisticated attacks from fraudsters. This is daunting for financial services companies — only half (52%) report they are confident in the effectiveness of their fraud mitigation processes at identifying fraudulent applicants.

Pressure from customers, competitors, and outside players raises the stakes on digital services. Consumers expect their financial service providers to march at the pace set by companies outside of financial services, such as Google and Amazon. Fintech players such as PayPal seek to usurp traditional banking roles, enabling consumers to seek out their preferred service for specific tasks such as saving and money movement, turning FIs into the "dumb pipes" behind consumers' financial activities. Despite the fraud risks that come with new digital products and capabilities, banks and insurers have no choice but to keep pace.

Building a foundation of trust with customers requires establishing confidence in digital security. Trust is the bedrock of the relationship with customers in financial services, and that trust is closely tied to the security of digital channels. In fact, the higher the degree of perceived online and mobile channel security, the more a consumer in the U.S. trusts her primary financial institution.

Consumers need to be persuaded of the security of digital banking channels. Trust is at risk as many consumers remain skeptical of the security of online and mobile banking. Just 50% of consumers believe mobile banking is secure, somewhat behind online banking (63%). For these users, visible security measures are key to providing tangible assurance that their accounts and information are protected.

Consumers' reluctance to trust digital banking channels is hampered by a high rate of authentication failure. Just more than 1 in 5 authentication attempts at financial services companies fails, with 13% of organizations experiencing a failure rate of 40% of higher, for an average failure rate of 22.8% across all businesses. Not only does failed authentication add unnecessary friction to legitimate customers' attempts to access their accounts, it drives customers to the call center to recover access to their accounts, imposing additional costs on the financial institution.

There are tangible benefits when customers perceive security in digital channels. Financial institutions that report their customers believe in the security of their digital channels see significantly higher monthly usage of their online portals and mobile apps: 52% vs. 44% for online and 43% vs. 38% for mobile. This

translates into a number of benefits for the financial institution, including lower costs when users shift from using branches or call centers to using online and mobile banking and increased opportunities for engagement.

Emerging fraud schemes are specifically designed to abuse trust. Over the last three years, fraudsters have begun aggressively targeting victims' financial and non-financial accounts simultaneously. The growth in this fraud scheme owes much of its momentum to fraudsters' compromising email or mobile phone accounts to overcome one-time passwords in step-up authentication for high-risk events. By taking over established communication channels, fraudsters are effectively able to completely compromise victim's identities for the purposes of remote interactions with their financial institution.

Digital transformation is progressing unevenly within financial services sectors. This differential manifests in differing priorities for digital investment between insurance and financial institutions. By far, insurers' top priorities are improving digital user experience and interface (23%) and offering new digital features and functionality (13%), while financial institutions — that are further along in their digital transformations — are more focused on security of existing customer accounts, listed as a top priority by 15% of FIs.

Insurance providers should learn from the experiences of banks and issuers. Accounts held with financial institutions tend to be much easier for fraudsters to monetize than insurance policies, which has traditionally made banks, credit unions, and card issuers primary targets for fraud. However, as financial institutions have responded to this pressure with more sophisticated anti-fraud measures, fraudsters' focus has broadened across the world. British fraud reporting agency Cifas found that reported identity fraud cases involving insurance companies increased more than hundredfold between the first half of 2016 and the first half of 2017.

Delivering on the promise of digital transformation requires a delicate balance. On top of the challenges posed by attacks from fraudsters, financial services companies must balance two conflicting sets of expectations from users. While the perception of security is critical to trust, users demand streamlined experiences in which fraud mitigation tools do not interfere with the tasks they are performing. For experience-oriented accountholders, invisible fraud protections are crucial for assuring that security measures appear only when absolutely necessary.'

Six in 10 financial services companies feel their organization strikes an appropriate balance in the pace at which they revise their fraud management processes. The remaining businesses tend to err in favor of an overly aggressive approach, with just more than a quarter of financial services companies reporting that they revise their identity verification (IDV) processes frequently enough to keep ahead of emerging fraud schemes but that the pace of change taxes their business' resources.

Recommendations

Align identity and authentication experiences throughout the customer journey. Use consumers' first experiences with the bank to bolster trust and to capture data to better protect them throughout the relationship. Enrollment in biometric authentication and use of tangible identity verification tools such as document scanning at account opening can

provide a consistent experience for later authentication and establish patterns that can be used to distinguish between legitimate and fraudulent activity later.

Minimize reliance on PII at account opening. With major breaches leaking consumers' personal details, simply validating that the personally identifiable information entered in an application matches a single individual is insufficient to protect against fraud. Drawing on the validation of information and intelligence from less conventional third-party providers such as mobile network operators can deliver additional context around the legitimacy of an applicant.

Use well-informed risk-based authentication to judiciously apply step-up authentication. Using tools such as behavioral biometrics, device recognition, and geolocation can help distinguish between legitimate and malicious users without requiring financial service companies to intervene with authentication challenges. This type of information can even allow enhancements to the customer experience by lowering barriers to different account activities and allowing higher limits for transactions.

Move away from one-time passwords. One-time passwords, delivered through a text message, email, or stand-alone app, are the most prevalent means of step-up authentication in financial services. Unfortunately, OTPs are prone to interception, with fraudsters having years of experience finding workarounds to this authentication method. As attacks on accounts at financial services companies have accelerated over the past several years, compromises of email and mobile phone accounts have risen in tandem as fraudsters completely take over victims' identities to overcome authentication challenges.

Embrace biometrics for login and step-up authentication. Not only do biometric modalities provide a smoother user experience than using one-time passwords, they can provide significantly more assurance that the user entering the authenticator is the individual associated with the account. Additionally, standards such as those put forth by the FIDO Alliance back biometric authentication with public key cryptography to essentially eliminate the risk of data interception. Under these arrangements, the user is authenticated against a biometric template stored solely on the user's device, which then certifies to the authentication server that the user has overcome the challenge.

WHY ARE BANKS AND INSURERS GOING DIGITAL?

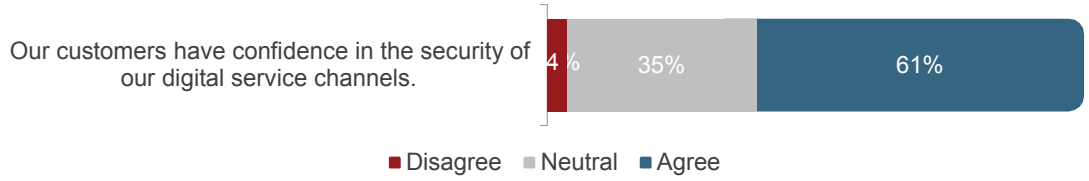
As financial services have largely moved from the physical to the digital world, establishing robust trust between financial services companies and their customers has become increasingly challenging. Broad digital capabilities combined with a flexible and streamlined user interface is a necessity for consumer-oriented financial services companies, regardless of what sector they operate in. However, new financial products and capabilities, such as person-to-person payments and digital account opening, depend on the ability to effectively identify users at the time the account is opened as the basis for accurately assessing risk throughout the customer relationship.

At the same time, while use of digital channels has reached ubiquity in many areas of digital financial services, many consumers still remain skeptical of the security of online and mobile banking. These concerns become even more acute when it comes to emerging services such as voice banking and virtual home assistants. Persuading consumers to have confidence in the security of their accounts is crucial for driving adoption of these services (see *Building Trust Throughout the Customer Life Cycle* section, Page 14). Yet for many financial service companies, there is still work to be done, as 4 of 10 don't believe customers have full confidence in the security of their digital channels (Figure 1).

These organizations' pace of innovation is being driven by the expectations of consumers whose expectations are being set by companies outside of financial services, such as Google and Amazon. Further still, many of the tech giants show signs of making incursions into financial services, such as Google's and Apple's movements into payments. More traditional fintech players such as PayPal seek to usurp traditional banking roles, enabling consumers to seek out their preferred service for specific tasks such as saving and money movement, which risks turning FIs into the "dumb pipes" behind consumers' financial activities. That only increases the pressure financial service organizations face, on top of the threat from new fraud schemes that accompanies new digital products and features (see *Understanding the Risks in Digital Financial Services* section, Page 11). Despite the risks that new digital products and capabilities introduce, banks and insurers have no choice but to keep up.

More Than Half of Financial Services Companies Believe Customers Have Confidence in Their Digital Security

Figure 1. Confidence in Security of Digital Channels



Source: Javelin Strategy & Research, 2018

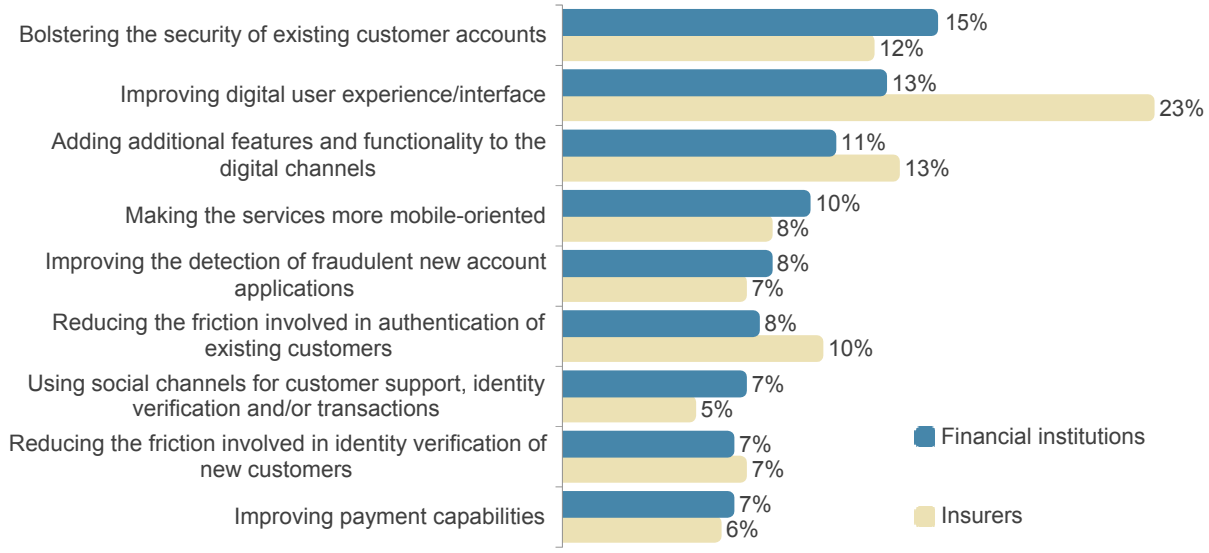
BANKS AND INSURERS HAVE DIFFERING DIGITAL PRIORITIES

While the transformation from offline to digital delivery has been underway for decades, progress is uneven across sectors. Financial institutions — largely banks, credit unions, and card issuers — have typically led the charge, since they face some of the most intense pressure from users. Online banking has reached ubiquity, with tremendous numbers of consumers of all ages turning to their computers as their primary point of contact with their financial institution, and the adoption of mobile banking is not far behind. And new channels are on the horizon as banks explore voice banking through virtual home assistants such as Amazon's Alexa. While financial institutions report that their top priority for digital transformation over the next year is bolstering the security of existing customer accounts, insurers are preparing to move more strongly along their digital transformation with investments in user experience and interface, along with additional features and functionality (Figure 2).

To accomplish this, insurers should learn from the experiences of financial institutions. Accounts held with financial institutions tend to be much easier for fraudsters to monetize than insurance policies, which has traditionally made banks, credit unions, and card issuers the primary targets for fraud, whether in opening fraudulent new accounts or taking over a legitimate customer's identity. This has become even more pronounced with the rise of online and mobile banking and digital account opening. Today, financial institutions are focused on bolstering security to counteract the fraud risks that new digital capabilities have enabled, as well as to meet evolving regulatory mandates such as PSD2 in Europe.

Insurance Companies Focus on User Experience as They Begin to Modernize

Figure 2. Most Significant Priorities for Digital Transformation Over the Next 12 Months



Source: Javelin Strategy & Research, 2018

There are early indications that as insurers increasingly go digital, they are experiencing some of the same symptoms of increased interest from fraudsters. British fraud reporting agency Cifas found that reported identity fraud cases involving insurance companies increased more than hundredfold between the first half of 2016 and the first half of 2017.[1] With banks on the back foot after years of investment in digital channel capabilities and under pressure from regulators, and fraudsters increasing their focus on insurers, the message to all of these organizations could not be clearer: Now is the time to invest in measures that protect the integrity of the application process and existing customer accounts.

[1] https://www.cifas.org.uk/newsroom/identity-fraud-soars-to-new-levels, accessed July 30, 2018.

UNDERSTANDING THE RISKS IN GOING DIGITAL

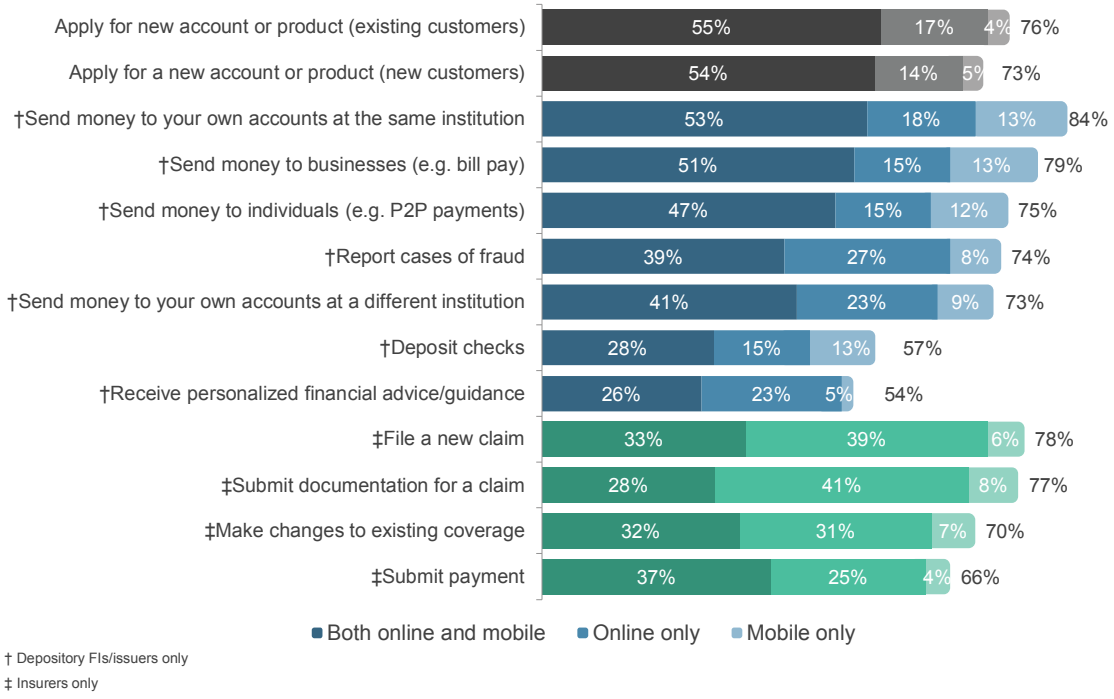
For financial institutions and insurers, digital channels offer opportunities for providing robust self-service capabilities that reduce costs, a range of transaction types to drive revenue, and bidirectional dialogue about the needs and goals of customers to grow relationships. The value of these opportunities is evidenced by the broad availability of digital capabilities such as account opening for new customers (73%), through P2P payments among banks (75%), and filing claims (78%) and submitting claim documentation among insurers (77%), (Figure 3).

The digital transformation of financial services is not without risks. Expanding digital functionality creates new avenues for fraudsters to target these organizations and their customers. Fraudsters have honed schemes that take advantage of weaknesses in both the application process and how organizations protect existing accounts:

- **Digital application fraud:** Just as with remote access to accounts, digital account opening provides fraudsters with greater opportunity for anonymity and the ability to automate attempts across many institutions simultaneously. Although tools such as device recognition and behavioral analytics can enable financial institutions to filter out malicious traffic regardless of the apparent validity of the application, less sophisticated organizations relying heavily on PII validation face tremendous exposure.

FIs Are Strong in Digital Transaction Capabilities but Not in Financial Guidance

Figure 3. Feature Adoption by Financial Institutions and Insurers



† Depository FIs/issuers only
‡ Insurers only

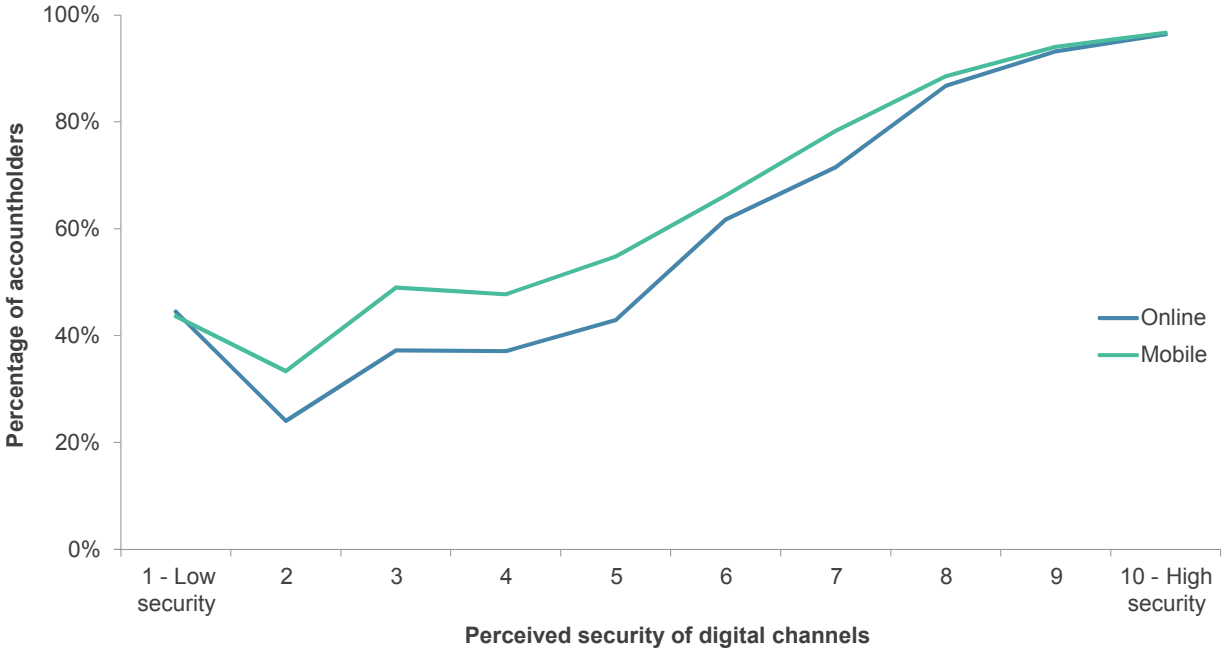
Source: Javelin Strategy & Research, 2018

- **Remote account takeover:** Armed with dumps of breached login credentials and tools to mask their location and device information, fraudsters relentlessly target financial institutions' login portals. With automated tools attempting huge numbers of credential pairs in quick succession, even a low success rate can mean significant losses for targeted institutions. Even if fraudsters are not able to gain direct access to an account, often the financial institution's response to the login attempt can yield valuable information — for instance, identifying where the credentials are valid but two-factor authentication is in use, enabling the fraudsters to return equipped for a more sophisticated attack.
- **Unauthorized payments and transfers:** Digital payment capabilities allow fraudsters to effectively monetize victims' accounts, rapidly moving funds to accounts under the fraudsters' control or shifting funds among multiple accounts to conceal fraudulent activity. As pressure mounts to move payments to real or near-real time, financial institutions have shrinking windows to assess the legitimacy of attempts to move money out of an account.

Anticipating and preventing fraud schemes through effective identification and authentication processes are crucial to preventing losses, as well as preserving the trust of customers. The perception of security among customers is crucial to maintaining the bedrock of a banking relationship because trust grows alongside their confidence in the bank's digital channel security (see Figure 4).

There Is a Strong Correlation Between Trust and Digital Security in Banking

Figure 4. Trust Among Primary FI Customers (U.S.) by Perceived Digital Security



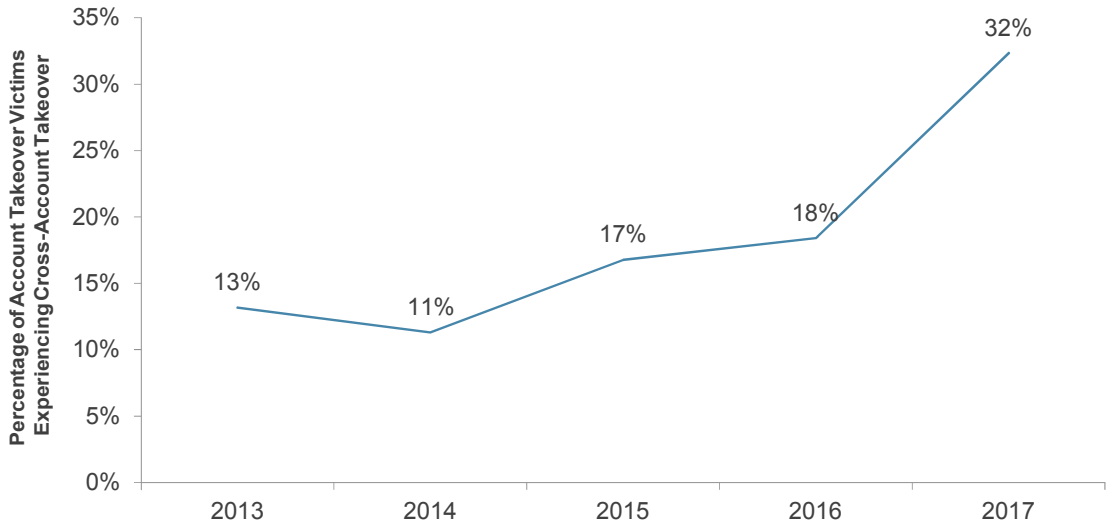
Source: Javelin Strategy & Research, 2018

The most challenging fraud schemes to address are the ones that are specifically designed to abuse previously established trust between financial institutions and their accountholders. From 2014 to 2017, the rate of cross-account takeover (defined as takeover of both a financial and a non-financial account) nearly tripled, from 11% to 32% of all account takeover victims (Figure 5). The growth in this particular fraud scheme owes much of its momentum to fraudsters' compromising email or mobile phone accounts in efforts to overcome financial institutions' use of one-time passwords as step-up authentication for high-risk events.

By taking over established communication channels, fraudsters are effectively able to completely compromise victim's identities for the purposes of remote interactions with their financial institution. This leaves less sophisticated institutions vulnerable if they overemphasize the strength of previously enrolled communication channels and do not take advantage of tools to assess behavioral or contextual risk indicators.

Fraudsters Target Multiple Accounts to Completely Take Over Victims' Identities

Figure 5. U.S. Cross-Account Takeover (2013-17)



Source: Javelin Strategy & Research, 2018

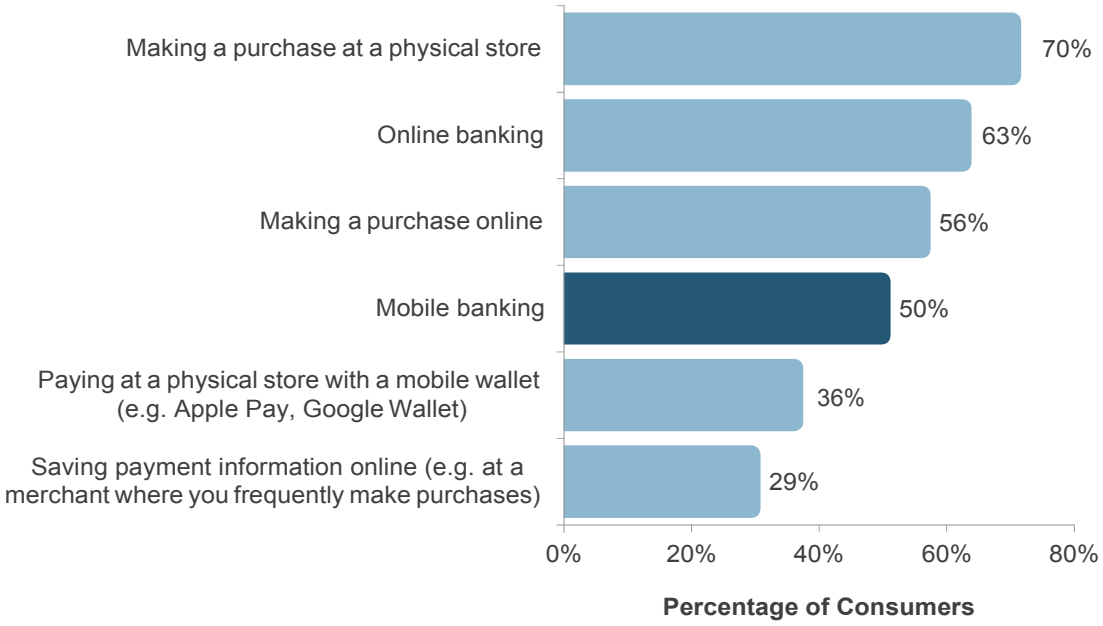
BUILDING TRUST THROUGHOUT THE CUSTOMER LIFE CYCLE

On top of the challenges posed by attacks from fraudsters, financial services companies must balance two conflicting sets of expectations from users. Financial services companies, as the stewards of consumers' finances and identities, have the burden of proving to their customers that there are robust measures in place to protect them. In spite of the near-ubiquity of digital financial services, many consumers remain skeptical of the security of online and mobile banking. Just 50% of consumers believe mobile banking is secure, somewhat behind online banking (63%) (Figure 6). For these users, visible security measures are the key to providing tangible assurance that their accounts and information are protected.

At the same time, users demand streamlined experiences, in which fraud mitigation tools do not interfere with the tasks they are performing. For experience-oriented accountholders, invisible fraud protections are crucial for assuring that security measures appear only when absolutely necessary.

Consumers Still Need Assurance That Digital Banking Is Secure

Figure 6. Perceived Security of Banking and Shopping Activities Among Consumers



Source: Javelin Strategy & Research, 2018

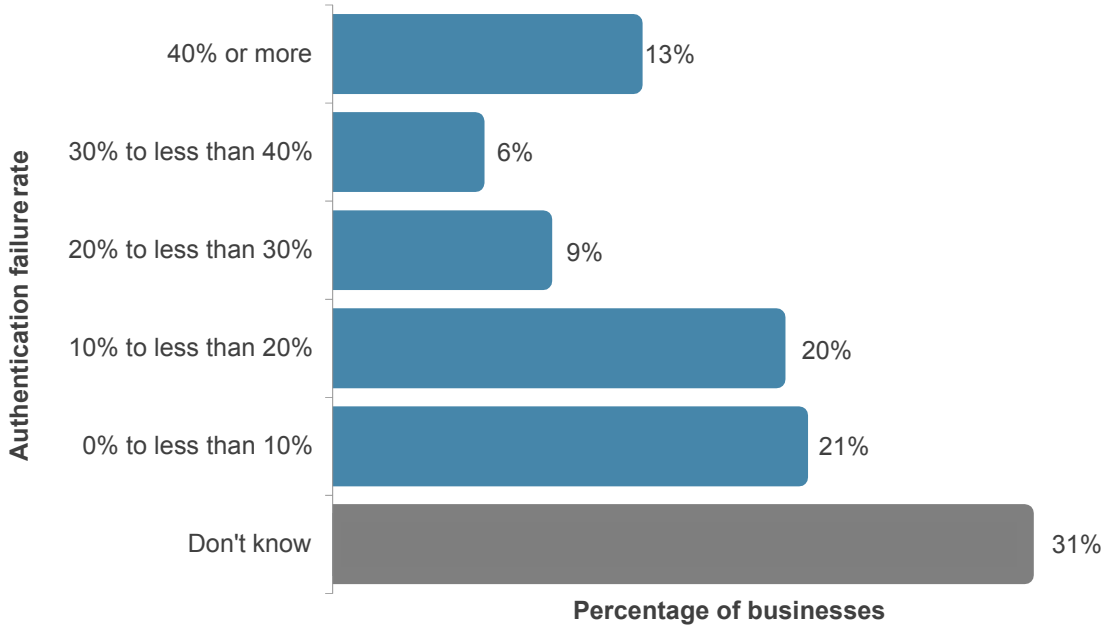
Consumers' reluctance to trust digital banking channels is not assisted by a high rate of authentication failure at many institutions. Just more than 1 in 5 authentication attempts at financial services companies fails, with 13% of organizations experiencing a failure rate of 40% of higher, for an average failure rate of 22.8% across all businesses (Figure 7).

Not only does failed authentication add unnecessary friction to legitimate customers' attempts to access their accounts, it demonstrates that the authentication methods used by their financial institution are faulty. Even if the error is in implementing with excessive sensitivity, it still shows customers their financial institution cannot effectively identify its users.

Poor choice of authentication methods can contribute to challenges with digital access. Passwords are notorious for the challenges they pose for user experience, especially for sites that are not likely to be visited regularly, such as an insurer's digital portals. Strong, unique passwords are difficult to remember,

1 in 5 Authentication Attempts Fails

Figure 7. Authentication Failure Rate at Financial Services Companies



Source: Javelin Strategy & Research, 2018

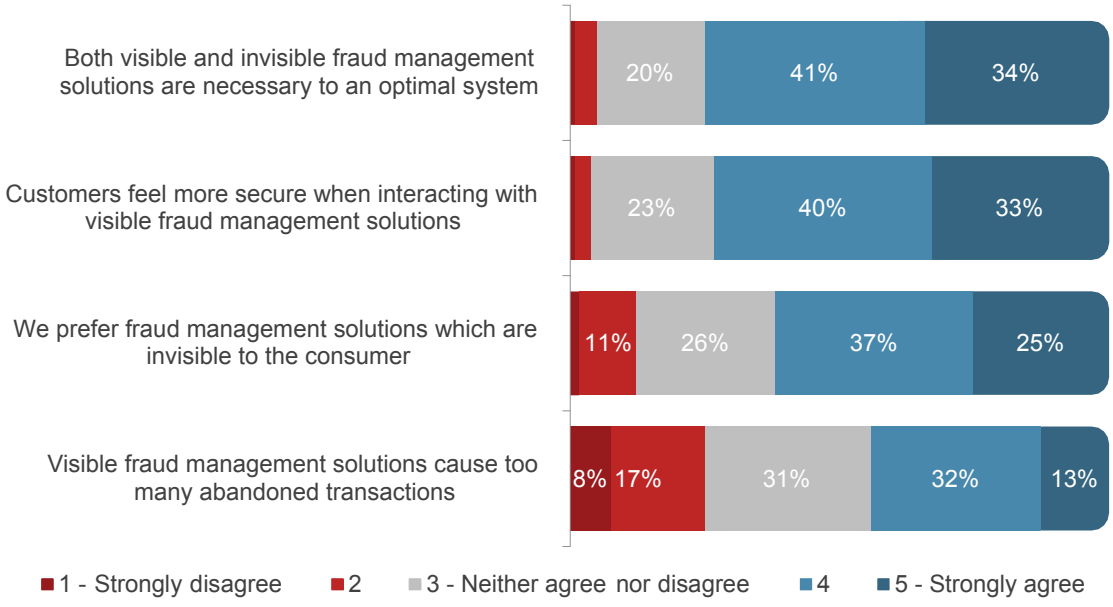
forcing users to reset their login information or call customer service, imposing additional costs on the financial institution. One-time passwords delivered by SMS can also impose more significant friction, especially for mobile users who have to switch back and forth between their messaging app and the app they are attempting to log into.

While biometric modalities can also be prone to false positive declines due to poor environmental conditions or changes in user characteristics, they also have the advantage that reauthentication is frequently less disruptive to user experience. For fingerprint biometrics in particular, reauthentication simply requires tapping the sensor again.

These dual pressures are reflected in the fact that while the overwhelming majority (75%) of financial institutions and issuers agree that both visible and invisible fraud management solutions are necessary in an optimal system (Figure 8), both types of organizations nevertheless tend to err on the side of visible fraud management tools, in part because these solutions help their users feel more secure. Financial institutions that report that their customers trust the security of their digital channels see significantly higher monthly usage of their online portal and mobile apps: 52% vs. 44% for online and 43% vs. 38% for mobile (Figure 9). This translates into a number of benefits for the financial institution, including lower costs when users shift from

Both Visible and Invisible Fraud Management Tools Are Crucial

Figure 8. Attitudes Around Visible and Invisible Fraud Management



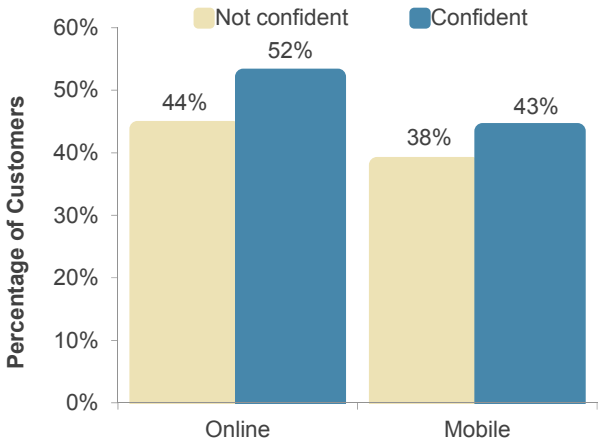
Source: Javelin Strategy & Research, 2018

using branches or call centers to using online and mobile banking and increased opportunities for engagement.

Laying a strong foundation in robust fraud management strategy can free up resources to focus on other aspects of building relationships with customers. Among organizations that have already achieved some measure of success and are above the median rate for monthly online usage among their accountholders, the primary focus is on improving the digital user experience and interface, the top priority for 25% of organizations. Conversely, organizations that lag in digital adoption tend to be forced to devote resources to reducing friction by revising their authentication processes, the top priority for 21% of organizations below the median in online channel usage (Figure 10).

Trust in Digital Channels Manifests in Higher Usage of Online and Mobile Banking

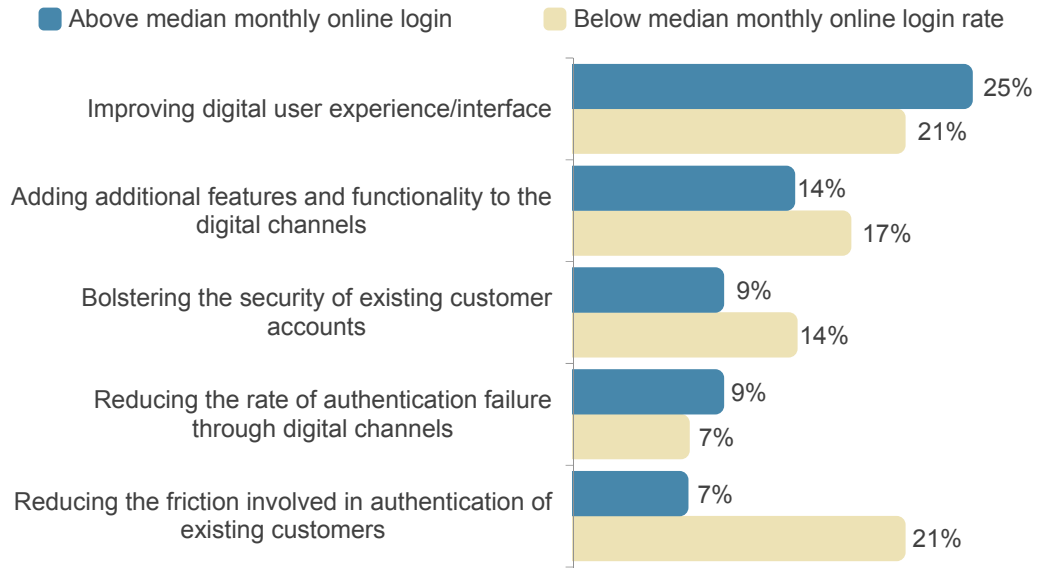
Figure 9. Percentage of Customers Logging into Digital Channels on a Monthly Basis, by Customers' Confidence in Security of Digital Channels



Source: Javelin Strategy & Research, 2018

Getting Authentication Right Frees Up Resources to Improve User Experience

Figure 10. Top Digital Priorities for the Next 12 Months, by Customers' Adoption of Online Portals



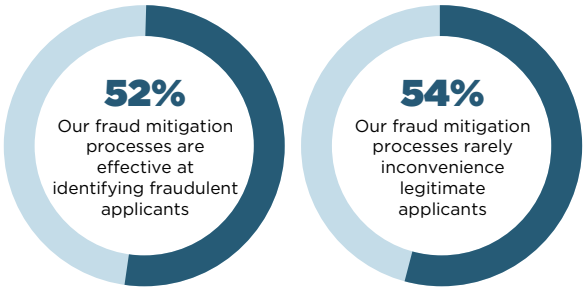
Source: Javelin Strategy & Research, 2018

Identity Proofing Tools: Trust Starts at the Application

Building trust with accountholders begins during the account opening process. This is likely to be the first real opportunity the applicant has had to interact with the financial institution and consequently can provide a powerful first impression. For many financial service providers, digital account opening starts with the same flow as when accounts were principally opened at the branch: collect data on the applicant and validate that information. Today, these institutions must go further to effectively prove that the identities being presented to them in digital channels are legitimate without alienating good customers. But many still have their work cut out for them, as just more than half believe their fraud mitigation processes rarely inconvenience legitimate applicants (54%) and are effective at identifying fraudulent applicants (52%) (Figure 11).

Many Organizations Are Not Confident in the Effectiveness of Their Identity Verification Measures

Figure 11. Effectiveness of Fraud Mitigation Measures

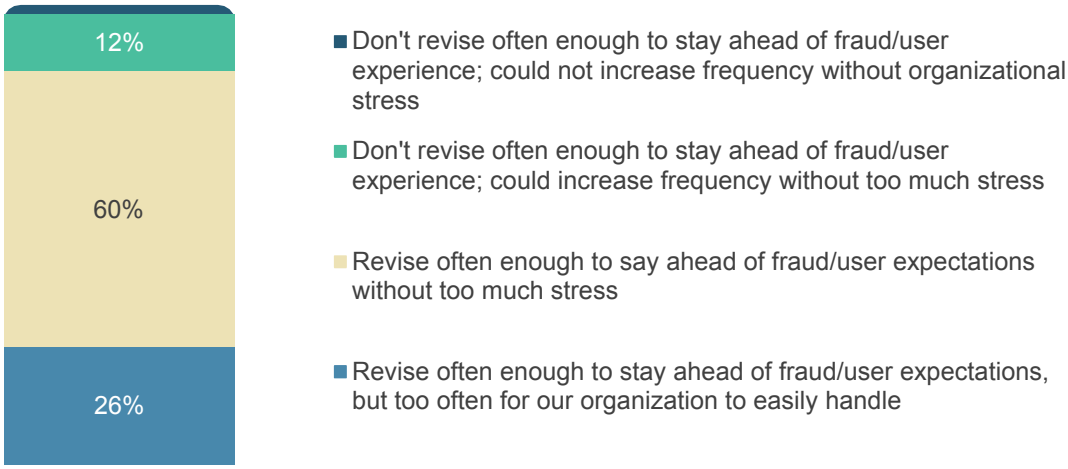


Source: Javelin Strategy & Research, 2018

The rapidly evolving nature of fraud schemes creates a challenging balance for financial services companies. Fortunately, 6 in 10 financial services companies feel their organization strikes an appropriate balance in the pace at which they revise their fraud management processes (Figure 12). For the other 40% of businesses, there are two types of challenges:

6 in 10 Businesses Are Comfortable With the Pace of IDV Process Changes

Figure 12. Frequency of Revising Identity Verification Process and Impact on Business



Source: Javelin Strategy & Research, 2018

Changing processes quickly by revising rules and adding in new tools can help address new threats as they arise but risks overtaxing business resources and confusing customers, who also have to adapt to new identity verification and authentication measures. Just more than a quarter of financial services companies fall into this trap, reporting that their IDV processes are agile enough to stop fraud but change too frequently for their business to easily handle.

Conversely, erring too far in the other direction can provide stability for customers but provides fraudsters with the opportunity to exploit gaps in identity verification measures. Fourteen percent of financial services companies fall into this bucket, taking a cautious approach that slows the pace of change at the risk of additional fraud.

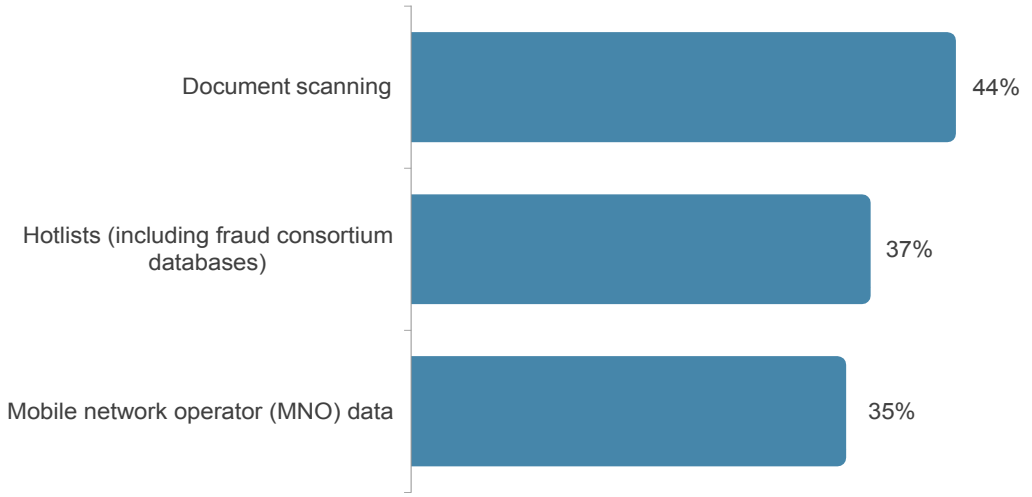
Despite their differing strategies, similar measures can help both types of businesses.

Placing a greater emphasis on automated tools and background fraud mitigation measures can help alleviate the strain on business resources and enable a more rapid pace of change that does not confound legitimate customers. Drawing on resources such as mobile network operators for additional context on an applicant and risk assessment tools such as device reputation and behavioral biometrics/ analytics provides additional layers of defense against fraud without requiring frequent changes to customer-facing portals (for more detail, see Assessing Risk in the Application and Beyond, Page 21).

Basic validation of personally identifiable information (PII) remains the primary tool used by both financial institutions and issuers to distinguish between legitimate and fraudulent applicants. This process is inherently vulnerable, as the wealth of persistent data compromised in breaches such as Equifax, Anthem, and the Office of Personnel

Adoption of Digital Document Scanning and MNO Data Is Far From Ubiquitous

Figure 13. Use of Identity Proofing Technologies Among Financial Service Providers



Source: Javelin Strategy & Research, 2018

Management makes it easy for fraudsters to find consistent sets of PII that they can use to apply for accounts at dozens of financial institutions using automated scripts until they find an organization lacking appropriate fraud controls.

Not only is PII validation insufficient to stop fraudsters, it also imposes unnecessary burdens on legitimate applicants. Manually entering data in fields on an account application is unwieldy at best and is especially painful for mobile account opening. Fortunately, there are additional steps that banks and insurers can take that help streamline the account application process and provide more tangible assurance of security for prospective accountholders, as well as definitively prove the identity of these applicants.

Document scanning, used by 44% of financial institutions and insurers, enables financial service companies to automatically extract data and autofill fields from an image of a driver's license or other ID document (Figure 14). Although document scanning does require more direct engagement by the user, this trade-off is easily accounted for by eliminating the need to manually enter data in fields, especially for applications initiated from a mobile device. Additionally, most document scanning solutions provide some degree of validation that the document scanned has not been tampered with or forged.

Drawing on data from mobile network operators (MNOs) provides a greater degree of identity assurance than traditional PII validation (35%), because these organizations are able to share additional context about the user, such as the type and tenure of the device associated with the account. Devices that have been associated with an individual whose PII matches the information in the application are more likely to be legitimate than ones that have only recently been added to the account or which have had their SIM card swapped out recently.

In addition to helping reassure accountholders of the security of their new accounts, using higher assurance identity verification can enable financial institutions to roll out new, higher risk features that are backed up by a higher degree of trust in the identity of the new customer. For card issuers, this can include features like temporary card numbers that enable instant access to credit, allowing new accountholders to begin making online purchases on the account prior the physical card arriving. This can tangibly show the issuers' trust in their customer and help begin instilling loyalty early.

Assessing Risk in the Application and Beyond

However important tangible assurance of security is in building trust among new and existing accountholders, regularly challenging customers with authentication hurdles impedes their ability to accomplish basic tasks remotely and becomes expensive as well. Background measures designed to invisibly assess risk helps financial services companies more judiciously apply authentication measures. Additionally, because these tools operate invisibly alongside other authentication methods, they can provide early indication that an application is fraudulent or that an account has been taken over and a previously trusted channel may now be unreliable.

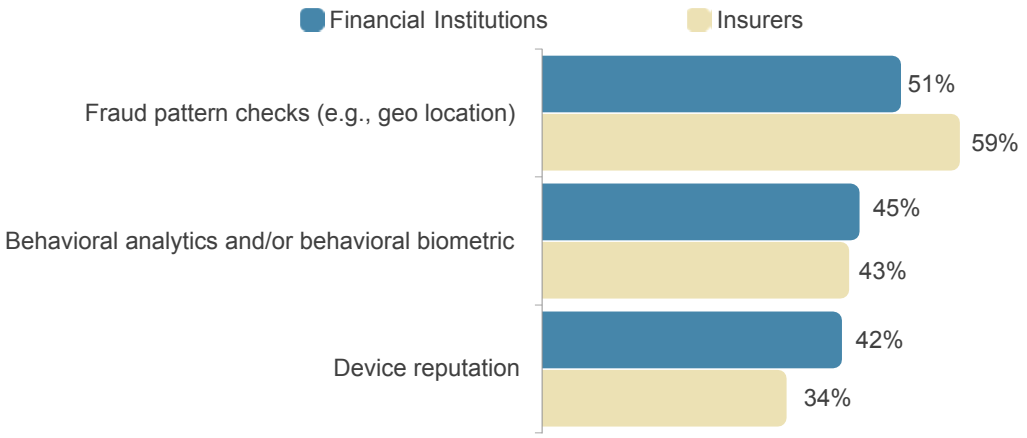
Basic rules-based pattern checks provide protection against consistent fraud schemes. These include monitoring the velocity of activity — i.e., the volume of applications or transactions that occur within a given period. This helps detect automated schemes such as credential replay attacks, in which fraudsters use scripts that take username and password pairs compromised in previous breaches and test them against dozens of major websites in attempts to identify reused credentials that can provide access to other accounts.

While rules-based pattern checks are the most prevalent risk assessment tool, they are limited to detecting previously identified fraud tactics and consequently create something of an arms race as fraudsters consistently seek to exploit blind spots in existing rules frameworks and defenders revise their techniques to shut down new fraud schemes.

Device reputation goes beyond simply matching the device to one used by the accountholder in the past to assess the risk associated with the device. This is typically accomplished by looking for indicators that the user is attempting to mask the actual details of the device through emulation or masking location through a virtual private network (VPN). Additionally, if the device has been previously identified, device reputation services may check whether this device is

Basic Pattern Checks Are the Most Common Risk Assessment Tool

Figure 14. Adoption of Risk Assessment Controls, Financial Institutions and Insurers



Source: Javelin Strategy & Research, 2018

associated with positive or negative behavior in its interactions with other organizations. This type of technology is somewhat more popular among FIs than among insurers (42% vs. 34%, respectively), but adoption is still lower compared with other technologies, such as behavior-based solutions (Figure 14).

Behavior-based solutions such as behavioral biometrics and behavioral analytics are finding strong adoption among financial service providers that seek to effectively assess risk without interfering with the customer experience, although there are notable differences between the types of behavior that these technologies examine:

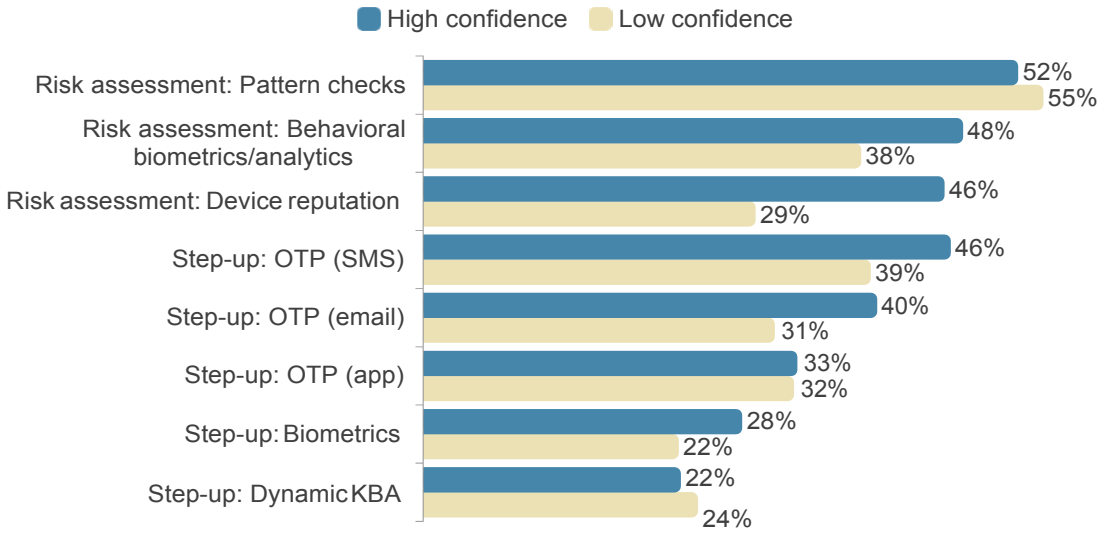
- **Behavioral biometrics** leverages the user's interaction with the device, through a keyboard, mouse, or touchscreen, to identify indicators of automation, remote control of a legitimate device, or fraudulent activity.
- **Behavioral analytics** considers the activities that users take within their digital session, such as the features they access, when they access them, and their location when accessing them.

By continuously monitoring behavior through an online or mobile banking session, these solutions can help identify account takeover even when the fraudster is able to overcome initial authentication challenges, enabling the financial institution, merchant, or insurance provider to deploy more rigorous authentication methods to stop the fraud before the fraudster is able to drain the account or complete the application.

Notably, use of both behavior-based solutions and device reputation is much higher among organizations with high trust from their accountholders (Figure 15). While neither technology is likely to be visible to users, both can manifest in much more streamlined experiences for users.

FIs With High Confidence Among Their Users Rely Heavily on Background Risk Assessment Tools

Figure 15. Risk Assessment, Step-Up Authentication Measures used, by Customer's Confidence in the Security of Digital Channels



Source: Javelin Strategy & Research, 2018

Authenticating the Customer to Preserve Trust

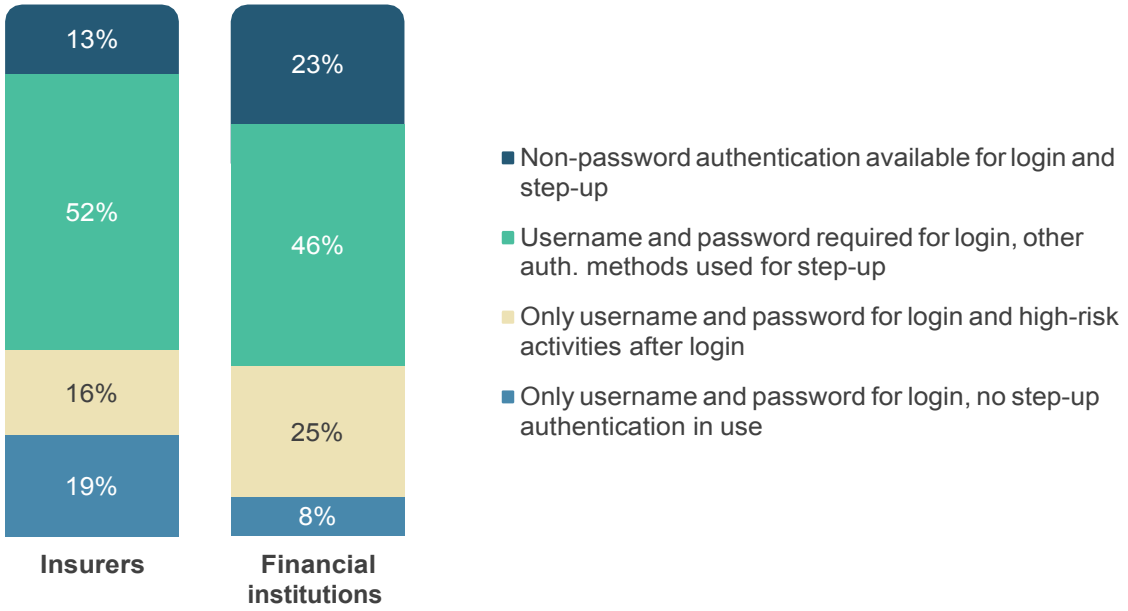
While robust risk assessment tools can help more strategically deploy authentication challenges, the types of authentication used to verify users' identity obviously matter a great deal in shaping both customers' perception of their financial services providers and the subsequent trust they have in these organizations.

Authentication is one particularly key area where insurers can benefit from financial institutions' experience with fighting account takeover. While just fewer than a quarter of financial institutions allow their customers to authenticate themselves with some method other than username and password at both login and for higher-risk activities — known as step-up authentication — fewer than a sixth of insurers offer this capability.

Even within step-up authentication, there are marked differences between the approaches of issuers and insurers. While both use one-time passwords as the most prevalent authentication methods for use when additional assurance of customer identity is needed, financial institutions tend to favor one-time password delivery by SMS text message, while insurers tend to deliver their OTPs via email (Figure 17).

Insurers Lag Behind FIs in Use of Non-Password Authentication

Figure 16. Authentication Methods Available for Login and Step-Up



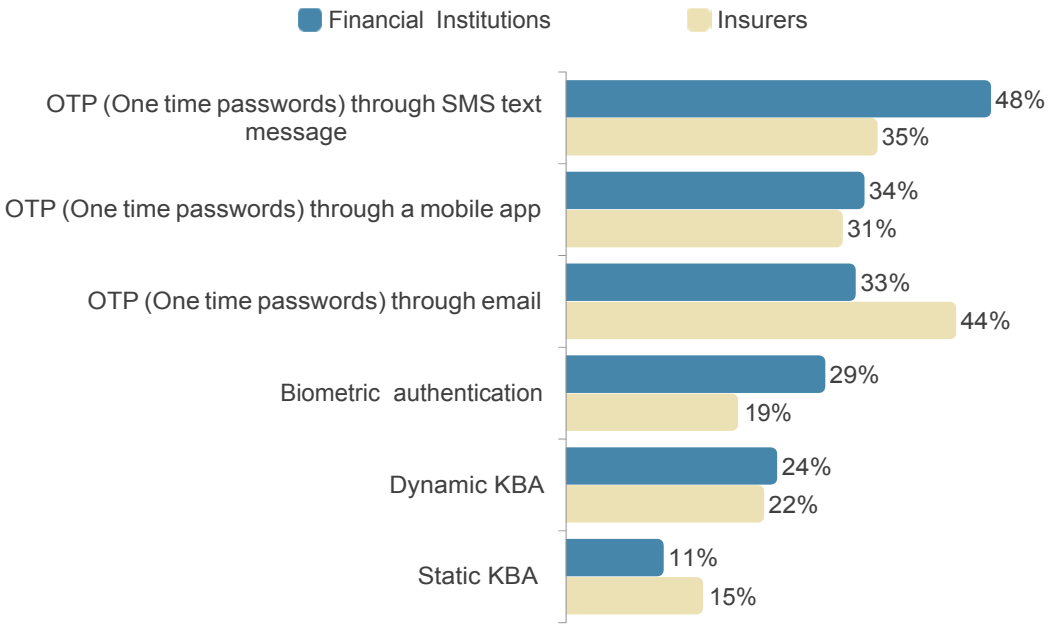
Source: Javelin Strategy & Research, 2018

Unfortunately, both of these methods are prone to interception through a variety of means. Prior to attempting to take over a financial account, fraudsters frequently target victims' mobile phone or email account with breached credentials or to abuse vulnerable password reset processes. With control over an email or mobile account, fraudsters can capture one-time passwords and successfully overcome authentication challenges. With these representing the two most common authentication challenges, it is no surprise that from 2016 to 2017, compromise of consumer email accounts in the U.S. rose by more than a third, and compromise of mobile phone accounts more than doubled.

Expanding use of biometric authentication is a key opportunity for both financial institutions and issuers, with 29% of FIs and just 19% of insurers using some biometric modality for step-up authentication (Figure 17). Not only do biometric modalities provide a smoother user experience than using one-time passwords, they are a tangible security control that can provide significantly more assurance that the user entering the authenticator is the same individual associated with the account — bolstering trust on the part of both the customer and the financial service provider.

Despite Vulnerabilities, SMS OTP Remains the Preferred Step-Up Authentication

Figure 17. Step-Up Authentication Capabilities



Source: Javelin Strategy & Research, 2018

[2] **2018 Identity Fraud: Fraud Enters a New Era of Complexity**, Javelin Strategy & Research, February 2018.

CONCLUSION

Digital transformation offers tremendous opportunities for financial services companies. Online and mobile banking makes it much easier for consumers to manage their finances and for financial institutions to consistently engage users and provide them with new tools such as mobile person-to-person payments. At the same time, new digital channel capabilities can open the door to fraud and security risks that threaten the trust that consumers have in banks and insurers.

This transformation is well under way, but many organizations have a long way to go. Progress is uneven across different sectors, as financial institutions and issuers lead the way and insurers are just beginning to modernize their services. This creates an opportunity for the latter to learn from the experiences of the former.

However, the pressure to modernize digital features is intense. Competitive pressures, customer expectations, and evolving fraud tactics require financial services companies to evolve quickly, often more quickly than they are able to easily handle. Fraudsters have also demonstrated themselves to be adept at targeting new services almost immediately after they are released, requiring financial institutions to proactively plan for how they will manage risk, rather than being reactive.

Successfully navigating the process of bringing a new product or feature to market requires implementing a comprehensive set of fraud controls that anticipate how both legitimate customers and malicious users will engage with the product. In both identity verification and authentication, financial services companies should move more fully toward a holistic and integrated identification and authentication capability, one that provides customers with the optimal mix of tangible security controls and the streamlined digital experiences they are accustomed to while still effectively countering fraudsters starting with the application and continuing throughout the customer life cycle.

METHODOLOGY

Enterprise data in this report is taken from a May 2018 survey of 300 financial institutions and insurers in the US (N = 150) and selected European Union countries (France: N = 50, Germany: N = 50, UK, N = 50).

Consumer data in this report is taken from a November 2017 survey of 5000 US adults. For questions answered by all 5,000 respondents, the maximum margin of sampling error is +/- 1.39 percentage points at the 95% confidence level.

ABOUT JAVELIN STRATEGY & RESEARCH

Javelin Strategy & Research, a Greenwich Associates LLC company, is a research-based consulting firm that advises its clients to make smarter business decisions in a digital financial world. Our analysts offer unbiased, actionable insights and unearth opportunities that help financial institutions, government entities, payment companies, merchants, and other technology providers.

Authors: Al Pascual, SVP Research and Head of Fraud & Security
Kyle Marchini, Senior Analyst, Fraud Management

Contributors: Sarah Miller, Research Manager – Custom Research & Operations
Crystal Mendoza, Production Manager

Editor: Mark Stevenson

Publication Date: September 2018

ABOUT IBM SECURITY

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 60 billion security events per day in more than 130 countries and has been granted more than 8,000 security patents worldwide. For more information, please check www.ibm.com/security.