AARP®

JAVELIN

IDENTITY FRAUD:
SUSCEPTIBILITY IS NOT SPECIFIC TO AGE

AUGUST 2021

PART OF THE ESCALENT FAMILY

TABLE OF CONTENTS

TABLE OF FIGURES

FOREWORD

This report explores the risk that identity fraud scams have on U.S. adults aged 50+. As criminals pursue multiple targets in their quest to steal personally identifiable information, there is a complete lack of regard for the person who loses his or her identity. There is no code of ethics that draws a line of acceptable behavior that cannot be crossed. This latest exploration of identity fraud, sponsored by AARP, will draw parallels between the actions of criminals and the overall effect those actions can have on victims of identity fraud and identify fraud scams.

Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

Though scams may vary across generations, all groups are prime targets for criminals. The impact of identity fraud scams on victims affects their quality of life, financially and emotionally. Those who experience scams are often reluctant to report the crimes out of shame that makes them feel incapable of handling their personal business affairs. The truth of the matter is that any person of any age can be ensnared by identity fraud and identity fraud scams. U.S. adults aged 50+ are in some ways faring better than other generations, due in part to their vigilance and cautious examination of contact with persons unknown to them. The stakes for U.S. adults aged 50+ are higher than for other age groups, however, as the average losses in an identity fraud scam tend to be higher for those who have accumulated more wealth and physical assets during their lifetime.

Being able to identify criminal red flags is a positive step toward reducing the incidence of identity fraud. Equal importance should be placed on the role provided by financial service providers to offer education and problem resolution as lifelines to identity fraud victims.

EXECUTIVE SUMMARY

Among US adults aged 18-49, 37% cite a severe effect on their lifestyles after experiencing identity fraud. Younger generations have more debt and tend to struggle with underemployment issues that magnify the problems associated with identity fraud.

US adults aged 50+ are less likely than younger generations to be victimized by identity fraud scams. Scams affected 38% of victims aged 18-49 in comparison to 18% of those 50+ who may have been aided by a growing knowledge about self-protection and stronger device security habits.

Identity fraud losses continue to grow as criminals adapt their tactics to consumers' lifestyles. Identity fraud losses in 2020 totaled $56 billion (USD). This figure represented a combined total of $13 billion (USD) for traditional identity fraud (down 21% from 2019) and $43 billion (USD) for identity fraud scams, which Javelin measured for the first time in 2020.

Tech-support scams are claiming more victims aged 18-49. 22% of US adults aged 18 to 49 experienced more tech-support scams than US adults aged 50-65 (13%) and 65+ (14%). Tech-support scams always begin with some form of unsolicited phone call or screen pop-up message that conveys urgency and prompts the victim to click on a dangerous link or provide the criminal with remote access to the victim's device.

US adults aged 65+ did not engage with criminal scammers in three specific incidences. Javelin discovered that criminals were not very successful in persuading US adults aged 65+ to participate in identity fraud scams involving gift cards and debt collection schemes, and face-to-face contact. Fake or stolen gift cards affected just 10% of US adults aged 50- 64; within that same demographic, 8% experienced debt-collection scams, and 13% reported actual face-to-face contact with criminals.

29% of American consumers aged 50+ made purchases online for goods and services that never existed. American consumers aged 18-49 did not fare any better, with similar numbers of consumers making purchases online for goods and services that did not exist. During the COVID-19 pandemic, there was such an incredible demand for protective gear and cleaning supplies that many consumers resorted to blindly trusting online entities for much-needed personal items.

Bill payment fraud is a growing threat to consumers. Bill payment fraud affected a wide stratum of consumers, with 21% of US adults aged 65+ experiencing bill payment fraud, a higher percentage than US adults aged 50-64 (13%). Bill payment fraud

happens when a criminal sends a falsified invoice to a potential victim and demands, for example, payment for a past-due utility bill or carpentry work.

Money-movement fraud affects more US adults aged 18-49. Fraud losses stemming from peer-to-peer payments (P2P), such as Venmo or Cash App, affected 21% of consumers aged 18-49. Older consumers fared much better, with 14% of consumers aged 50-64 and 19% of consumers aged 65+ reporting fraud within the same P2P category.

Impostor scams remained a huge problem in 2020. US adults aged 50+ reported speaking to an impostor during a phone call more so than younger generations. Criminal impostors often pose as government officials or other persons of authority in an effort to persuade victims to divulge information or to deceive them into performing funds transfers for urgent expenses.

RECOMMENDATIONS FOR FINANCIAL SERVICE PROVIDERS

Use new terminology for describing victims of identity fraud. Criminals clearly have no conscience when it comes to targeting people—their goal is simply financial gain and manipulation when it comes to identity fraud. Financial service providers (and others) who are interested in removing the stigma from identity fraud need to be more conscious about the words they choose to describe victims. Eliminating phrases that suggest the victim is responsible for having been defrauded is the first step in liberating victims to seek counsel with trusted advisors without shame or fear of financial ruin.

Learn how to identify the red-flag behaviors of identity fraud victims. Financial service providers and trusted caregivers need to familiarize themselves with behaviors exhibited by most identity fraud victims. Being able to spot the early stages of criminal manipulation can lessen the impact felt by victims in terms of financial loss and shame. Changes in behavior like increased spending, unusual secrecy, and unexplainable urgency are more obvious to spot with some increased sensitivity.

Focus on account-takeover fraud (ATO). Those who perpetrate Identity fraud have a high degree of affinity for ATO fraud. As consumers embrace technology and adopt digital behaviors across multiple platforms, their risk increases for ATO. Financial institutions need to ensure that supporting technology is in place to help identify behavioral and device anomalies that are typically consistent with ATO and identity fraud.

Automate fraud reporting across apps and other digital channels. Consumer frustration can often begin with the process of reporting unusual activity on an account. Identity fraud victims, if unassisted by identity-protection services, are often working by themselves to resolve their fraud situation. Financial service providers need to realize that a streamlined process for reporting fraud is necessary within branded banking apps and other online options. Consumers should be able to quickly flag a transaction and report it as fraud without having to cross over to a browser-based option.

RECOMMENDATIONS FOR CONSUMERS

Ignore requests for urgent forms of payment. Consumers need to understand that urgent requests for payment from someone they have never met face-to-face are immediate red flags. Equally important consideration should be given any time a stranger asks for an unusual form of payment, such as gift cards, as payment for debts and urgent matters.

Protect passwords and login information with the same consideration given to your medical information. Usernames and overly-simple passwords are risky elements. Varying usernames and marrying them to more complex and varied passwords is a much safer alternative. Writing down password hints and usernames and keeping them in a safe location can also be a low-tech solution for consumers who are afraid of forgetting multiple combinations. Tech-savvy consumers can also utilize password managers.

Avoid communicating with strangers about serious matters. People who have never physically met before are technically strangers, to varying degrees. Criminals can adopt a series of personas designed to deceive consumers into trusting them, so it is still never a good idea to discuss highly confidential or financially sensitive matters with unknown parties.

Verify everything and follow up at a later date. Identity thieves count on several elements to optimize their theft of consumer information. The faster a criminal incites a consumer with threatening or financially lucrative ploys the more chances they have to be successful as criminal impostors. To curtail this classic behavior simply hang up, disconnect, go offline and verify with legitimate business partners and others whether a matter requiring attention truly exists.

THE CRIMINAL RACONTEUR: TELLER OF TALES

Javelin's *2021 Identity Fraud Study: Shifting Angles* explored traditional identity fraud along with a contemporary categorization for identity fraud originating from scams. Javelin's study revealed that Identity fraud losses in 2020 totaled $56 billion (USD). This figure represented a combined total of $13 billion (USD) for traditional identity fraud (down 21% from 2019) and $43 billion (USD) for identity fraud scams, which Javelin measured for the first time in 2020. The increase in overall fraud losses and a renewed focus on identity fraud scams necessitated a change in how Javelin analyzes identity fraud. As criminal tactics have changed over the years, the consumer has become an intense focal point as the path of least resistance to criminal success. Javelin found it necessary to redefine identity fraud into two tactics—the traditional means of fraud and scams—to best reflect how criminals have changed their approaches in the years since the inception of this study.

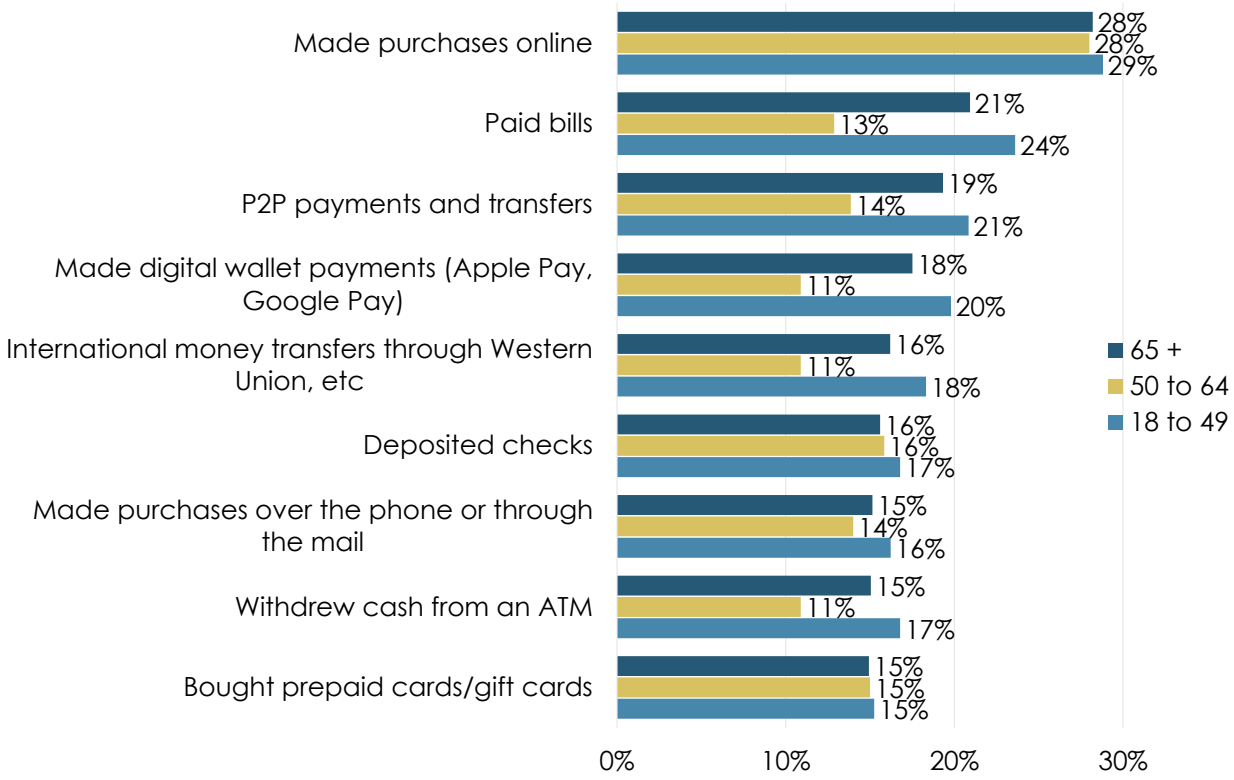
The routine theft and usage of consumers' personally identifiable information (PII) for criminal profit is still regarded by Javelin as traditional identity fraud. When it comes to traditional identity fraud, consumers have a scant perspective on the exact time and technique used by criminals to steal their information; they simply understand that a loss of PII occurred, resulting in financial damage that they must resolve. Identity fraud scams, on the other hand, are relatively easy to orchestrate and present an opportunity for criminals to bypass the fraud-detection barriers maintained by financial services providers by directly targeting consumers. A noteworthy characteristic of identity fraud scams is that consumers often recall the moment they interacted with a criminal, for example, through a text, a call, or an email.

Criminal scammers are successfully persuading consumers to perform a variety of actions that result in financial losses (see Figure 1). Just more than a quarter of American consumers (28%) aged 50+ made purchases online for goods and services that never existed. During the COVID-19 pandemic, there was such incredible demand for protective gear and cleaning supplies that many consumers resorted to blindly trusting online entities for much-needed personal items.

American consumers aged 18-49 did not fare any better, as 29% of them also made purchases online for nonexistent goods and services. Bill payment scams also affected a wide stratum of consumers, with 21% of US adults aged 65+ experiencing bill payment fraud, a higher percentage than those 50-64 (13%). Bill payment scams typically happen when a criminal or impostor contacts a potential victim and

Generational Losses During the Execution of an Identity Fraud Scam

Figure 1. Criminals Have More Success with Consumers Ages 18-49



Source: Javelin Strategy & Research, 2021

demands direct payment for a past-due utility bill, as an example.

The contact with the crook can be via email, phone, or in-person, and the sheer urgency of losing essential utilities is just one trigger that results in a successful identity fraud scheme for the criminal. Sadly, many consumers are reluctant to report fraudulent or suspicious contact because they are left feeling responsible for the actions of the criminal, just one of the emotional byproducts for victims to process. No one wants to feel like they were incapable of making good decisions, especially when those feelings are magnified by the perceived judgment of others. As identity fraud victims shoulder self -doubt and shame, they can spiral into moral distress that leads to feelings of toxic anger, social isolation, and even suicide.

The ability of the perpetrator to suspend the consumer's disbelief is part of the process of identity fraud scams and why they are successful. The "teller of tales," in

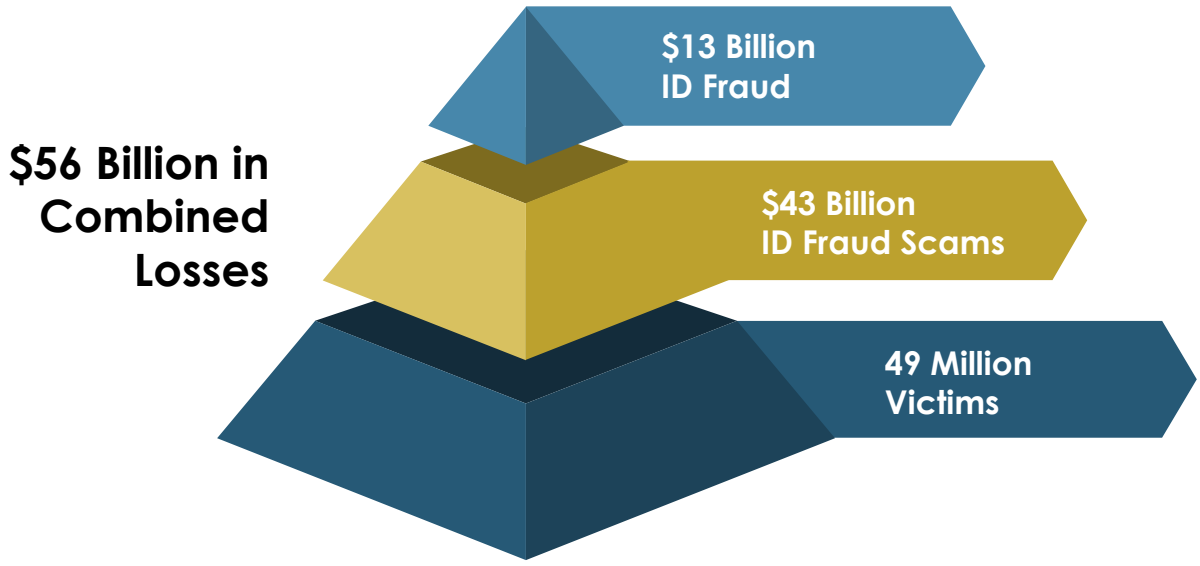
this case, is simply a criminal raconteur who has the ability to strike the right balance between the consumer's sense of risk and reward and thus can manipulate the victim into divulging information or making payments and transfers that directly send funds to criminally controlled accounts.

Identity fraud scams that used money-movement products—ranging from P2P payments like Cash App and Venmo, takeovers of digital wallets like Apple or Google Pay, and wire transfer services like Western Union—tended to ensnare American consumers aged 18-49, but across other generations, consumers aged 65+ experienced more P2P fraud than their peers aged 50-64.

A similar loss pattern involving digital wallets showed that 61% of US adults aged 65+ having more fraud than US adults aged 50-64. The higher fraud rates affecting US adults aged 18-49 more so than their older counterparts could be related to several factors, including digital curiosity, longer screen time, and activity spread across multiple digital platforms. Javelin reported on a similar generational phenomenon in the 2020 Identity Fraud Study, *Genesis of the Identity Fraud Crisis*, which demonstrated that younger generations are often victimized more by identity fraud because they have an optimism bias that makes them feel impervious to fraud risk.

2020 Combined Identity Fraud Losses

Figure 2. The Impact of Identity Fraud



Source: Javelin Strategy & Research, 2021

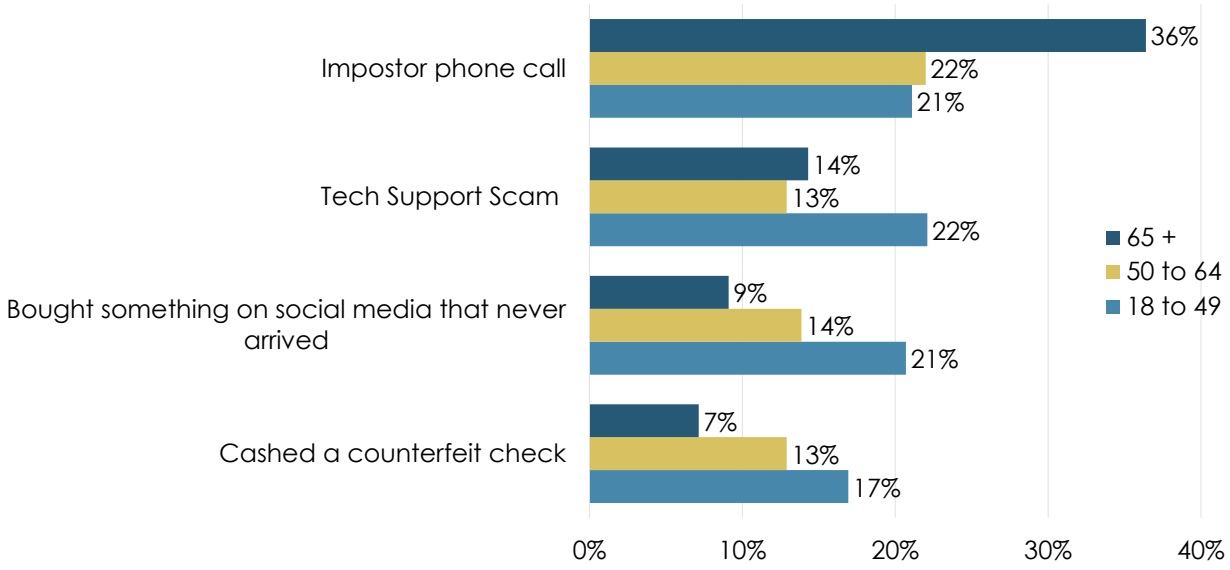
THE CRIMINAL LIFELINE: IMPOSTOR AND TECH SUPPORT SCAMS

The Federal Trade Commission received more than 2.1 million fraud reports from consumers in 2020, with impostor scams remaining the most common type of fraud reported to the agency. Javelin, in a similar fashion, discovered that impostor scams alone took the top spot in how multiple generations were victimized by criminals in 2020. A combined 27% of US adults aged 50+ reported speaking to an impostor during a phone call. Impostor fraud begins simply with a criminal pretending to be someone else.

The goal of impostor calls is to trigger the scam victim into sending funds or purchasing gift cards or taking some other action that directly benefits the impostor with financial gain. Criminal impostors might make individual calls to their victims or pre-record mass "robocall" messages that are randomly sent to thousands of potential victims. Robocalls might announce a special opportunity to obtain a preferred interest rate on a credit card or make claims that the call recipient is somehow negligent in paying bills. A

Criminals Succeed with Impostor Calls Made to US adults 50+

Figure 3. US adults 50+ Are Targeted More Frequently by Impostor Calls



Source: Javelin Strategy & Research, 2021

[1] https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers. Published February 4, 2021; accessed July 6, 2021.

combination of scam triggers, whether negative or positive, best represents why criminals cast emotional arrows during the execution of impostor scams.

Criminals are also targeting consumers aged 50+ via tech support scams that prey on victims' fears that a serious virus is present on computers or mobile devices, thus necessitating an immediate repair. Tech support scams always begin with some form of unsolicited phone call or screen pop-up message that conveys urgency and pushes the consumer to take immediate (and costly) action to repair his or her device. When criminals onboard a consumer device using mobile remote access technology, the losses can be even higher because the criminal is now able to take over the computer or mobile device to harvest login credentials and access financial accounts.

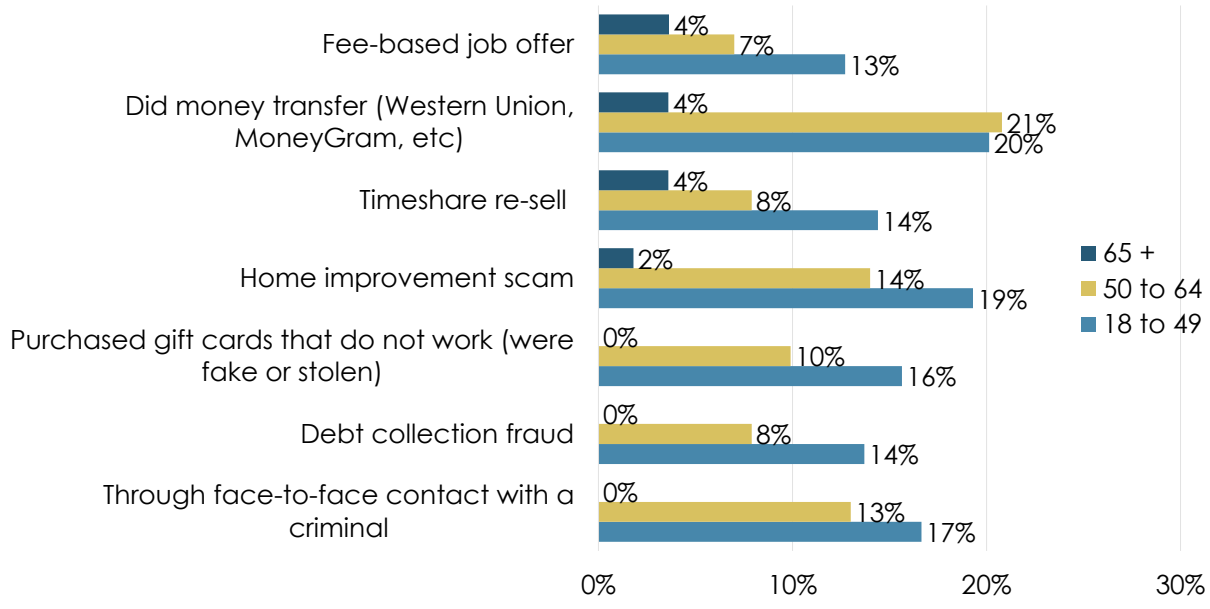
CRIMINAL MISCALCULATION: US ADULTS AGED 65+ MIGHT NOT BE THE IDEAL TARGETS

Consumers often identify with the products and services they use. This normal inclination to make purchasing decisions based on need, status, and price has fueled the success and legend of Madison Avenue advertising companies for years. Criminal scams also seem to have a higher level of success when they address needs specific to a particular victim's lifestyle, interests, and habits. More damage was experienced in every case by US adults aged 18-49 who were victimized by scams that focused on debt collection, gift cards, and face-to-face interactions with criminals. The opposite held true at the upper end of the age scale, as US adults aged 65+ remained impervious to such criminal tactics, with zero percent of study respondents reporting fraud linked to debt collection, gift cards, and face-to-face interactions with criminals.

Fee-based job offer scams in 2020 (see Figure 4) affected 13% of U.S. adults aged

Victims Respond to Scams that Align with Their Lifestyle and Habits

Figure 4. Identity Fraud Scams Are Not One-Size-Fits-All



Source: Javelin Strategy & Research, 2021

18 to 49. Success rates for this identity fraud scam make sense because the victim age group fits well into the normal workforce age in the United States. Other examples that illustrate the correlation between age and scam tactics were more dramatically obvious. Wire transfer scams resulted in similar rates of loss for respondents in the 18-49 and 50-64 age groups (20% and 21%, respectively). Only 4% of US adults aged 65+ responded to scams involving wire transfers, perhaps because they lacked a supporting mobile app or were unwilling to travel to an appropriate outlet to perform the requested transfer. Timeshare re-sell scams were also avoided by the majority of US adults aged 65+, with only 4% reporting scam activity.

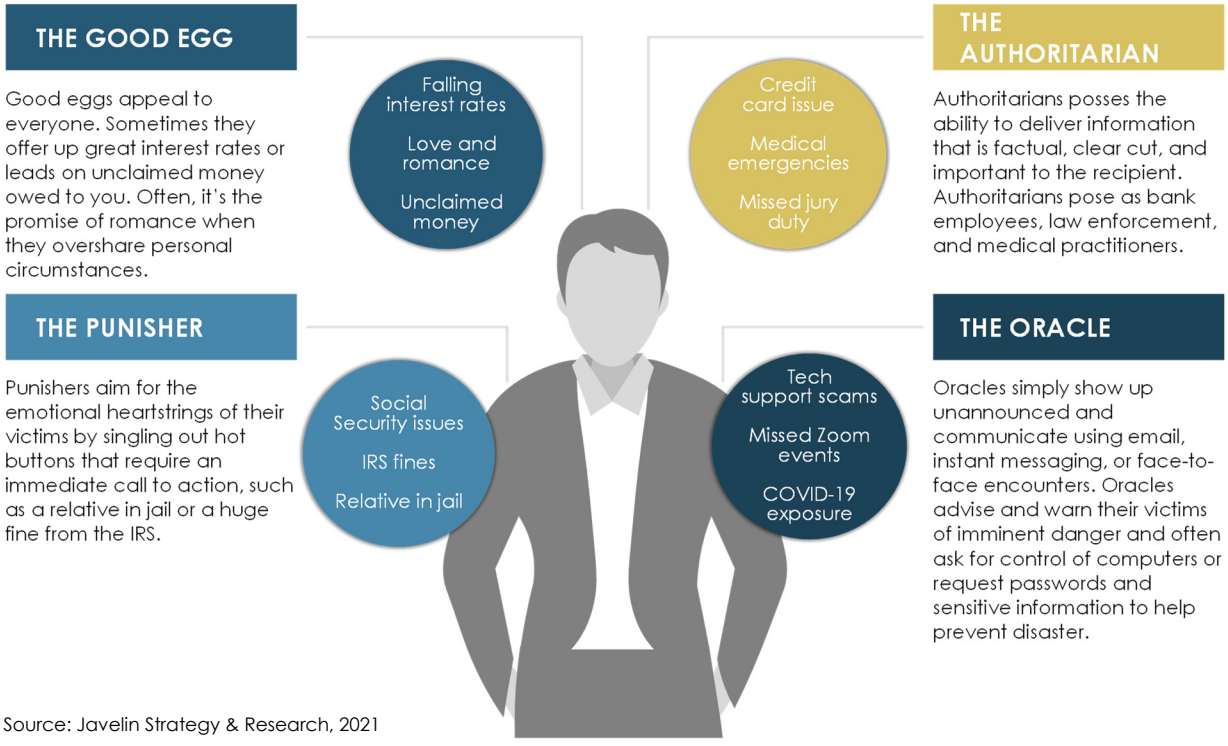
THE SIGNS OF DECEPTION

Criminals will often adopt various personas to help them manipulate their victims. Their goal is to take advantage of consumers 100% of the time without remorse or regard for the victim's wellbeing. Understanding how criminals manipulate outcomes by assuming particular personas during an identity fraud scam casts a powerful lens on scenarios that are repeated over and over across a wide stratum of victims. Threats can be minimized when victims and their trusted advisors are able to quickly spot potential criminal behavior.

The only thing that criminals' value is the opportunity to extract financial gain by manipulating their fellow human beings with false narratives, coercive or insincere personas, and psychological insight that would make Sigmund Freud proud. Criminals who perpetrate identity fraud scams are sometimes labeled social engineers because they manipulate social interactions for personal financial gain. Experienced criminals understand that one size does not fit all in terms of how their potential victims respond to certain personas. The right persona applied alongside the perfect emotional trigger

Common Personas Criminals Use to Manipulate Outcomes

Figure 5. The Criminal Zodiac



Source: Javelin Strategy & Research, 2021

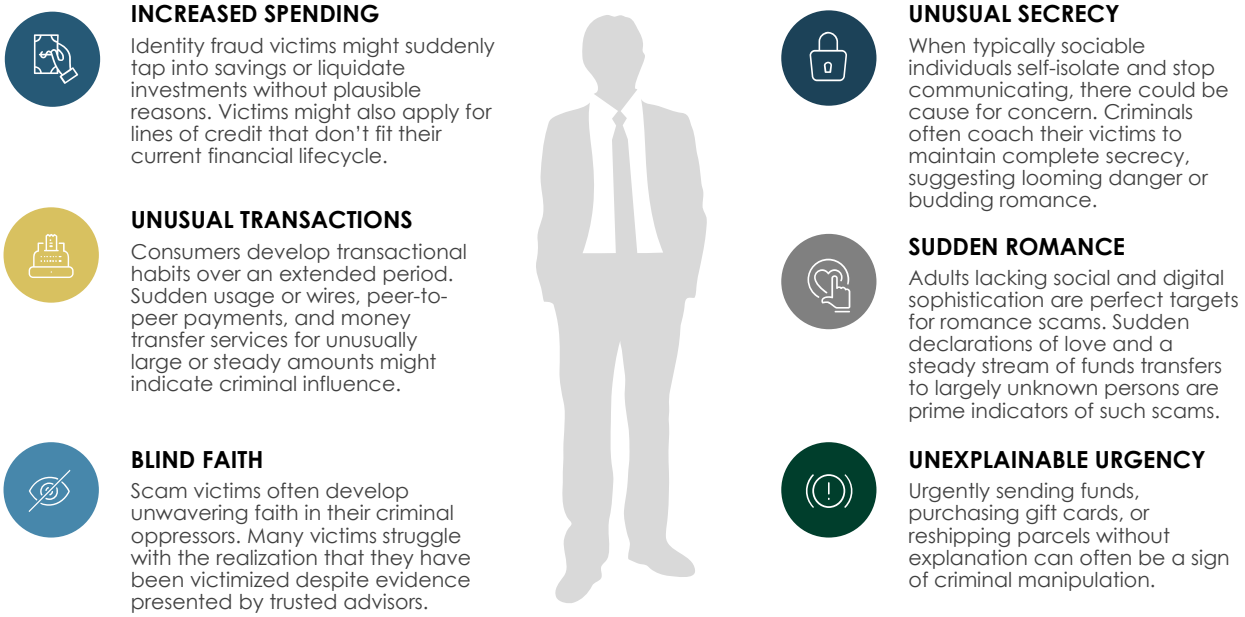
can often deliver the exact outcome a criminal is seeking. A great example involves the *Punisher* persona (see Figure 5), which relies on heightened emotional triggers that require prompt resolution, such as a relative in jail who needs immediate bond for release. The criminal in this scenario always offers up a succinct payment solution, such as money transfers, or the acceptance of gift cards in exchange for a speedy resolution. Victims, in turn, might display unexplained urgency and secrecy that is not even disclosed to their trusted relatives and advisors. These situations create a heightened emotional state that often prevents the victim from accessing the logical thinking required to verify if their relative is actually in jail.

Part of the problem here is the shame and judgment that scam victims experience when they come into contact with words that reference victims as duped, swindled, or rooked. Saying someone "fell for" a scam immediately suggests a lack of intelligence or wisdom and places blame on the victim and not squarely on the criminal, where it belongs.

Being able to identify the traits of deception can be a valuable tool for consumers and financial services providers alike. (see Figure 6) Financial service providers, emotional support professionals, and trusted advisors need to better identify the red flags associated with victims of identity fraud so they can help potential victims realize that they might be

How to Spot Potential Identity Fraud Victims

Figure 6. Common red flag behaviors



Source: Javelin Strategy & Research, 2021

interacting with a criminal or have done so in their recent past.

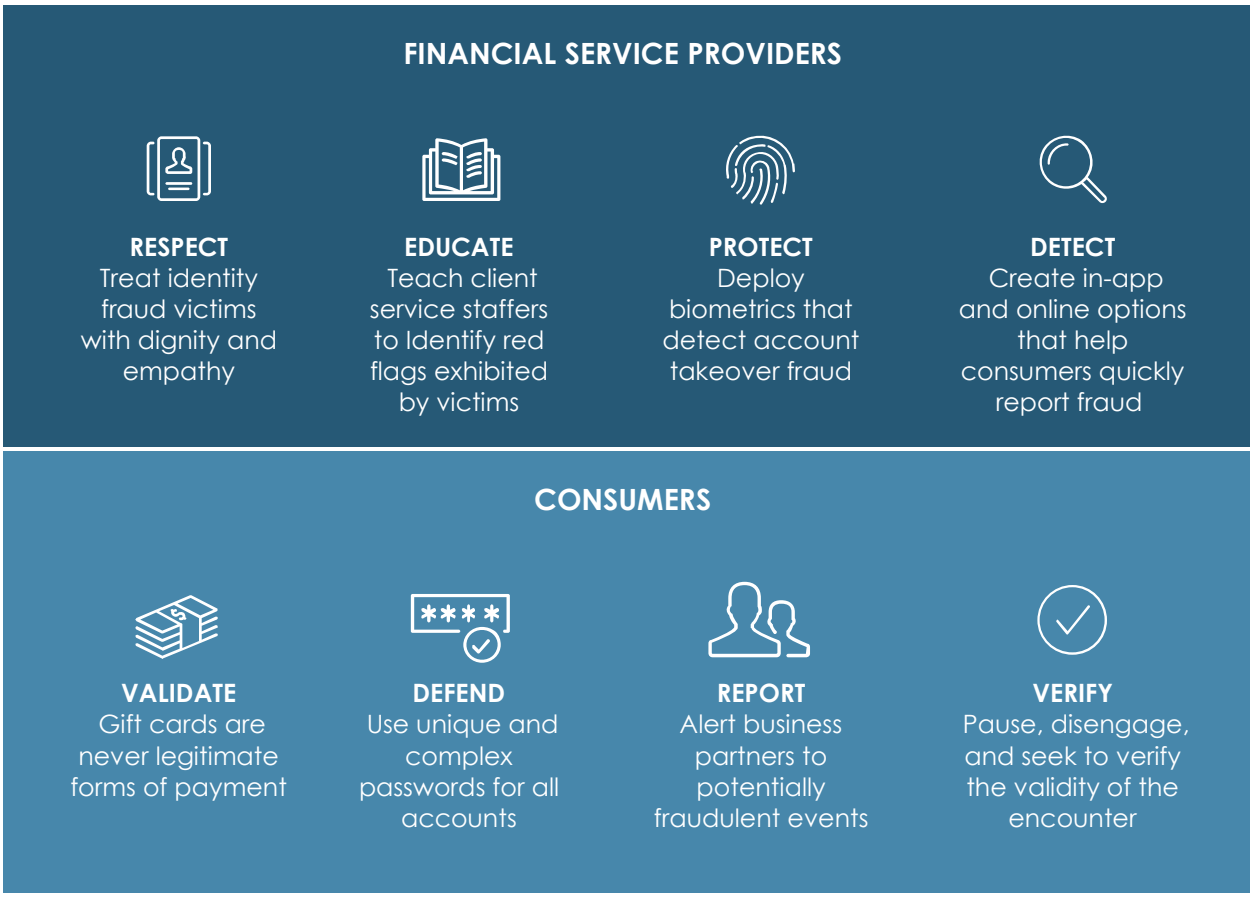
Identity fraud victims may, for example, exhibit unusual secrecy in their personal and business dealings when a criminal is manipulating them. Often the scenarios that criminals use to ensnare their victims involve the resolution to financial problems and, quite often, the promise of romance. Increased spending and unusual financial transactions such as wire transfers are all red flags that require careful evaluation. Thoughtful conversations that encourage a slower and more cautious approach to sending money or reacting to the pressing demands of potential scammers should be conducted in a way that preserves victim dignity while diminishing the blind faith the victims may have invested in their criminal oppressor.

GOLDEN RULES FOR MAINTAINING A SAFE DISTANCE FROM IDENTITY FRAUD

Consumers and financial institutions are often seeking identity fraud information for similar purposes. The consumer usually wishes to increase personal security while resolving complications that arise from identity fraud. Financial institutions, on the other hand, are often seeking information that unlocks how consumers will react to the measures they wish to take to better educate and protect their account holders. These corresponding goals easily align into a series of golden rules that should be embraced by consumers and their trusted advisors.

Recommendations for Consumers and Financial Service Providers

Figure 7. Identity Fraud Golden Rules

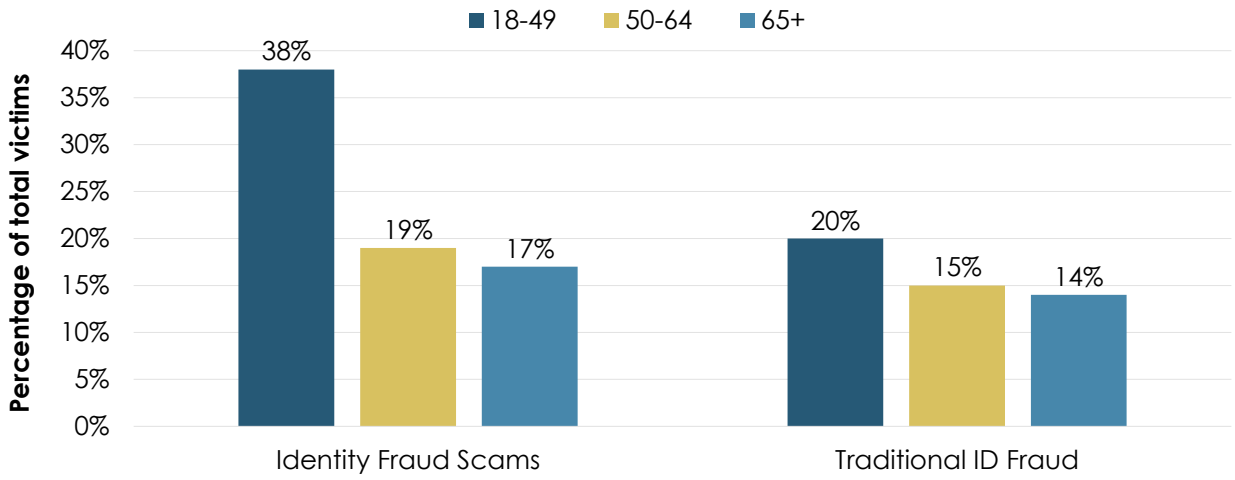


Source: Javelin Strategy & Research, 2021

APPENDIX

U.S. Adults Aged 18-49 are Victimized at a Higher Rate than Older U.S. Adults

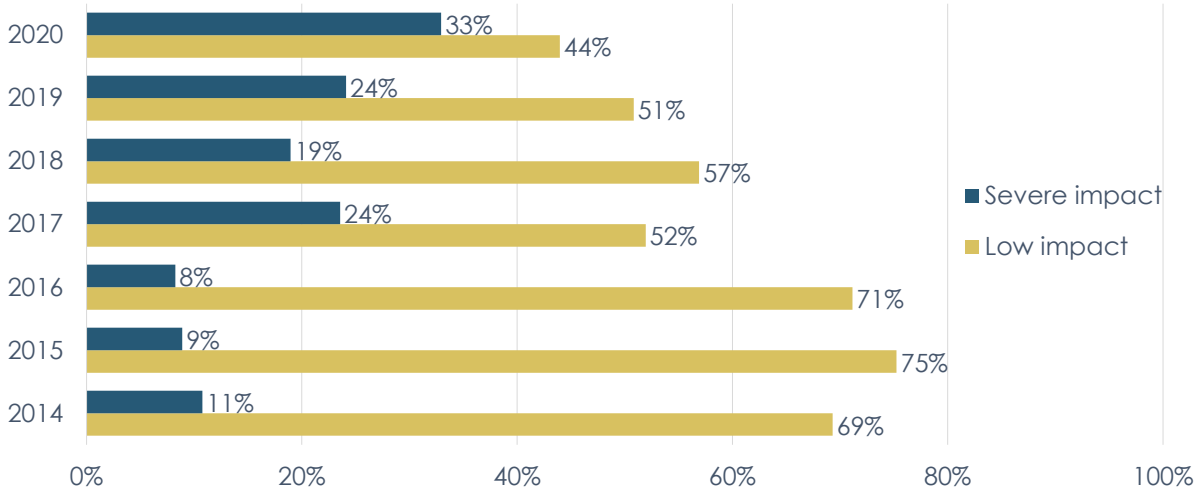
Figure 8. Percentage of Victims Affected by Scams and Identity Fraud



Source: Javelin Strategy & Research, 2021

Identity Fraud Victims Experience Growing Impact to Their Lives

Figure 9. Severe Impact of Identity Fraud Has Increased 200% Since 2014



Source: Javelin Strategy & Research, 2021

JAVELIN

METHODOLOGY

This report, sponsored by AARP, focuses on how U.S. adults aged 50+ are affected by identity fraud and identity fraud scams. This report was adapted from the 2021 Identity Fraud Study, published by Javelin Strategy & Research in March 2021. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

ABOUT AARP

AARP is the nation's largest nonprofit, nonpartisan organization dedicated to empowering people 50 and older to choose how they live as they age. With a nationwide presence and nearly 38 million members, AARP strengthens communities and advocates for what matters most to families: health security, financial stability, and personal fulfillment. AARP also produces the nation's largest-circulation publications: AARP The Magazine and AARP Bulletin. To learn more, visit http://www.aarp.org or follow @AARP and @AARPadvocates on social media.

ABOUT THE AUTHOR

John Buzzard
Lead, Fraud & Security

CONTRIBUTORS:

Jacob Jegher
President

Tracy Kitten
Director, Fraud & Security

Alec Frank
Analyst, Cybersecurity

James Lee
Analyst, Digital Banking

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