Mitek

JAVELIN

CONSUMER PREFERENCE DRIVES SHIFT IN AUTHENTICATION

JULY 2021

PART OF THE ESCALENT FAMILY

TABLE OF CONTENTS

TABLE OF FIGURES

FOREWORD

This report, sponsored by Mitek Systems, explores shifting consumer preference in authentication methods and what financial services can do to both instill consumer confidence and maintain continuous authentication across the account and transaction life cycle.

This report is derived from the 2021 Identity Fraud Study: Shifting Angles, published by Javelin Strategy & Research in March 2021. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

2020 was a year that saw enormous change with little time for strategizing. What started as a two-week, temporary isolation transformed into a global lockdown and forever changed the way we work, educate, spend, and invest. Consumers were required to shift to digital channels for their payments and banking needs, from mobile deposits to remote loan origination. This also meant a change in how financial institutions were expected to authenticate consumers' identities. According to Javelin's 2021 Identity Fraud Study: Shifting Angles, combined identity fraud losses reached $56 billion in 2020, with many of those losses attributable to poor authentication during account access by the consumer.

Javelin believes that insufficient and/or lacking stepped-up authentication was to blame for the uptick in new account fraud, particularly within the automotive and mortgage-lending spaces. The need for advanced authentication continues to grow, as the threat of identity fraud and identity fraud scams escalates. Consumers also are showing increased interest in the use of biometrics for authentication, particularly because of the security and convenience they offer. Financial services should follow consumers' lead by providing layered authentication approaches that capitalize on consumers' interest in advanced authentication and delivering continuous authentication as a resilient defense against identity fraud and identity fraud scams.

EXECUTIVE SUMMARY

Consumer trust in static passwords dipped from 55% in 2019 to 45% in 2020. Additionally, one-time passcodes saw a 4% decrease in consumers' perceived effectiveness. Consumers appreciate the ease of use that traditional passwords and one-time passcodes offer, but they also recognize the risk involved with using those methods for authentication. An "optimal friction" experience provides better fraud defenses, and consumers finally have reached the tipping point of understanding that.

Confidence in biometrics authentication is steadily increasing. Consumers' perceived effectiveness of facial recognition (63%) and retinal scanning (62%) remained steady from 2019 to 2020, but voice recognition for the first time finally reached a 50% perceived effectiveness rate. This serves as a beacon to financial institutions and solutions providers that consumers are ready to begin accepting strengthened account security through biometrics.

Acceptance of biometric authentication will follow the implementation of more stringent passwords. Convincing consumers to adopt biometrics will be easy and inject less friction into the experience after they have grown accustomed to more stringent password adoption. What's more, Javelin data already shows consumers moving in this direction, with 60% saying they understand biometrics (specifically fingerprint scanning, voice recognition, facial recognition, and eye scanning) to be a more secure and reliable authentication method.

Adoption of layered security will make the case for biometrics. The adoption of layered authentication by financial institutions will push consumers toward the more frictionless authentication experience provided by biometrics. By employing numerous authentication and security measures, financial institutions will establish a robust identity fraud defense and reinforce consumer trust. And that trust will build confidence in biometrics.

23% of consumers describe themselves as early technology adopters. Understanding how the emerging technology works and having proven assurances of security go a long way toward fostering consumer trust. Tech-savvy consumers are often seen as ambassadors when it comes to technology and user-experience. As the number of consumers who provide positive feedback regarding advanced authentication experiences grows, so, too, will the number of consumers who willingly adopt new technology.

RECOMMENDATIONS

Phase out one-time passcodes. Given the ease with which criminals hijack one-time passcodes sent via text message or email and the drop in perceived effectiveness among consumers, it's clearly time to leave this authentication method behind and rely on more secure and convenient options.

Offer biometrics authentication, and educate consumers about its security benefits. Financial institutions should strongly consider requiring the use of biometrics for authentication. Replace more unstable authentication methods, such as one-time passcodes, with biometrics. Many consumers are already leveraging biometrics — from unlocking their mobile phones via touch ID or facial recognition to using voice recognition with virtual assistants like Amazon's Alexa and Apple's Siri. With proper notice, the shift to biometrics for account authentication will not be a challenge.

Employ continuous authentication. Financial institutions should verify the identity of a user throughout the interaction or session to ensure transaction security and authenticity. Use key data points, such as behavior-tracking, biometrics, and geolocation. Regular evaluations of fraud-detection solutions should also be performed to expose potential vulnerabilities and to safeguard against identity fraud and cybersecurity threats.

Prioritize adoption of voice recognition as a valuable biometric authentication method. Consumers want convenience and security in their login experiences, and it doesn't get much more reliable than biometrics. Because biometrics is already a part of the consumer, this creates a significant obstacle for criminals to overcome. There also is less friction for the consumers — all they have to do is be present. The rise in consumers' perception of the effectiveness of voice recognition should lead financial institutions to push for voice recognition as an authentication option for consumers.

Add friction to the experience. Friction is not always bad. In fact, layered authentication requires a little friction, and Javelin highly recommends this. As trust in passwords decreases and general biometrics trust increases, Javelin believes consumer acceptance of advanced authentication methods — even those that create more friction — will naturally increase. Financial institutions should immediately update password policies to introduce more stringent password requirements (e.g., length, multiple character types, etc.).

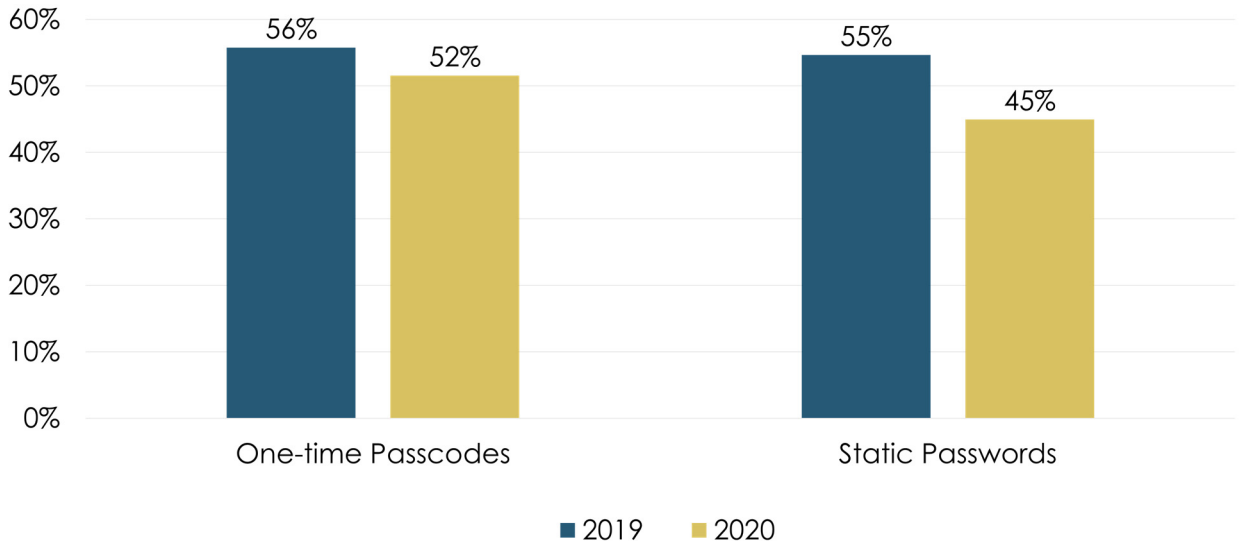
STEPPING AWAY FROM TRADITIONAL PASSWORDS

Static passwords once upon a time were deemed satisfactory tools to secure account access. Users could choose a word or phrase they could easily remember. They also turned out to be easy for cybercriminals to exploit as more personal information about consumers became readily available on the internet, via anything from public records to social media. Over time, passwords required more complexity. What once was a simple word, easy for a user to remember, took more effort to recall. In order to preserve a sense of simplicity and convenience, consumers often reused passwords across numerous platforms. The establishment of password managers aided in retaining some of that expediency and offered the ability to auto-generate strong passwords at the user's discretion.

An unfortunate fact remains: Even with advancing password technology like password manager solutions, consumers still recycle passwords. That proves to be particularly risky, as 22% of identity fraud victims had their passwords and email credentials stolen in 2020.[1] While 75% of

Traditional Account Authentication Methods Take a Hit

Figure 1. Perceived effectiveness of one-time passcodes and static passwords dips



Source: Javelin Strategy & Research, 2021

consumers say passwords are one of the easiest authentication methods, they also understand that passwords are easily compromised. Therefore, it's no surprise that static passwords' perceived effectiveness among consumers dropped 10 percentage points from 2019 to 2020. In an attempt to mitigate the risk of stolen log-in credentials, financial institutions should use this opportunity to focus on more secure biometrics authentication methods, which are significantly more difficult to steal or impersonate. This is a meaningful call to action for more modern and robust authentication adoption.

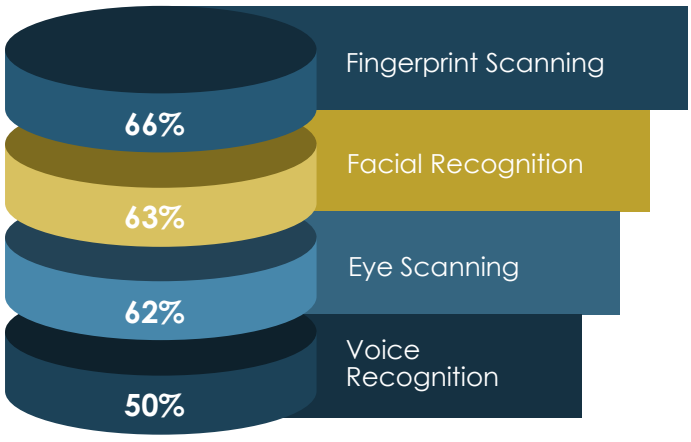
One-time passcodes also dropped in perceived effectiveness, from 56% in 2019 to 52% in 2020. Consumers realize that one-time passcodes are not the gold standard of authentication. This also suggests that consumers are beginning to acknowledge the need for and convenience of more advanced authentication methods. Consumers expect convenience and a bespoke user experience; memorizing long and complex passwords does not fit in with those expectations. Financial institutions must make the most of this moment of weakness for passwords and begin requiring the use of biometric authentication.

PREFERENCE DRIVES CHANGE IN AUTHENTICATION SOLUTIONS

Javelin data shows a clear growing consumer interest and trust in biometric authentication, as discussed above. Interestingly, only 23% of consumers describe themselves as early adopters of new technology. What's more, nearly half (44%) of consumers say they experience a level of apprehension when trying new technology as soon as it becomes available. A gap undoubtedly exists between the desire for convenient and secure authentication and the actual adoption of this technology. The solution is twofold. Consumers must accept and adopt technology more rapidly, and the way to make that happen is through increased trust built by financial institutions. Financial institutions and financial solution providers must demonstrate the value of advanced authentication through open and effective communication with consumers, in an effort to facilitate a faster adoption rate of more secure authentication methods. Voluntary consumer production pilots for newly developed technologies, regular interest surveys, and biometrics educational campaigns will encourage consumers to more readily embrace modern biometrics authentication.

Consumers Show Strong Acceptance of Advanced Biometrics Authentication

Figure 2. Consumers' perceived effectiveness of biometrics



While experiencing a dip from 2019 (73%), fingerprint scanning leads the pack in perceived effectiveness by consumers

Facial recognition software holds steady from 2019 to 2020 at 63%

Eye scanning remains at 62% as an effective authentication method

Voice recognition, for the first time, has reached a 50% effectiveness rating by consumers

Source: Javelin Strategy & Research, 2021

Though financial institutions are tasked with convincing a large population of hesitant consumers to try new authentication methods, an encouraging sign for the fight against fraud is consumer perception of the efficacy of biometrics authentication. Fingerprint scanning dipped from 73% in 2019 to 66% in 2020 but still floats to the top in terms of perceived effectiveness. Javelin suggests this decrease is due to the COVID-19 pandemic; as general trust in sanitization declined, consumers were apprehensive about physical contact with personal belongings, including mobile phones. Facial recognition (63%) and eye scanning (62%) each remain unchanged from 2019. And, for the first time, voice recognition has cracked the 50% mark.

A fundamental takeaway: Though consumers still consider static passwords the easiest authentication method, they clearly understand that some friction in the authentication process is a good thing, particularly if it means creating a formidable defense against fraud. Instead of focusing on establishing a frictionless experience, which could easily result in fraud risk, financial institutions should aim to design an "optimal friction" experience. This means introducing multiple layers of authentication that rely on advanced biometric technology. While this may require an adjustment period for consumers, the payoff of reduced fraud risk and robust security is invaluable.

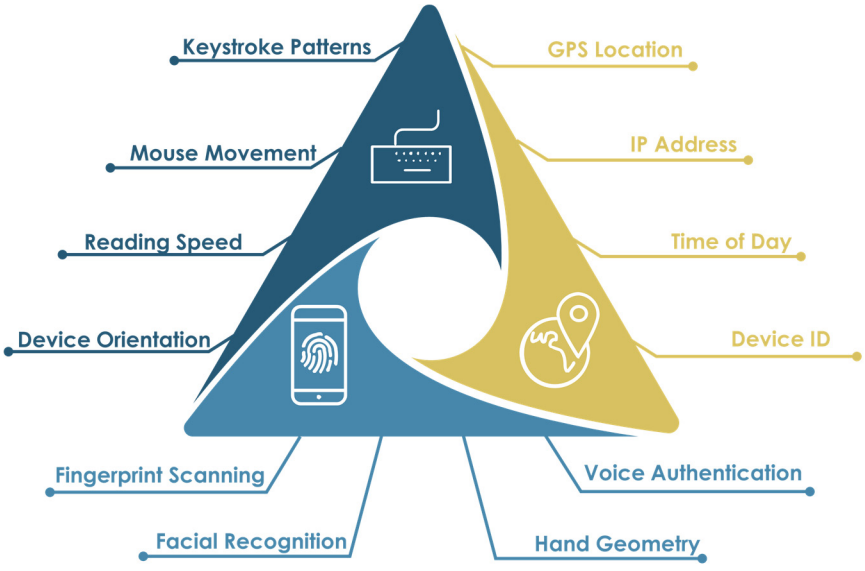
CONTINUOUS AUTHENTICATION — A FUNDAMENTAL REQUIREMENT

Authentication should not stop at a securely verified user login. A layered approach also does not simply mean just implementing biometrics or multifactor authentication. Continually verifying a consumer's identity throughout the session via a variety of checks will significantly reduce the chance of identity fraud or unauthorized account access.

Once the identity of a consumer is verified, the system should be consistently verifying and confirming that identity throughout the user's interaction. Behavioral analytics can provide insight into a consumer's usual habits and pinpoint anomalies. Using geolocation can determine if the user's location remains consistent with the device's location upon login. If there are any deviations from the typical login location, this also can be detected by geolocation. Biometrics such as facial recognition can confirm a consumer's identity through sessions with interactive teller machines or cardless ATM transactions.

Users Should Be Verified for Duration of Interaction to Mitigate Risk

Figure 3. Continuous authentication relies on many data points



Source: Javelin Strategy & Research, 2021

These methods are all effective on their own in identifying potential fraud attempts, but criminals will work to no end to get around these security checkpoints. Financial institutions should consider a risk-tiered approach to layered security, introducing friction and additional authentication layers. When these measures are employed together throughout the entire session, criminals will have a considerably more difficult time gaining unauthorized account access.

The responsibility for moving toward advanced account authentication does not lie only with financial institutions. While FIs play a critical role in providing secure options for consumers to adopt, consumers also must be willing to take the appropriate steps in accepting biometrics as the future of authentication. They have already shown that there is growing trust in these methods, and the next step is to actually use them.

Consumers should be made to feel as though they aren't just along for the ride but that their opinions matter; many system enhancements are developed to fill gaps in the user experience. Financial institutions will see improvements in adoption of biometric authentication if they engage consumers in the process. Allow for participation in development and rollout of new biometrics technology, and educate consumers about advanced authentication, as well as account security and personally identifiable information privacy assurances.

Consumers will see the value in additional friction within the authentication process, when institutions are able to demonstrate convenience and security associated with these methods. With adoption of continuous authentication, layered security, and a stepped-up authentication approach, financial services firms will be in good position to maintain durable fraud defenses and increase consumer trust and engagement.

METHODOLOGY

In October 2020, Javelin conducted a nationally representative online survey of 5,000 U.S. consumers to assess the impact of falling victim to fraud, uncover where fraudsters are making progress, explore consumers' actions and behaviors, and identify segments of consumers most affected by fraud.

ENDNOTES

1. Javelin Strategy & Research. Published March 2021. https://www.javelinstrategy.com/coverage-area/2021-identity-fraud-study-scams

ABOUT MITEK

Mitek (NASDAQ: MITK) is a global leader in mobile capture and digital identity verification built on the latest advancements in computer vision and artificial intelligence. Mitek's identity verification solutions enable organizations to verify an individual's identity during digital transactions to reduce risk and meet regulatory requirements while increasing revenue from digital channels. More than 7,500 organizations use Mitek to enable trust and convenience for mobile check deposit, new account opening, and more. Mitek is based in San Diego, Calif., with offices across the U.S. and Europe. Learn more at www.miteksystems.com. Follow Mitek on LinkedIn, Twitter, and YouTube, and read Mitek's latest blog posts here.

ABOUT THE AUTHOR

Suzanne Sando
Senior Analyst
Fraud Management

CONTRIBUTORS:

Jacob Jegher
President

Tracy Kitten
Director, Fraud & Security

Crystal Mendoza
Production Manager

ABOUT JAVELIN

Javelin Strategy & Research, part of the Escalent family, helps its clients make informed decisions in a digital financial world. It provides strategic insights to financial institutions including banks, credit unions, brokerages and insurers, as well as payments companies, technology providers, fintechs and government agencies. Javelin's independent insights result from a rigorous research process that assesses consumers, businesses, providers, and the transactions ecosystem. It conducts in-depth primary research studies to pinpoint dynamic risks and opportunities in digital banking, payments, fraud & security, lending, and wealth management. For more information, visit www.javelinstrategy.com. Follow us on Twitter and LinkedIn.

JAVELIN