GIVING CONSUMERS CONTROL AND ENHANCING FRAUD PREVENTION

OCTOBER 2021

PART OF THE ESCALENT FAMILY

TABLE OF CONTENTS

Foreword 3
Overview 3
Executive Summary 4
Recommendations 5
Digital channel use accelerated by pandemic 8
Fraud Reduction Gives Consumers a Sense of Control 10
Educate Consumers about Fraud and Scams 14
Strengthen Authentication: Employ Behavioral Biometrics 15
Methodology 17
About Experian 17
About Javelin Strategy & Research 18

TABLE OF FIGURES

Figure 1. Use of Mobile Wallets and P2P Payments Has Increased Since 2018, Especially among Younger Consumers. 8
Figure 2. Consumer Sentiment Regarding Various Forms of Data Collection. 10
Figure 3. Consumers Will Share Personal Information to Reduce Fraud. 11
Figure 4. Consumers Will Leave a Business or Close an Account Because of a Breach, Even if PII Was Not Compromised. 13
Figure 5. FIs and Businesses Must Clearly Explain the Benefits of Behavioral Biometrics to Ensure Consumer Opt-In 15

FOREWORD

This report, sponsored by Experian®, explores how the COVID-19 pandemic accelerated consumers' use of digital channels, which in turn has presented increased fraud risks. This has necessitated the need for financial institutions to implement stronger controls on identity proofing and consumer authentication, as well as more effective fraud prevention and consumer empowerment educational campaigns.

This report was adapted from two U.S. consumer surveys conducted by Javelin Strategy & Research in June 2020 and October-November 2020, as well as a survey of cybersecurity professionals conducted in May 2021. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

The COVID-19 pandemic accelerated consumers' transition to digital channels. What's more, consumers increasingly desire numerous options that give them more control over their financial affairs in ways that are personalized to their individual needs. Thus, providers of financial services have been forced to quickly transition to accommodate the shift toward digital. A big part of that control relates to fraud prevention. Offering consumers numerous authentication options — physical biometrics, one-time passcodes, multifactor, etc. — as well as various options of fraud-prevention empowerment (via text and email alerts with balance updates, transaction history, and suspicious activity, to name a few) also improves the customer experience.

EXECUTIVE SUMMARY

The pandemic accelerated consumer adoption of mobile wallets and peer-to-peer (P2P) payments. One of the biggest shifts Javelin noticed last year was in younger consumers' use of P2P payments. Adoption of such payments saw the greatest increase among consumers ages 18 to 34, a group that already had the highest usage.

By 2020, consumers across all generations were using more digital channels. While the 18-to-34 age group stood out in P2P payments, mobile banking also showed an uptick for this group, with 94% saying they conducted a mobile banking transaction in 2020. Along with that, 84% of consumers ages 35 to 54 said they, too, conducted a mobile banking transaction last year. Even among the 55-plus category, a majority (54%) in 2020 said they used mobile banking.

Consumers want to play more active roles in preventing fraud. This again points to consumers' ongoing desire for more education and involvement when it comes to fraud detection, prevention, and resolution. They highly favor the ability to sign up for fraud alerts and notices, which allows them to track their transaction and account activity as well as account balances in real time.

Consumers are much more privacy-aware. Transacting and interacting in a predominantly digital way for a good part of 2020 put consumers at greater risk online as well as at a greater risk of fraud. While there is never a "positive" side to falling victim to fraud, consumers who were victimized did become more aware of the cyber risks they faced in 2020, because they saw upticks in fraud. Consumers in 2020 used social media and telecommuting platforms on a much broader scale, communicating with family and friends as well as learning and working. As a result, they were much easier for criminals to target, especially with scams. Consumers felt the pain, attributing $43 billion of the $56 billion in reported 2020 ID fraud losses in 2020 to scams.[1]

Consumers need to understand how data collection and behavior tracking improve security. Consumers don't like having their personal information tracked, especially when they don't know or understand how that information is being used. Among U.S. consumers, 60% say they are uncomfortable with the collection of their personally identifiable information and images/photographs from mobile devices.[2]

Consumers are OK with device and location monitoring if it prevents fraud. Nearly half (45%) of consumers say they are very comfortable having their device and location monitored if it also prevents fraudulent activity.[3] If consumers clearly understand the security benefits of tracking

their personal information, data usage, and behaviors, their comfort with and interest in such tracking improve dramatically.

Consumers blame FIs for fraud. When consumers suffer a fraud loss, they will blame the institution, even if that loss is linked to a scam that falls outside the purview of the institution's or business's responsibility. In 2020, 38% of consumers say they closed the bank account affected by fraud, and 69% say their primary FIs did not resolve their fraud concerns or losses.[4]

Fraud is the No. 1 reason consumers leave an FI or change how they interact with it. The second most likely reason is a breach, even if PII and/or other information was not stolen. This supports why empowering consumers to play a role in fraud prevention is vital. Fraud prevention improves the customer experience and is a win for the FIs, because fraud prevention reduces customer/member attrition.

RECOMMENDATIONS

Push consumers toward taking responsibility for their digital behaviors. Clearly explain the benefits of stronger authentication, such as behavioral biometrics authentication. Consumers would embrace behavioral biometrics if organizations were transparent about how and why they are being used. 59% of U.S. consumers say they are "very comfortable" with having their devices and locations tracked *if* doing so will help prevent fraud.[5] Transparency about data collection and usage should be part of consumer cybersecurity and anti-fraud education.

Empower consumers to prevent fraud. Help consumers play more active roles in preventing fraud by educating them about activity such as scams. Empower consumers with tools that help them to assist institutions and businesses in detecting suspicious activity before it results in fraud. Text, email, and voice notifications, which raise flags for consumers if and when transaction amounts or account balances are outside the norm, are essential first steps. By offering a security hub, where consumers can monitor transactions more readily, institutions empower consumers to play more active roles in fraud prevention. In the hub, consumers can turn on alerts, set card controls for transaction limits, notify their FI of travel plans, and manage mobile banking apps, just to name a few options.

Educate consumers about emerging scams. Javelin defines a scam as any action taken by a criminal to directly influence a consumer to divulge personal information or conduct transactions that expose their PII.[6] Scams flourished during the height of pandemic-induced isolation, because they directly targeted consumers. Consumers are ultimately responsible for fraud losses that result from scams, so educate them about what to look for and how to avoid falling victim. That will help prevent a poor customer experience if fraud does occur and will help to build and develop trust with the FI.

Develop a playbook for fraud resolution and breach response. A well-developed plan for fraud resolution and breach response should include how to work with consumers when fraud occurs. It also should fall under the purview of existing planning for disaster recovery and business continuity, which many companies had to quickly revamp as the pandemic raged. A response plan including fraud, cyber and marketing/communications teams will prepare your company to act quickly. A well-thought-out response in the event of fraud also will help to build consumer confidence in the institution.

Encourage acceptance of behavior tracking. Behavioral biometrics, which involve the tracking of behaviors, locations,

and device usage, to name a few, is an effective way to reduce fraud and cybersecurity risks. But consumers must be convinced. Educate consumers with digital videos about the benefits of behavioral biometrics, which include device monitoring, data tracking, and behavior tracking over time. Be mindful that it's an uncomfortable notion for consumers to have their movements tracked. This is why building a strong, trusting relationship with consumers is so critical for FIs. Consumers will be more apt to allow the tracking of their behaviors if they trust the entity tracking them. What's more, the creation of a unique and personalized profile can distinguish a consumer's legitimate activity from illicit activity. If consumers understand how behavioral biometrics is used to create such a unique and personalized profile, which in turn will reduce fraud, they will be more likely to accept them.

Don't just encrypt data; strengthen perimeter security. Organizations must strengthen perimeter security, which requires strong cybersecurity. Strong perimeter security also ensures safe interactions with consumers. Even if personal information is protected, consumers will perceive a penetration of the network as a breach and will be more apt to stop doing business with that entity.

DIGITAL CHANNEL USE ACCELERATED BY PANDEMIC

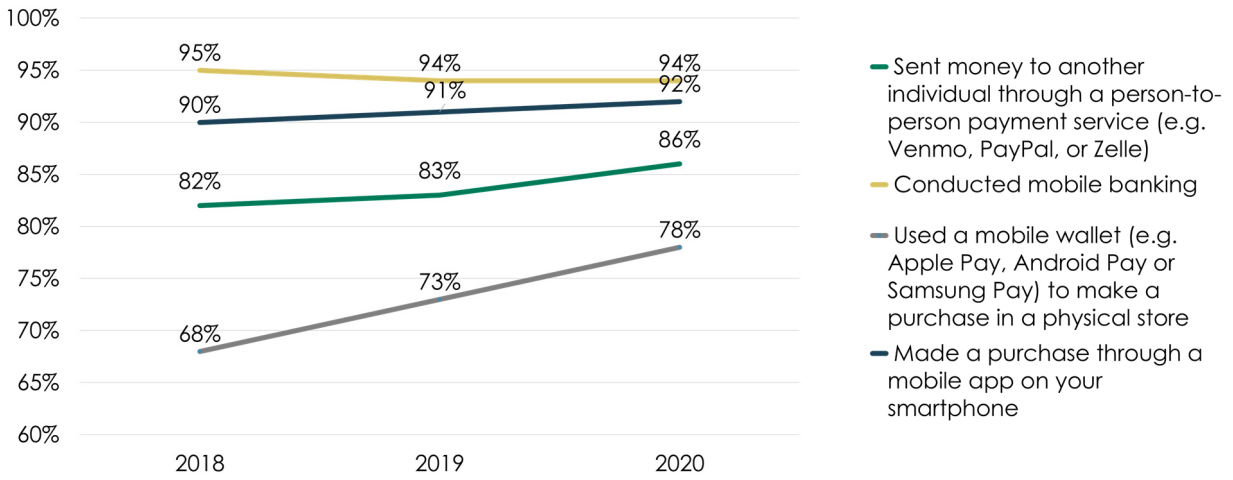
The COVID-19 pandemic accelerated consumers' transition to digital channels as well as their expectations for the user experience. In turn, it forced financial-services providers to quickly transition their offerings to accommodate that digital shift, including more effective and modern online and mobile options for such things as account opening, loan origination, and mobile check deposit. P2P payments also took on more prominence as consumers were forced into isolation; these payment methods also subjected consumers to heightened fraud risks linked to scams. But even before the pandemic, consumers' preferences for payments and account access had moved toward digital.

Consumers want convenience, which means ample choices and channels that are easy to use and make them feel like their experiences are personal. They also want to have control over the data being collected and the privacy measures put in place to prevent fraud.

A big part of that control relates to digital privacy options and fraud prevention. Offering consumers numerous authentication options—physical biometrics, one-time passcodes, multifactor, etc.—is critical. Consumers also want the ability to personalize their fraud prevention via various options, such as text and email alerts for balance updates,

Majority of Consumers across Age Groups Today Use Digital Channels

Figure 1. Use of Mobile Wallets and P2P Payments Has Increased Since 2018, Especially among Younger Consumers



Source: Javelin Strategy & Research, 2021

transaction history, and suspicious activity, to name a few. All of these things improve the customer experience.

The primary message for financial institutions is simple: Fraud prevention is the key. More transactions across more channels expand the footprint for fraud. In 2020, fraud losses spiked, primarily because of increased digital activity and transactions. Fraud losses in 2020 totaled $56 billion, up from $17 billion in 2019.[7] It will be a fine balance, as financial-services providers want to ensure a positive customer experience. The best way to strike that balance is by empowering and educating consumers about fraud prevention. Help consumers play more active roles in preventing fraud by educating them about activity such as scams and how their data is collected. Empower them with tools that will help detect suspicious activity before it results in fraud. Offer consumers a security hub, where they can turn on alerts, set card controls for transaction limits, notify their FI of travel plans, and manage mobile banking apps, just to name a few options. Credit monitoring also should be offered in the hub, so consumers can track credit inquiries or if their Social Security numbers have been used to apply for new accounts. The security hub is a necessary tool and a prime example of fraud-prevention empowerment. Fraud prevention improves the customer experience and should be deemed a partnership, because FIs and consumers have a common interest in preventing fraud.

To that end, the acceleration toward digital channels and the significant uptick in fraud losses in 2020 support the need for more education and empowerment. One of the biggest shifts Javelin noticed last year was in younger consumers' use of P2P payments. Adoption of such payments saw the greatest increase among consumers ages 18 to 34.[8] This also happens to be the age group with the riskiest digital behaviors—the greatest use of social media, the greatest willingness to share personal information on social media, and the greatest tendency to accept friend requests from strangers. But by 2020, consumers across all generations were using digital channels and making more purchases online.

While the 18-to-34 age group stood out in P2P payments, mobile banking also showed an uptick for this group, with 94% saying they conducted a mobile banking transaction in 2020. Along with that, 84% of consumers ages 35 to 54 said they, too, conducted a mobile banking transaction last year. And for both age groups, the use of mobile wallets and P2P payments have increased since 2018. Only the 55-plus category lags behind where adoption of digital channels is concerned. But even among that group, a majority (54%) in 2020 said they used mobile banking.

That all should be concerning to institutions and other businesses in terms of shopping behaviors. PayPal, as an example, is often used in e-commerce for faster checkout. But the use of these types of P2P platforms increases the number of endpoints that must be monitored for suspicious activity. These P2P channels also put merchants at risk when they're used for faster checkout.

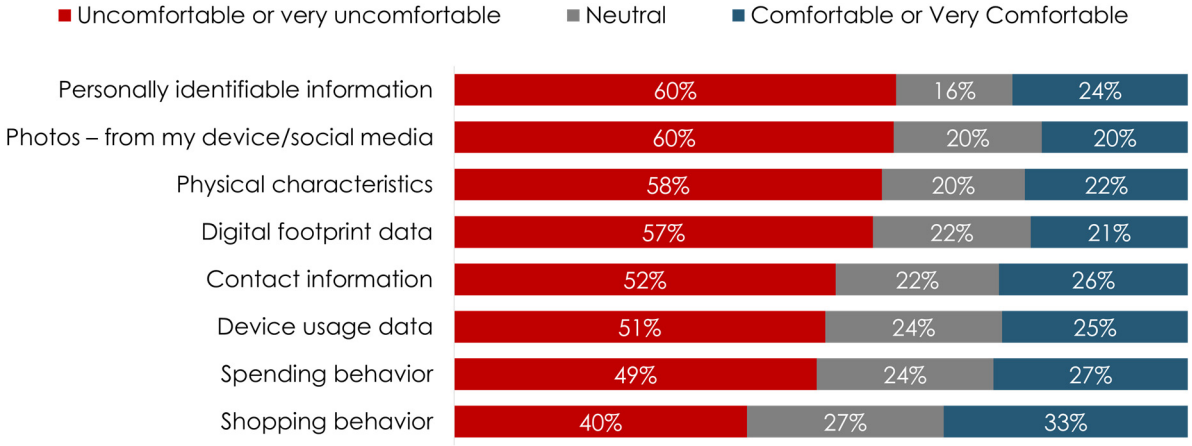
FRAUD REDUCTION GIVES CONSUMERS A SENSE OF CONTROL

Consumers want options in how they transact and bank. This is why we've seen the adoption of digital offerings such as P2P payments steadily increase. This also plays into fraud reduction and why offering consumers multiple options is so critical, especially when it comes to how they are authenticated.

Consumers' desire for more options and control has been progressively increasing since the advent of online and mobile banking. And the pandemic accelerated that desire. Today, because of heightened digital channel use, which in 2020 was widely exploited by criminals, consumers are much more privacy-aware. Privacy awareness also has been fueled by the significant number of data breaches publicized in the media. Even if a consumer's PII is not compromised and/or fraud does not result from a so-called breach, consumers are on heightened alert. Transacting and interacting in a predominantly digital way for a good part of 2020 put consumers at greater risk. While there is never a positive side to falling victim to fraud, consumers who were victimized did become more aware of the cyber risks they faced in 2020, because they saw upticks in fraud. Consumers in 2020 used social media and telecommuting platforms on a much broader scale, communicating with family and friends as well as learning and working. This also made them much easier for criminals to target, especially through scams. Consumers felt the pain, as

Consumers Are Broadly Uncomfortable with Data Collection

Figure 2. Consumer Sentiment Regarding Various Forms of Data Collection



Source: Javelin Strategy & Research, 2021

$43 billion of the $56 billion in reported 2020 ID fraud losses was attributed, by consumers themselves, to scams.[9]

Cybersecurity and fraud awareness were already on an upswing, prompting consumers to demand more control over how their personal information and data are tracked and used;[10] the pandemic just accelerated that awareness. More than half of consumers are uncomfortable with the idea that someone is tracking their PII, the photos they store on their smartphones or post on social media, their physical characteristics, their digital footprints, their contact information, and their device usage (see Figure 2).

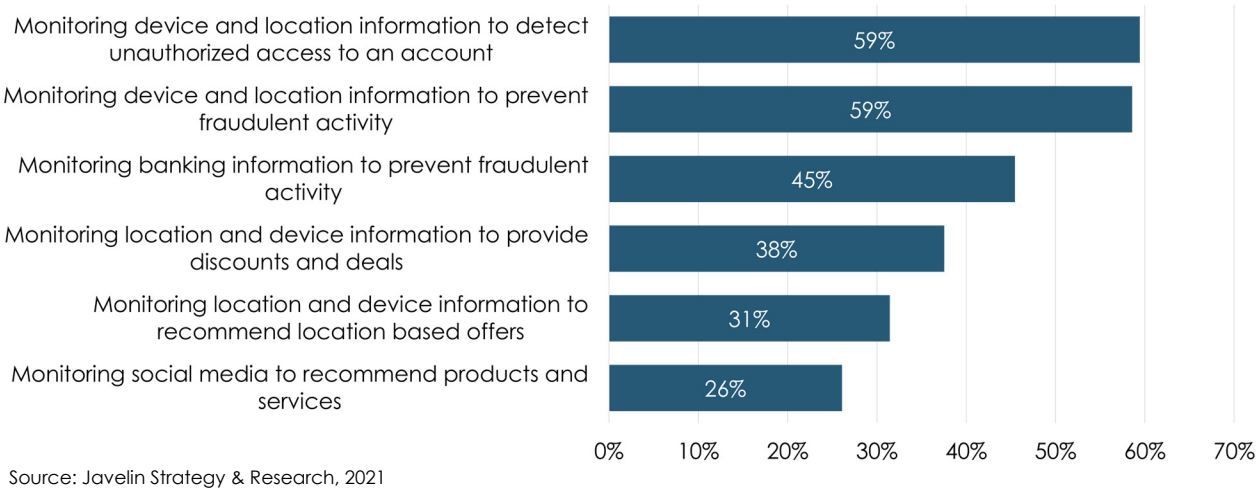
Among U.S. consumers, 60% say they are uncomfortable with having their PII and images/photographs from mobile devices and social media collected.[11] That's not surprising, given that most scams targeting consumers last year were waged via social media platforms and SMS/text messages. (See Why Scams Are a Growing Threat to Financial Institutions, https://www.javelinstrategy.com/coverage-area/why-scams-are-growing-threat-financial-institutions.)

That increased awareness of cyber risks is a double-edged sword. Consumers want heightened protections, but they don't want their personal information tracked, as they see such tracking as putting them at greater risk. This heightens the need for FIs to demonstrate how data collection and behavior tracking actually enhance and improve security. The message for financial institutions is clear: Consumers and FIs benefit when fraud is reduced, and if consumers can be given control in reducing fraud, they're more likely to buy in.

An interesting shift in consumer acceptance of personal data tracking takes place when the benefits of fraud prevention are clearly outlined and explained (see Figure 3). Nearly six in 10 consumers say they are very comfortable with a business monitoring their device

Education Can Push Consumers to Accept PII Tracking

Figure 3. Consumers Will Share Personal Information to Reduce Fraud



Source: Javelin Strategy & Research, 2021

and/or location activity if doing so more readily detects unauthorized account access. What's more, nearly half (45%) of consumers say they have high comfort with monitoring of their banking information if it prevents fraud. Compare that with the consumers' discomfort with having PII, photographs, digital footprint and device-usage tracked and collected (See Figure 2). The takeaway is simple: If consumers clearly understand the security benefits of tracking their personal information, data usage, and behaviors, their comfort with and interest in such tracking improve dramatically.

Fraud is the No. 1 reason consumers leave a business, change the way they interact with that business, or close an account where fraud occurred. If consumers suffer a fraud loss, they typically will blame the institution, even if that loss is linked to a scam that falls beyond the institution's or business' responsibility. In 2020, nearly 70% of consumers who reported suffering a fraud loss said their primary FIs did not resolve their fraud concerns or losses. And 38% said they closed the bank account affected by fraud.[12]

The second most likely reason, and one that should be equally concerning to FIs, is a breach, even if PII and/or other information was not stolen. This is why having a solid plan for fraud response and breach resolution, which falls under the purview of an existing business-continuity/ disaster-recovery plan, is so important. Consumers need to know and trust that even if a network intrusion does occur, their data is safe. And that the institution or business has a solid plan for mitigating losses and assisting with resolution if data is breached.

A couple of things are worth noting from these findings. First, fraud reduction is the best way to retain customers and members. Second, consumer perception of cybersecurity plays a major role in attrition and retention. Even if personal information is protected, if an organization is attacked or its network is penetrated, consumers are more likely to stop doing business with that institution, even if no data was actually compromised.

Consumer cybersecurity and fraud-prevention empowerment is paramount. It drives 22% of consumers' satisfaction ratings with online banking.[13] The COVID-19 pandemic forced consumers to curtail their normal routines and rely more on digital channels and payments. Losses stemming from ID fraud scams, a category of fraud that Javelin began tracking in 2020, totaled a whopping $43 billion.[14] These scams underscore the adage that criminals follow the path of least resistance. In this case, criminals exploit consumers directly with texts, emails, and phone calls—thereby bypassing an FI's traditional fraud-detection barriers. In a nutshell, these criminals socially engineer consumers, convincing them to give out PII that ultimately results in fraud.

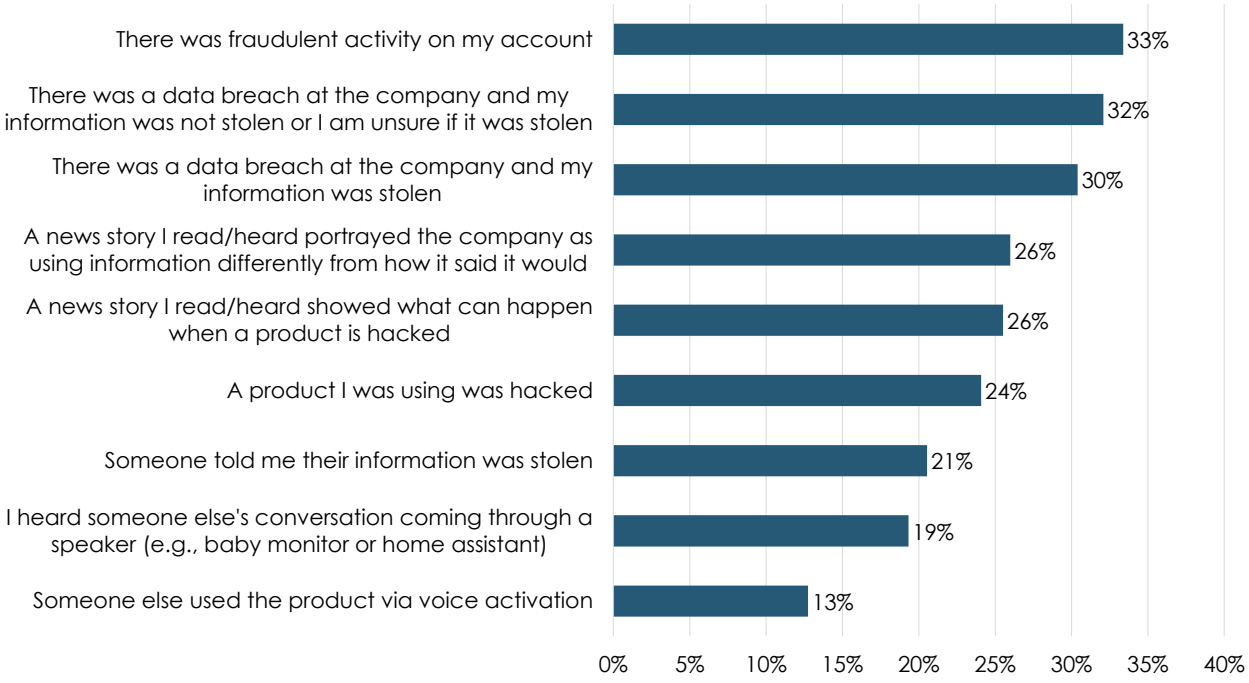
The financial damage of these scams demonstrates the necessity of a prominent, open, plain-language conversation that

treats customers as partners in Javelin's three phases of the fight against fraud: prevention, detection, resolution.

Organizations must strengthen perimeter security, which requires strong cybersecurity and ensures safe interactions with consumers. Even if personal information is protected, consumers will perceive penetration of the network as a breach and will be more likely to stop doing business with that entity.

Data Breaches are Primary Drivers of Data Privacy Concerns

Figure 4. Consumers Will Leave a Business or Close an Account Because of a Breach, Even if PII Was Not Compromised



Source: Javelin Strategy & Research, 2021

EDUCATE CONSUMERS ABOUT FRAUD AND SCAMS

Humans truly *are* the weakest links in the cybersecurity chain. But they don't want to be.

This is why education about cybersecurity, safe online and mobile practices, the need for strong authentication, and an overall understanding of scams and how they target consumers is so important. Javelin has been preaching this message throughout 2021 and will continue to push the importance of cyber and anti-fraud education in 2022. That consumers need more education about scams and how they socially engineer victims based on unique and personal qualities and characteristics is a given. They also need to understand that so much of their personal data already is available on the dark web because of data breaches that have spanned the past decade. This, too, makes it much easier for criminals to target consumers because they have enough information about them to personalize their scams and messaging.

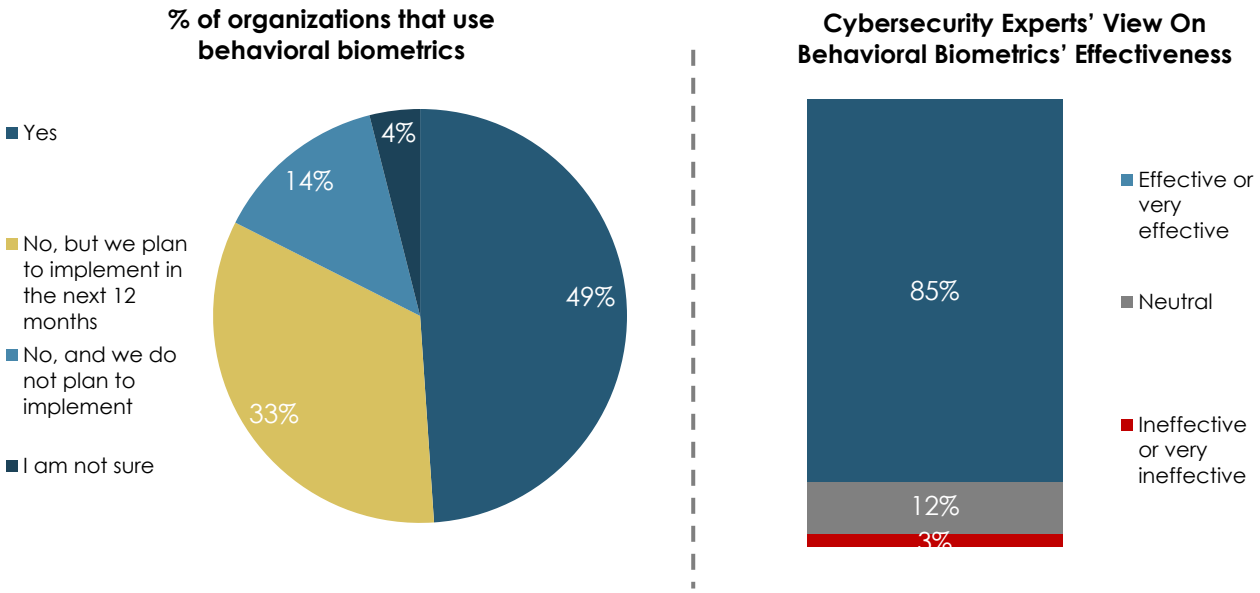
Scams flourished during the height of pandemic-induced isolation, as those scams directly targeted consumers. Consumers are ultimately responsible for fraud losses that result from scams, so educate them about what to look for and how to avoid falling victim. Any time consumers must cover their own fraud losses, it's a poor client experience. Educational videos posted in digital banking are a great place to start. But don't forget the empowerment piece. Provide customers and members with access to a security hub, where they can access educational materials, sign up for alerts regarding balance updates, enable real-time transaction notifications, and set card limits for transactions, just to name a few options. Credit monitoring also should be offered in the hub, as previously noted. Consumers must be provided the ability, in a centralized place, to track things like credit inquiries for new-account applications and openings. Give consumers control.

STRENGTHEN AUTHENTICATION: EMPLOY BEHAVIORAL BIOMETRICS

Education also plays into the use and adoption of behavioral biometrics. Behavioral biometrics, which track a consumer's device usage, geolocation, keystrokes, etc., are an effective way to reduce fraud and cybersecurity risks without creating a lot of friction. Consumers do not have to do anything beyond their normal "behaviors" to be authenticated via behavioral biometrics. Unfortunately, fewer than half of organizations surveyed by Javelin say they are using behavioral biometrics as part of a layered authentication strategy (see Figure 5). Their logic is that consumer acceptance has been low. Organizations don't see a need to implement if consumers aren't willing to have their information and behaviors tracked. But with proper education about the fraud-prevention benefits of behavioral biometrics, many consumers can be swayed.

Behavioral Biometrics Is Favored by Cyber Experts, but Adoption Lags

Figure 5. FIs and Businesses Must Clearly Explain the Benefits of Behavioral Biometrics to Ensure Consumer Opt-In



Source: Javelin Strategy & Research, 2021

While 85% of the cyber and IT specialists Javelin polled in May 2021 say they deem behavioral biometrics to be an effective or very effective way to reduce fraud and cyber risk, only 49% say their organization is using them. Consumers' worries about the tracking of data and PII are clearly driving, and in most cases hindering, the use of behavioral biometrics. That's unfortunate, because with proper education about the effectiveness of behavioral biometrics, consumers would undoubtedly opt in. And because behavioral biometrics add no friction for the consumer, their use does not adversely affect the client experience, meaning consumers do not have to take additional steps to authenticate themselves. Behavioral biometrics work on the back end, so it is an authentication layer that is invisible to the user. And while behavioral biometrics should be just one layer used to authenticate a user or transaction, they can be highly effective at reducing fraud.

Many consumers will embrace behavioral biometrics if organizations are transparent about how and why they are used. This should be part of an overall cybersecurity and anti-fraud education campaign that outlines what personal information is being tracked and how it is being stored. These types of disclosures can be sensitive, but it is the job of cybersecurity and marketing/communications teams to come up with effective campaigns that provide consumers with knowledge. That said, the messages must take care to avoid tipping off cybercriminals about ways to circumvent the system. Post videos with simple, understandable messages about how tracking a user's location could quickly raise a flag regarding suspicious activity, or how understanding a user's typical shopping behavior over time could lead to the detection of an anomaly and proactively prevent fraud.

The digital-first experience is here to stay. Put consumers in the driver's seat and give them control over their digital identities. Build trust through transparency and education to drive the adoption of data-collection methods and help them understand how they can play active roles in fraud prevention. Doing so will improve the customer experience—meaning consumers will be much less likely to leave, even in the wake of a fraud event.

METHODOLOGY

The data in this report was collected from three surveys, two of U.S. consumers and one of a random sample of cybersecurity professionals across numerous industry verticals.

- U.S. consumer privacy survey conducted in June 2020 of 2,006 U.S. consumers. The margin of error is +/-2.19 percent at the 95% confidence level.
- The 2020 ID Fraud survey, conducted between Oct. 30 and Nov. 16, 2020, of 5,000 U.S. consumers. The maximum margin of sampling error is +/- 1.41 percentage points at the 95% confidence level. For questions answered by all victims of identity fraud, the maximum margin of sampling error is +/- 3.22 percentage points at the 95% confidence level.
- U.S. cyber professionals survey conducted in May 2021 of 500 IT decision-makers across financial services, retail, telecommunications, information technology, and health care.

ABOUT EXPERIAN

Experian Partner Solutions is the provider of the most comprehensive platform powering financial and identity services for more than 220 partners and 114 million active consumers. Experian Partner Solutions' mission is to help partners better serve their customers with capabilities and services that help consumers achieve better financial wellness and protection of their identity. Through illuminating every facet of value, Experian drives bigger outcomes, uncovers new opportunities, and provides ongoing value for businesses and customers.

ENDNOTES

1. https://www.javelinstrategy.com/coverage-area/2021-identity-fraud-study-scams, Javelin Strategy & Research. March 2021.
2. https://www.javelinstrategy.com/coverage-area/ethics-behavioral-biometrics%C2%A0, Javelin Strategy & Research. December 2020.
3. https://www.javelinstrategy.com/webinar/ethics-behavioral-biometrics,Javelin Strategy & Research. August 2021.
4. https://www.javelinstrategy.com/coverage-area/2021-identity-fraud-study-scams, Javelin Strategy & Research. March 2021.
5. https://www.javelinstrategy.com/coverage-area/rising-cyber-awareness-changing-consumer-privacy-profiles, Javelin Strategy & Research. February 2021.
6. https://www.javelinstrategy.com/coverage-area/2021-identity-fraud-study-scams, Javelin Strategy & Research. March 2021.
7. https://www.javelinstrategy.com/coverage-area/2021-identity-fraud-study-scams, Javelin Strategy & Research. March 2021.
8. https://www.javelinstrategy.com/coverage-area/rising-cyber-awareness-changing-consumer-privacy-profiles, Javelin Strategy & Research. February 2021.
9. https://www.javelinstrategy.com/coverage-area/2021-identity-fraud-study-scams, Javelin Strategy & Research. March 2021.
10. https://www.javelinstrategy.com/coverage-area/cybersecurity-implications-californias-consumer-privacy-act-why-everyone-needs-be, Javelin Strategy & Research. February 2020.
11. https://www.javelinstrategy.com/coverage-area/ethics-behavioral-biometrics%C2%A0, Javelin Strategy & Research. December 2020
12. https://www.javelinstrategy.com/coverage-area/2021-identity-fraud-study-scams, Javelin Strategy & Research. March 2021.
13. https://www.javelinstrategy.com/coverage-area/2021-online-banking-scorecard, Javelin Strategy & Research. June 2021.
14. https://www.javelinstrategy.com/coverage-area/2021-identity-fraud-study-scams, Javelin Strategy & Research. March 2021.
15. Javelin Strategy & Research Cybersecurity Survey. Javelin Strategy & Research. Fielded 500 cybersecurity executives and IT specialists across five industry verticals, including financial services and retail. May 2021.

ABOUT THE AUTHOR

Tracy Kitten
Director, Fraud & Security

CONTRIBUTORS:

Jacob Jegher
President

Crystal Mendoza
Production Manager

ABOUT JAVELIN STRATEGY & RESEARCH

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