DIGITAL CONVERGENCE AND FRAUD:
CONNECTING THE DOTS

November 2020

Independently produced by:

JAVELIN

PART OF THE ESCALENT FAMILY

TABLE OF CONTENTS

TABLE OF FIGURES

FOREWORD

This report, sponsored by FIS, explores the risk that financial institutions are experiencing as a result of consumers' adoption of technology through the usage of devices, digital tools, and social media.

This report was adapted from the *2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis.* Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

Consumers are reshaping their online behaviors today with a fast-moving adoption of digital payments, including increased usage of banking apps and money movement products as well as frequent participation on multiple social media platforms. As consumers increase their digital footprint, they are essentially increasing their own risk of exposure to criminal schemes. Poorly secured consumer devices and repurposed account logins and passwords underscore the need for businesses to deploy stronger fraud detection and prevention strategies.

Every entry point where the consumer interacts digitally with their financial services provider has to be completely secure out of necessity to the consumer experience and to reduce the impact identity fraud will have on the business. A failure to properly authenticate consumer identity throughout the entire digital experience will lead to more fraud losses and eventual attrition. Digital behaviors and activity, when possible, should be evaluated across multiple devices and platforms to maximize fraud detection while increasing consumers' trust through stronger fraud prevention.

EXECUTIVE SUMMARY

KEY FINDINGS

Fraud victims are much more digitally connected than the average consumer. Fraud victims have 33% more connected devices than consumers who have not experienced identity fraud. The overall security risk in self-protecting personal devices, depending on the manufacturer and personal security measures, is impossible to scale for the average consumer and can lead to more vulnerabilities and loss of personally identifiable information (PII).

Cumulatively, the increase in multiple access points coupled with the increased number of devices and social media accounts makes fraud easier to commit. Credential stuffing, sim swapping, and social engineering to facilitate account takeovers are all made easier by access to publicly shared data that resides on platforms that may not execute appropriate security protocols, leaving consumer information vulnerable to theft.

Fraud victims have disproportionately high trust in the security of payment channels. 34% of identity fraud victims are more likely to believe storing card credentials online is secure. Another 23% of fraud victims still think making a browser-based purchase online is secure.

Fraud victims are super users of social media platforms. Criminals often target their victims through social media platforms. More than half of all fraud victims use popular social media platforms like Facebook, Instagram, and Twitter, where they have been exposed to scams like phishing attacks, recruitment of money mules, and account takeover fraud.

Fraud victims have a higher confidence in protecting themselves from financial fraud. A higher ownership of digital devices combined with an overly optimistic point of view regarding personal safety may be the reason 79% of fraud victims (compared with 60% of all consumers) think they have a good understanding of how to protect themselves against financial fraud. This overt optimism enables consumers to form a false sense of security in matters that require much-needed improvement.

Cybersecurity vulnerabilities are not always exploited immediately by criminals. It is a common practice for criminals to delay exploiting a vulnerability to increase their profits by allowing more consumer victims to fall into their technological trap. Criminal dormancy also leads to higher instances of zero-day efficacy, as cybersecurity experts fail to identify vulnerabilities because there are no fraud indicators driving their research for solutions.

Anti-malware protection isn't enough to protect against identity fraud. Victims of identity fraud are not that different from their non-victim counterparts when it comes to leveraging an anti-malware scanning product. While the usage of anti-malware products is considered essential, they cannot solely defend a consumer from identity fraud.

Criminals are circumventing more secure browser-based fraud prevention models by targeting consumers' mobile devices instead. Malicious mobile apps are being used to mimic financial institutions' interfaces and steal login credentials. Malicious apps can also intercept SMS messages to collect PII, harvest one-time passwords, and bypass two-factor authentication.

The dark web has played a major role in the proliferation of identity fraud. The dark web has evolved into a primary hub for criminals to buy and sell customer data and to disseminate information and technologies to bypass fraud detection strategies. This information highway is fueled by the sale of consumer PII.

RECOMMENDATIONS

Companies should develop and enable new enterprise-wide password standards. Criminals exploit consumers' tendency to reuse the same password across multiple sites, creating an enormous risk for credential-stuffing attacks. Companies should build upon the password standard of eight digits and characters to prevent consumers from using popular and easy-to-crack password combinations.

Implement dark web monitoring to proactively protect consumers. Dark web monitoring includes both identifying consumer data for sale and tracking when that data is sold. Tracking when data is sold also serves as a powerful early-warning system that one or more consumer accounts could be at risk for payment fraud or account takeover.

Ensure that identity verification and fraud management capabilities span all consumer-facing banking channels. Good practices, such as continuous authentication using behavioral biometrics for browser-based banking, can be rendered ineffective by insufficiently secured mobile banking channels. Because criminals will preferentially target the least-secure access points, strong security in only one banking channel is insufficient to deter fraud.

Monitor social media sites for suspicious activity. Criminals' increasing tendency to identify targets using social media can be turned against them if financial institutions work with social media companies to identify and respond to these threats.

Promote the safety of only using authenticated digital apps. Consumers need to understand the risks associated with unauthorized versions of digital apps. Online distractions and a tendency to be more influenced by postings they see on their peers' social media accounts make consumers more vulnerable to downloading counterfeit applications containing malware.

Eliminate knowledge-based authentication questions. The abundance of opportunities for criminals to take over consumer accounts through the usage of PII collected and purchased from a variety of public sources and illicit cyber sources make knowledge-based questions completely ineffective in deterring criminal access to personal financial accounts.

Offer account passphrases to supplement existing authentication practices. Allow consumers to select a passphrase that can be permanently appended to their contact records. When consumers initiate account access via customer service, they will be asked to correctly identify their security passphrase in addition to meeting other authentication criteria.

Socialize consumers about the dangers of *malvertisements* and click-bait. Consumers need to understand that dangers lurk behind look-alike online ads, which can contain links to harmful malware and counterfeited websites. One click in the wrong place can easily expose consumers to SQL injections and key-logger malware that captures every keyboard entry. It makes perfect sense to develop a few visuals to show consumers how misleading (and seemingly identical) advertisements and websites can be.

DIGITALLY SAVVY CONSUMERS EXPERIENCE GREATER LEVELS OF FRAUD

Consumers are exhibiting greater usage of digital channels for personal business and entertainment today by making more payments using peer-to-peer (P2P) products and services such as Facebook Pay. As consumers increase their use of multiple social media platforms for communication and entertainment, they are also conducting myriad digital banking and e-commerce transactions to help solve the problem presented by social distancing and the need to manage personal lives and busy households. The growing consumer demand for digital connectivity serves as a constant reminder that P2P payments and digital wallets have become essential components in the daily lives of consumers. Most of the challenges that are faced by financial institutions today fall squarely on each organization's ability to provide a seamless and safe client experience, as trust in banking remains tantamount to the continued success of the digital transformation.

In nearly all cases, victims of fraud are inordinately likely to be more digitally connected than the general population. This connectedness falls short, however, as 30% of fraud victims indicate that they would like to receive fraud alerts and account notifications less frequently. This admission alone highlights a mismatch between consumer preferences and an obvious need for increased account activity awareness.

Fraud Victims Are Often Tech-Savvy Early Adopters

Figure 1. Which of the Following Best Describes Your Actions When a New Technology Becomes Available?

Source: Javelin Strategy & Research 2020

Adding more reason for concern is the fact that 79% of fraud victims think they have a good understanding of how to protect themselves from fraud. This creates a false sense of capability where much room for improvement is needed.

The reticence to interact with financial service providers on account-related matters could be linked philosophically to the overall trust victims of fraud have placed on virtually every transaction activity, ranging from ATM withdrawals to saving payment information online. (See Figure 2).

The perception of tech-savvy consumers that payment channels are safe until proven otherwise is a perfect example of why consumers need guidance conducting their personal business using safer practices.

There are sizable gaps in the level of trust victims of fraud and their non-victim counterparts place in payment channel behaviors. Fraud victims generally trust payment channels at rates 11 percentage points to 41 percentage points higher than those of non-victims. This prevailing optimism on the part of fraud victims needs to be fortified with increased monitoring capabilities by financial service providers, which will help facilitate a safer experience that ultimately affects whether long-term adoption of more digital behaviors will continue.

Millions of U.S. consumers access social media in varying degrees throughout the day. In a relatively short period, consumers have adopted countless online platforms from Facebook to TikTok, where they seek entertainment, gather information, and pursue their special interests.

Fraud Victims Have Disproportionately High Trust in All Payment Channels

Figure 2. Measure of Trust Across Multiple Payment Channels

Source: Javelin Strategy & Research 2020

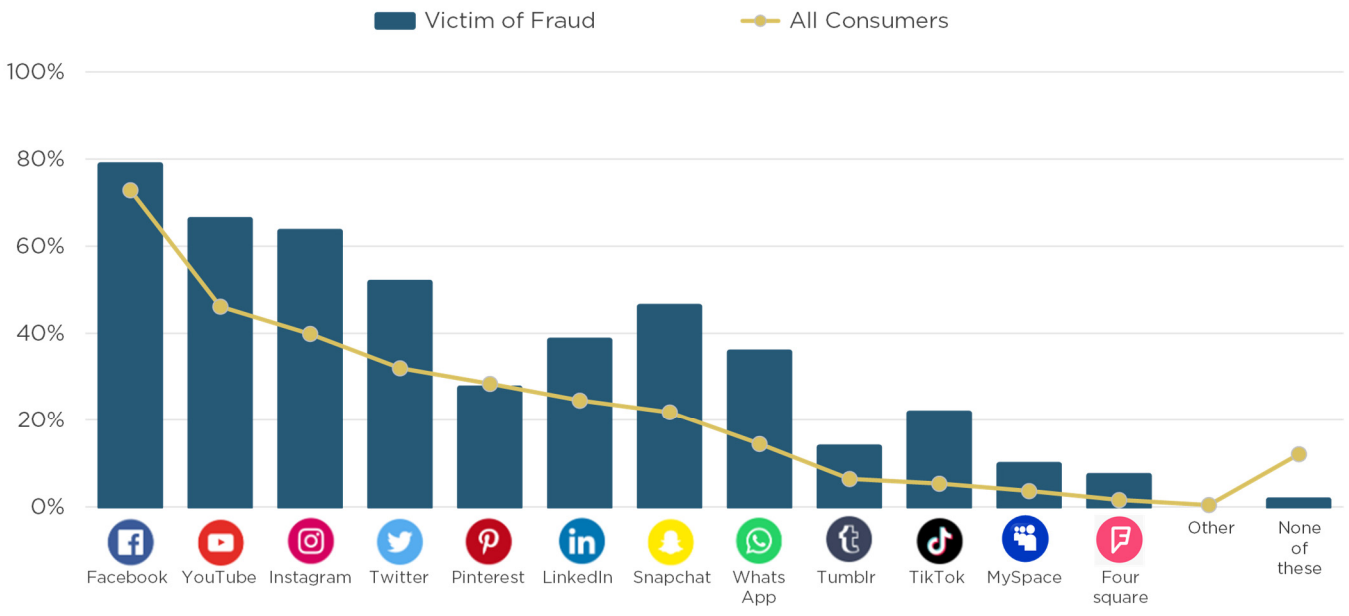
As consumers become more familiar with each social media platform, they may find themselves inadvertently sharing more personal data online regularly. A typical consumer who embraces social media with great dexterity may not understand the dangers of oversharing. Most of the personal information posted by consumers online resides in the open public domain with little protection from criminals, who are then able to harvest the information for identity fraud schemes through page views and direct messaging with the consumer.

The aggregation and wholesale monetization of consumer information seamlessly move from social media platforms to dark web marketplaces, where the information is used to fuel the dark web economy. Consumer information, however liberally spread throughout social media, often takes on a critical mass in the form of full account takeover, P2P payment fraud, and criminal control of consumer mobile and email accounts. The disadvantage here is clear for financial institutions that do not execute heightened monitoring and analysis of consumer online behavior.

There is a need to protect and nurture tech-savvy consumers with added security in order to facilitate strong long-term digital growth. Dark web intelligence offers financial institutions the ability to identify consumers with compromised credentials and to prepare fraud teams for potential fraud on those accounts.

Social Engineering, Scams, and Phishing are Made Easier with Social Media Connectivity

Figure 3. Social Media Adoption by Fraud Victims Compared with Non-Victim Consumers



Source: Javelin Strategy & Research 2020

LAYERS OF PROTECTION ARE THE NEW SILVER BULLETS

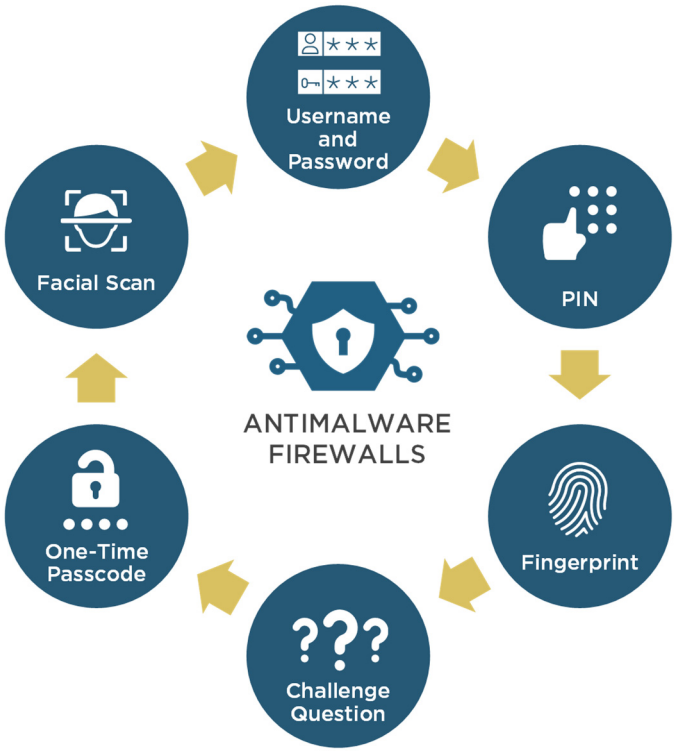
Digitally savvy consumers may not always engage with their primary financial services provider with the same enthusiasm that they leverage digital products. Identity verification and fraud management capabilities need to span multiple channels to protect the consumer and the organization and counteract the underlying threats of risky digital behavior and the relentless harvesting of information by criminals.

Sometimes the actions that consumers take to protect themselves are not always correctly executed or entirely effective at preventing the myriad criminal attack vectors that target multiple channels.

Anti-malware scanning and firewalls, as an example, are almost equally deployed by fraud victims (65%) and all other consumers (72%), but the overall effectiveness falls short as a

Fraud Victims' Security Habits Do Not Differ Greatly from Those of Non-Victims

Figure 4. Most Consumers Use the Same Methods for Identity Proving and Device Protection



Source: Javelin Strategy & Research 2020

standalone solution for preventing identity fraud, giving consumers a false sense of security. Login and authentication practices for both fraud victims and non-victims are universally accepted but require heightened monitoring and specialized tactics to facilitate more digital adoption. It's clear that the presence of static passwords, antiquated challenge questions, and repurposed user credentials are hindrances to consumers despite their obvious familiarity and universal usage.

Deploying a singular tactic like anti-malware scanning is not enough protection to handle the multiple payment and information platforms used by consumers today. As more consumers embrace contactless payment opportunities, their risk for fraud increases through newer payment channels like P2P and mobile banking.

During the 2020 COVID-19 pandemic, consumers have been demonstrating their need for payment products that accommodate their need for social distancing and for consumer staples that may be available only through digital channels. P2P payment fraud, according to Javelin's report *Securing P2P Payments*, has increased more than 700%. The risk that consumers are facing with less-than-secure personal security habits coupled with the need to adopt newer digital payment channels has compressed responsibility for protecting the consumer directly on the shoulders of the financial services provider.

CONNECTING THE DOTS: USHERING IN A NEW ERA FOR SAFER PAYMENTS

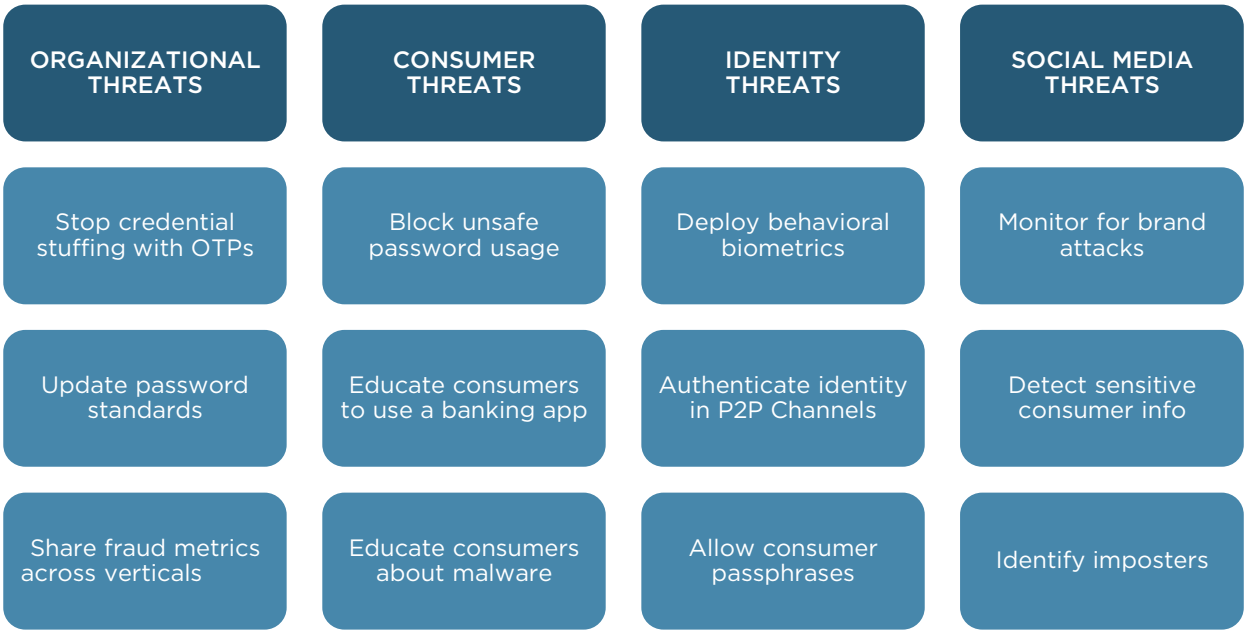
As consumers rely more on digital banking and payment channels, financial institutions are finding themselves in the new territory of bringing cybersecurity practices to each consumer connection point. Financial institutions and payment organizations spend considerable time and resources on protecting the ecosystem, but there is substantial room for improvement. Successful organizations will need to find the resources necessary to usher in a new era for safer payments that consumers can embrace with confidence.

Digital payments will continue to expand, so the tactics deployed by financial institutions need to encapsulate identity management and transaction monitoring along with a specialized focus on preventing consumer information from falling into the hands of criminals, thus fueling the dark web economy.

There is an absolute necessity for verticals to communicate and work together to prevent the onslaught of fraud created by overlapping criminal schemes. Anti-money-laundering departments should work closely with P2P fraud prevention teams to help battle organized

Creating Stronger Consumer Security and Authentication

Figure 5. How Financial Service Providers Can Increase Overall Security



Source: Javelin Strategy & Research 2020

criminals groups that seek to take over P2P payment products and move illicit funds.

Continuous identity validation will be necessary at every connection point where the consumer encounters a digital product login.

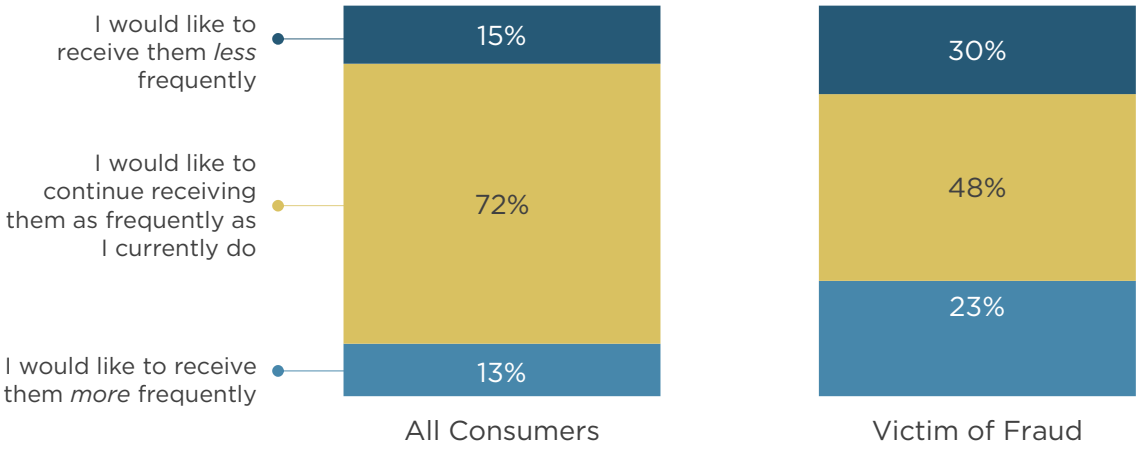
Brand protection will be required to counteract the proliferation of counterfeit banking apps and spoofed websites. Consumers will need to be socialized to deploy stronger forms of security protection at home and within the confines of social media platforms.

The Herculean tasks involved in coordinating a safer digital adoption have to begin with increased threat monitoring and risk strategy from a centralized location. A combination of consumer awareness, resourcefulness by financial service providers, and a long-term focus on redirecting consumers to safer digital habits will pave the way for a wider digital convergence with fewer dots to connect.

APPENDIX

Attitude Toward Account Alert Notification Frequency

Figure 6. Consumer Attitude Toward the Frequency with Which They Received Alerts and Notifications Over the Past Year



Source: Javelin Strategy & Research 2020

Fraud Victims Own More Connected Devices than Non-Victims

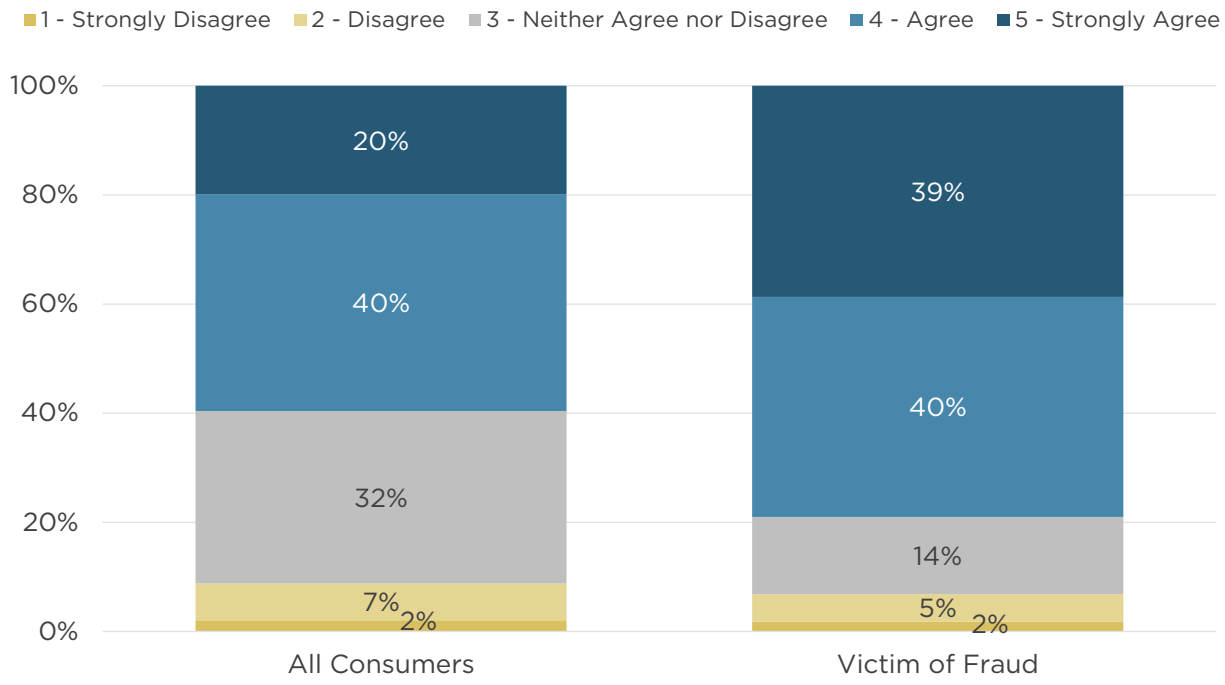
Figure 7. Devices Consumer Own in Their Household

Connected Device	All Consumers	Victim of Fraud
Internet-connected fitness equipment (Peloton)	2.1	2.9
Internet-connected appliances (Nest thermostat)	2.0	2.9
A smartphone	2.0	2.6
Voice assistants (Google Home)	1.8	2.0
Internet-connected TV or set-top box (Roku)	1.8	2.3
Mobile phone (NOT a smartphone)	1.7	2.5
Tablet	1.7	2.5
Wearables (Google Glass, Fitbit)	1.7	3.2
A laptop or Chromebook computer	1.7	3.0
Smartwatch (Apple Watch)	1.7	3.3
A desktop computer	1.4	2.2

Source: Javelin Strategy & Research 2020

Fraud Victims Misjudge Their Ability to Protect Themselves

Figure 8. Consumers' Level of Agreement Regarding Ability to Protect Themselves Against Financial Fraud



Source: Javelin Strategy & Research 2020

METHODOLOGY

The 2019 ID Fraud survey was conducted online among 5,000 U.S. adults over the age of 18; this sample is representative of the U.S. Census demographics distribution. Data collection took place from Oct. 22 through Nov. 4, 2019. Data is weighted using 18+ U.S. population benchmarks on age, gender,race/ethnicity, education, census region, and metropolitan status from the most current CPS targets.

ABOUT JAVELIN STRATEGY & RESEARCH

Javelin Strategy & Research helps its clients make informed decisions in a digital financial world. It provides strategic insights for financial institutions, government, payments companies, merchants, fintechs and technology providers. 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, and lending. For more information, visit javelinstrategy.com. Follow us on Twitter and LinkedIn.

Author: John Buzzard, Lead Analyst, Fraud & Security

Contributors: Paul McCormack, Senior Adviser
Alexander Franks, Cybersecurity Analyst
Jacob Jegher, President, Javelin
Krista Tedder, Director of Payments
Crystal Mendoza, Production Manager

Publication Date: November 2020

ABOUT FIS

FIS is a leading provider of technology solutions for merchants, banks and capital markets firms globally. Our more than 55,000 people are dedicated to advancing the way the world pays, banks and invests by applying our scale, deep expertise and data-driven insights. We help our clients use technology in innovative ways to solve business-critical challenges and deliver superior experiences for their customers. Headquartered in Jacksonville, Florida, FIS is a Fortune 500® company and is a member of Standard & Poor's 500® Index.