# TABLE OF CONTENTS

Overview ............................................................................................................................................................................. 3  
The Facts Surrounding Identity Fraud........................................................................................................................................... 4  
Consumer Action Plan.................................................................................................................................................................. 5  
Act 1: Why Is Consumer Information So Valuable? ........................................................................................................... 6  
Act 2: Making Room for Improvement ........................................................................................................................................ 8  
Act 3: The Blueprint to Success .................................................................................................................................................... 10  
Appendix .................................................................................................................................................................................. 13  
Methodology ............................................................................................................................................................................. 15

# TABLE OF FIGURES

Figure 1. How Personal Information is Stolen by Criminals ........................................................................................................ 6  
Figure 2. How Consumers Aged 55+ Regard New Technology ................................................................................................. 7  
Figure 3. % of Victims of Identity Fraud Sorted by Age ................................................................................................................ 8  
Figure 4. Fraud Victims Aged 55+ Reluctant to Change Habits ................................................................................................... 9  
Figure 5. How to Increase Security by Changing Your Digital Behavior ..................................................................................... 10  
Figure 6. How to Properly React to Suspicious Events ............................................................................................................. 13  
Figure 7. Actions Taken After Information Was Compromised ................................................................................................. 14  
Figure 8. I Have a Hard Time Remembering My Passwords ................................................................................................. 14  
Figure 9. Desired Features to Include With Online and Mobile Banking .................................................................................. 15
FOREWORD
This report sponsored by AARP explores the impact of identity fraud on U.S. consumers aged 55+ and how technology may play a role in the ability of consumers to protect themselves from financial harm as a result of identity fraud.

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

OVERVIEW
Javelin’s 2020 Identity Fraud Study Genesis of the Identity Fraud Crisis revealed that identity fraud losses were estimated to be $16.9 billion (U.S.) in 2019. The sizable losses could increase as more consumers adapt to a digitally infused lifestyle. Problems will continue to increase as criminals take full advantage of consumers’ trust around personal security and browsing habits to make higher profits from identity fraud scams.

Consumers are constantly forced to balance the need for convenience with the need for personal identity protection. Criminals are regularly targeting Americans aged 55+ through a combination of sophisticated scams via computer malware and also through more traditional low-tech channels via telephone and U.S. mail. The combination of high-tech and low-tech strategies unfortunately gives the upper hand to the criminal — not the consumer.

As society continues to adapt to the confinement created by the 2020 Covid-19 pandemic, there will continue to be a metamorphosis in shopping and transactional behavior that will eventually be best described as the great digital migration. The desire for contactless, safe, and faster forms of personal and financial transactions will drive commercial innovation in tandem with increased criminal acts that target consumers and monetize their personally identifiable data.
Americans 55 and older are leading digitally infused lives. 81% of people aged 55-64, and 77% of people aged 65+ have smartphones, and two-thirds of 55+ Americans use online banking weekly (surpassing the percentage of 18-44-year-olds who do so).

Consumers aged 55 and over want to bank using stronger security authentication. Roughly 90% of consumers aged 55+ state a desire to use more fingerprint scanning, and roughly 80% of additional consumers in the same age range view facial recognition capabilities as trustworthy forms of technology for financial transactions and private business matters.

Older consumers adopt technology at a slower pace. An abundance of caution may be the reason 62% of consumers aged 55–64 (and 69% of consumers aged 65+) consider themselves slow adopters of new technology. There are many excellent fraud prevention technologies that exist in the marketplace today like voice pattern recognition or VPR. VPR is designed to detect a criminal imposter’s voice when an attempt is made to access important financial accounts like a brokerage or home equity line account.

Age doesn’t necessarily correlate to higher instances of identity fraud losses. 27% of Americans aged 55-64 and 26% of Americans 65+ have been victims of identity fraud. When identity fraud does occur, the financial damage incurred by older groups is far lower than that of the national average.

Identity fraud victims do not necessarily change their behavior after an information loss. Consumers aged 65+ typically do not change how they shop, bank, or pay following a fraudulent event. A surprising 70% of consumers 65 and older exhibit reluctance to change familiar habits. Personal convenience and payment card zero liability protection may be part of the reason consumers are exhibiting such elasticity after a fraudulent event.

Criminals still use low-tech communication options to reach fraud victims. Criminals are still calling their victims directly over the phone in order to execute scams. Covid-19 and missing parcel themes are just a few of the most recent scams that are flourishing as more victims fall prey to criminals’ efforts.

55+ consumers are adopting safer business practices. Americans aged 55+ are taking additional precautions to prevent losses of personal information following the compromise of their information. 29% or more have enabled credit freezes on their credit bureau information, and more than 50% have enrolled in identity protection or credit monitoring services.

Passwords still represent a significant security threat. Multiple usernames and password combinations may be the reason 56% of Americans in the 55-64 age range and 60% of Americans aged 65 and over have trouble remembering passwords. Repeating overly-simplified passwords in combination with a variety of usernames/websites makes it incredibly easy for criminals to take over multiple accounts belonging to the same consumer.
Hang up on strangers, and independently verify everything. Do not engage in conversations with persons you do not know who contact you about sensitive, urgent, or threatening personal business matters. If you receive a troubling phone call, email, or text message from an unfamiliar contact, the best idea is to avoid responding to the incoming communication. Quickly initiating your own contact with a business partner or provider to investigate further is the only way to sidestep contact with a criminal.

Write down important numbers and keep them in a safe place. Criminals are now posting fake customer service numbers online. When you use a search engine to locate an important number, you may not be viewing the legitimate contact information for the company you wish to contact. A safer alternative is to simply make a list of trusted companies you do business with in case you need to quickly reach them.

Secure every device by using stronger security methods. Mobile phones, laptops, and tablets typically contain sensitive personally identifiable information (PII), so access to every digital device should be secured with complex passwords and screen locks that utilize fingerprint or facial recognition. A good rule to follow is to apply additional security to devices that are used for any activity that requires a password to initiate activities ranging from social media to financial transactions.

Utilize anti-malware protection on all digital devices. Malware is a term that is often used today to refer to anything that poses a cybersecurity threat and ultimately results in device failure or loss of personal information. Consumers should, whenever possible, use a high-quality anti-malware protection product to help secure laptops, mobile phones, personal computers, and tablets.

Start using a password manager tool or app. Password managers such as LastPass or Bitwarden store and protect passwords using strong encryption. Password managers can be purchased most commonly through the app store that is provided with most mobile devices or via Internet search.

Secure personal payments with digital wallets. Digital wallets such as Apple Pay and Google Pay are now standard features on most smartphones and enjoy wide acceptance in the U.S. at most retailers including gas stations. Digital wallets are safer stand-ins for actual payment cards because they use unique encryption that prevents actual payment card information from being shared in the open with merchants.

Lock your doors, and don't forget to lock your payment cards, too. Many financial institutions offer card controls that automatically manage how and where payments can be made. Card users can decide if they want to limit dollar amounts, restrict geographical areas, or prevent card usage at certain types of merchants like jewelry stores. Most card controls are offered at no charge to bank or credit union customers.

Adopt security practices that go beyond a single password. One-time access codes for user authentication make it difficult for criminals to take over sensitive email, financial, and mobile phone accounts. Consumers should utilize one-time passcodes whenever possible with the understanding that they should be treated like a PIN and not disclosed to anyone as they are being used to access accounts.
IDENTITY FRAUD IN THREE ACTS:
A CONSUMER GUIDE

Identify fraud garners so much attention and concern not only because of the widespread financial damage it wreaks upon the U.S. economy but also because nearly everyone is susceptible to it. According to Javelin's 2020 Identity Fraud Survey, *Genesis of the Identity Fraud Crisis*, identity fraud-related financial losses amounted to $16.9 billion in 2019, with 1-in-20 American consumers victimized.

Simply put, identity fraud is the use of a person’s identity by another individual, without permission, to defraud that person or to commit a crime. So much information residing in so many digital spaces online has triggered a new marketplace in which information is aggregated and sold by criminals. Dark web merchant websites that are accessible only using a special browser are typically where consumer information is offered for sale. The street value for Social Security numbers, dates of birth, and payment cards are often sold right alongside the username and passwords to popular rideshare apps (like Uber and Lyft), merchants like Amazon and eBay, and entertainment products like Netflix and PlayStation. The ultimate criminal goal? Find a willing buyer.

Being able to understand that personally identifiable information, or PII, has significant value to criminals is really key to the realization that every consumer, regardless of age or income,

**ACT 1:**
WHY IS CONSUMER INFORMATION SO VALUABLE?

Figure 1. How Personal Information is Stolen by Criminals

The following example reflects how information ends up in the hands of criminals

1. **Malware infects an unprotected laptop and sends every keystroke to a criminal.**
2. **Imposters pose as bank security and steal payment card and PIN information during a phishing scam.**
3. **Fake websites lure bargain hunters with great prices that result in stolen information.**

Source: Javelin Strategy & Research 2020
has to become more vigilant in protecting personal information as more and more consumers embrace a vigorous digital lifestyle. 81% of people aged 55-64, and 77% of people aged 65+ have smartphones, and two-thirds of 55+ Americans use online banking weekly. The degree of potential risk involved with such avid use of online banking, smartphones, and all of the amenities and tools that come with them necessitates some extra care and attention toward identity fraud prevention.

The good news here is that more than half of consumers aged 55+ state a desire to use more fingerprint scanning and facial recognition capabilities (also known as biometrics) as trustworthy authenticators for financial transactions and private business matters. The acceptance of stronger forms of authentication is a huge step toward reducing the threat criminals pose to consumers on a daily basis.

The only major drawback to a wider efficiency in reducing more fraud is the fact that 62% of consumers aged 55-64 (and 69% of consumers aged 65+) consider themselves slow adopters of new technology like voice pattern recognition, or VPR. There are many excellent fraud prevention technologies, and many of them are offered upon request by brokerage houses, banks, and card issuers. It is highly recommended that any technology that offers additional security to further stabilize static passwords is worth exploring.

**Figure 2. How Consumers Aged 55+ Regard New Technology**

Slow Technology Adoption May Place Consumers at a Higher Risk for Identity Fraud

Source: Javelin Strategy & Research 2020
Good news: It’s impossible to label someone by age and then predict with accuracy that they will become a victim of identity fraud solely based on their birth year. Age doesn’t necessarily correlate to higher instances of victimization or identity fraud losses. While 27% of Americans aged 55-64 and 26% of Americans 65+ have been victims of identity fraud, nearly the same rate (27%) applies to the overall U.S. population surveyed.

More good news: When identity fraud does occur, the financial damage incurred by consumers aged 55+ is far lower than the national average. 55+ consumers are adopting safer business practices following compromises of their personal information. The value in securing and protecting credit health, finances, and credit ratings has been possible through the adoption of relatively new security measures like:

- Personal monitoring of financial and non-financial accounts using card controls and self-monitoring.
- More than 50% of consumers aged 55+ have increased their use of identity protection and credit monitoring services to help detect and remediate problems that arise from identity fraud.
- 29% of consumers aged 55-64 and 30% of consumers 65+ have initiated credit report security freezes to prevent criminals from using the credit ratings of identity theft victims to open mobile phone, credit, and loan accounts.

**Figure 3. % of Victims of Identity Fraud Sorted by Age**

Have you ever been a victim of identity fraud?

- 27% Consumers Aged 55-64
- 26% Consumers Aged 65+
- 27% All Consumers

Source: Javelin Strategy & Research 2020
Despite indications that some consumers are taking solid measures to protect themselves from identity fraud, there is much room for improvement. Identity fraud victims do not necessarily change their behavior after they have experienced identity fraud. Consumers aged 65+ typically do not change how they shop, bank, or pay following a fraudulent event. A surprising 70% of consumers 65 and older exhibit reluctance to change familiar habits. Personal convenience and payment card zero liability protection may be part of the reason consumers exhibit such flexibility following a fraudulent event. Consumers are better off spending time updating their usernames, passwords, and contact information immediately following a loss associated with identity fraud. Passwords still represent a significant security threat. Multiple username and password combinations may be the reason 56% of Americans in the 55-64 age range and 60% of Americans aged 65 and over have trouble remembering passwords. Repeating overly-simplified passwords in combination with a variety of usernames/ websites makes it incredibly easy for criminals to take over multiple accounts belonging to the same consumer.

Identity fraud is not always perpetrated using sophisticated technology. Low-tech tools are still working very well for criminals as more and more persist in calling their victims over the phone to execute scams. Covid-19 scams and missing parcel scams are just a few of the most recent angles used by criminals to steal information from unwitting consumers. If you receive a troubling phone call, email, or text message from an unfamiliar contact, the best idea is to avoid responding to the incoming communication. Quickly initiating your own contact with a business partner or provider to investigate further is the only way to sidestep contact with a criminal.

Figure 4. Fraud Victims Aged 55+ Reluctant to Change Habits
As a result of being a fraud victim, do you do any of the following?

<table>
<thead>
<tr>
<th>Action</th>
<th>55 to 64 years</th>
<th>65+ years</th>
<th>All Consumers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avoid certain merchants</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switched forms of payment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spend less money online</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switched credit card companies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switched your primary bank or credit union</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spend less money in physical stores</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I do none of these</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Javelin Strategy & Research 2020
As technology continues to evolve, there are much better options that come along with it to improve personal security. Anti-malware programs on devices and stronger passwords are just the tip of the iceberg in terms of developing safer digital habits. It’s almost easier to think of personal security protocol in terms of what level of protection each action provides. Being able to see how a routine digital habit can be further secured with a simple change in behavior is a really great way to immediately reap the benefits of stronger personal security.

**Figure 5. How to Increase Security by Changing Your Digital Behavior**

How risk can be lowered simply by adopting stronger technology and digital behavior

- **Safer Banking**
  - Using an internet browser to conduct online banking
  - Using the mobile banking app provided by your bank or credit union

- **Password Safety**
  - Use random passwords that are complex
  - Utilize a password manager to encrypt and store your passwords

- **Device Security**
  - Utilize a password protected screen lock
  - Enable biometric screen locks using fingerprints or facial scanning

- **Payment Card Security**
  - Always perform a chip-enabled transaction whenever possible
  - Load your payment card into a digital wallet

- **Scam Avoidance**
  - Use caution when speaking or texting with unknown persons
  - Hang up on suspicious callers, delete unusual emails and suspicious texts

- **Safer online behavior**
  - Avoid ecommerce websites that are offering incredible bargains
  - Always deploy anti-malware protection scans on a daily basis

Source: Javelin Strategy & Research 2020
During a time of crisis, there are often moments in which logical solutions to problems become elusive as stress hormones battle it out with the more logical side of the human brain. It is reasonable to assume that having a plan of action at the ready for dealing with identity fraud is the most sensible way to prepare.

**Payment card fraud** is a common component of identity fraud. Credit card skimming is really only part of the story since other forms of your personally identifiable information may have simultaneously been compromised during a much more comprehensive identity theft scheme.

**POTENTIAL ISSUE**
Unusual charges appear on your statement

**HOW TO HANDLE IT**
Immediately contact your card issuer and open a fraud case

**Credit and loan fraud** can encompass a wide variety of consumer and business financing methods. Identity fraud is often linked to loan fraud when criminals, posing as legitimate consumers, apply for credit, business, or personal loans and access to existing home equity lines of credit.

**POTENTIAL ISSUE**
A bill collector contacts you about a debt you didn’t create

**HOW TO HANDLE IT**
Contact the original creditor and review a current example of your credit report

**Account takeover fraud** is one of the most prevalent and dangerous permutations of identity fraud. Criminals utilize a rich array of information about account holders to log into sensitive financial accounts with the intention of taking complete control of the account for financial gain.

**POTENTIAL ISSUE**
Your financial account login and password aren’t working despite several tries

**HOW TO HANDLE IT**
Contact your financial institution. Verify recent account changes
**SIM swap fraud** is literally the theft of your mobile phone number and text messages within the smartphone desktop of your device. When criminals gain unlawful access to the information required to clone a SIM card that is identical to your mobile device, they can access sensitive information that leads to account takeover fraud.

**POTENTIAL ISSUE**
Your mobile device has power, but the service and apps appear to be missing

**HOW TO HANDLE IT**
Contact your mobile provider and the providers of all payment apps stored on the device

---

Mobile devices and email have been plagued with a variety of criminal schemes most commonly referred to as phishing. There are multiple terminologies that all essentially contain one element: Criminals who contact consumers using any means possible in order to steal information, distribute malware, and harvest information that can be used for illicit financial gain.

**POTENTIAL ISSUE**
You receive personalized texts from an unknown person or company

**HOW TO HANDLE IT**
Do not respond directly to any messages or click on links. Contact affected business partners as needed to verify the legitimacy of the recent text messages

---

**Tech-support scams** are potentially dangerous to everyone and easy to detect by simply applying logic to how this scam typically targets a victim. Impostors posing as employees of large technology companies like Microsoft target their victims over the phone in a conversation or through an instant messenger pop-up message. The criminal’s goal is to steal your payment information and infect your device with information-stealing malware that copies every keystroke you make.

**POTENTIAL ISSUE**
You suddenly receive an unsolicited call or pop-up message from someone telling you that your account login is frozen or that your laptop or phone is infected with a computer virus

**HOW TO HANDLE IT**
Terminate contact immediately. If you feel that your device has been compromised, have it evaluated locally by a technician you source on your own
**APPENDIX.**

**Figure 6. How to Properly React to Suspicious Events**

Use this guide as a means of diagnosing the common indicators of identity fraud

<table>
<thead>
<tr>
<th>Potential Issue</th>
<th>Signs to watch out for</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment cards</td>
<td>Unusual charges appear on your statement.</td>
<td>✓ Immediately contact your card issuer and open a fraud case.</td>
</tr>
<tr>
<td>Credit and Loan Fraud</td>
<td>A bill collector contacts you about a debt you didn’t create.</td>
<td>✓ Contact the original creditor&lt;br&gt; ✓ Review your credit report, and report anomalous activity as you identify it.</td>
</tr>
<tr>
<td>Financial Account Takeover</td>
<td>You are suddenly unable to log into your account using your designated credentials and password.</td>
<td>✓ Contact your financial services provider immediately.&lt;br&gt; ✓ Request a new payment card.</td>
</tr>
<tr>
<td>Mobile Phone SIM Swap</td>
<td>Your mobile device appears to have no functionality other than power, and the display may be different.</td>
<td>✓ Contact your mobile phone carrier immediately.&lt;br&gt; ✓ Monitor all financial and ecommerce apps that were associated with your device to prevent unauthorized purchases.&lt;br&gt; ✓ Notify your financial institution.</td>
</tr>
<tr>
<td>Text and Email Phishing</td>
<td>You suddenly begin to receive unsolicited texts and emails from unknown persons and or senders who have a username similar to your friends or family.</td>
<td>✓ Ignore and delete all suspicious text and emails.&lt;br&gt; ✓ Contact your friends and family independently to see if they attempted to reach you.</td>
</tr>
<tr>
<td>Tech Support Scams</td>
<td>You suddenly receive an unsolicited call or pop-up message from someone telling you that your account login is frozen or that your laptop or phone is infected with a computer virus.</td>
<td>✓ Do not take action.&lt;br&gt; ✓ Remember: Technology companies do not make outbound calls randomly to consumers.&lt;br&gt; ✓ If you suspect that your device has malware, have it evaluated locally by a trusted company.</td>
</tr>
</tbody>
</table>

Source: Javelin Strategy & Research 2020
Figure 7. Actions Taken After Information Was Compromised
What actions did you take following a compromise of your personal information?

- I changed my password at the breached company
- I enrolled in identity protection or credit monitoring
- I froze my credit

Consumers Aged 55-64  Consumers Aged 65+  All Consumers

Source: Javelin Strategy & Research 2020

Figure 8. I Have a Hard Time Remembering My Passwords
On a scale where 1 is ‘Strongly disagree’ and 5 is ‘Strongly agree’, please indicate your level of agreement

Consumers Aged 55-64  Consumers 65+

Source: Javelin Strategy & Research 2020
Figure 9. Desired Features to Include With Online and Mobile Banking

Which of these features would you most want your financial institution(s) to include as part of their online or mobile banking?

- Fingerprint scanning
- Facial recognition
- One-time password
- Eye scanning
- Voice recognition

Source: Javelin Strategy & Research 2020

METHODOLOGY

This report, sponsored by AARP, focuses on how Americans aged 55 and over are impacted by identity fraud and how they can manage it. This report was adapted from the 2020 Identity Fraud Study, published by Javelin Strategy & Research in April 2020. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.
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: Jacob Jegher, President
Krista Tedder, Director of Payments
Crystal Mendoza, Production Manager

Publication Date: October 2020

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.