Research Report

CENTER for VICTIM RESEARCH

IDENTITY THEFT AND FRAUD VICTIMIZATION:

What We Know about Identity Theft and Fraud Victims from Research- and Practice-Based Evidence

August 2019

Robert Buchanan Taylor/Shutterstock

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Fraud includes a range of crimes that use deceptive or false acts for the personal, usually financial, gain of the perpetrator. Identity fraud is a subcategory in which individuals' personally identifying information is used without authorization to commit fraud.

Millions of people in the United States fall victim to identity theft, identity fraud, and other types of fraud each year, knowingly or unknowingly.[1]

Victims of fraud can experience more than severe financial consequences; their victimization experiences can include legal complications, damaged relationships, physical health problems, and trauma responses similar to those of victims of violent crime. Further, fraud often overlaps with other victimization experiences—including child exploitation and domestic violence—making the understanding of these crimes important to victims and service providers of all types. Understanding the varied needs of fraud victims is an important step in improving practitioners' responses to them.

Despite the multitude of negative harms that fraud can cause, evidence on how best to serve identity fraud and other fraud victims is limited, as few research studies have examined which responses are most effective in remediating harms and preventing revictimization. However, the field's knowledge of and ability to respond to victims of fraud is growing.

This report by the Center for Victim Research summarizes existing evidence from research and practice to identify what we know and where the field needs to grow to improve our nation's response to identity fraud and other fraud victimization.

Fast Facts

- **Millions of Americans fall victim to identity fraud and other fraud each year.** According to the 2016 National Crime Victimization Survey, 25.9 million people in the U.S. aged 16 and older reported *identity fraud* (or attempted identity fraud) in the previous year (Harrell 2019).
- **The most common types of identity fraud are credit card fraud, employment/tax fraud, and utilities fraud** (FTC 2017a). The same year, the most common non-identity frauds were imposter scams; telephone frauds; and prize, sweepstakes, and lottery scams.
- **While identity fraud and other fraud can impact people of all backgrounds and circumstances, certain traits are associated with vulnerability to subtypes of fraud.** Income, age, language, and ability status are some of the characteristics that can make certain groups more vulnerable to certain types of fraud.
- **Many victims lose money to fraud**; while some victims experience minimal losses that are resolved quickly, others experience extensive losses that may never be recovered.
- **The harms of identity fraud and other fraud extend beyond direct financial losses. Victims of identity fraud can have indirect financial losses** from lowered credit, legal fees, and lost employment opportunities. Non-financial harms, such as emotional and physical health problems, can affect all fraud victims. Yet, the evidence on the extent and distribution of fraud consequences is limited.
- **Educational programs are the interventions most supported by research evidence in preventing identity fraud and other fraud victimization**. Other services to fraud victims include reporting and assistance hotlines, support groups, and legal services. Common responses to identity fraud victims include credit and identity monitoring, insurance, and identity restoration.
- **The field needs more specialized services to address identity fraud and other fraud victims' needs**—including help navigating indirect financial harms and non-financial harms of victimization. More program evaluations are also needed to determine which responses to fraud victims are most effective.

1 Although the terms *identity theft* and *identity fraud* are often used interchangeably, not all theft of personally identifying information results in fraud, at least not immediately. This report focuses on identity theft coinciding with fraud (identity fraud), as well as other types of fraud victimizations.

ABOUT THE CENTER FOR VICTIM RESEARCH

The Center for Victim Research (CVR) is a Vision 21 resource center funded by the Office for Victims of Crime (OVC) with the vision of routine collaboration between victim service providers and researchers to improve practice through the effective use of research and data. CVR's mission is to serve as a one-stop resource for service providers and researchers to connect and share knowledge to increase: 1) access to victim research and data, and 2) the utility of research and data collection to crime victim services nationwide. CVR is a collaborative partnership of researchers and practitioners from three organizations: the Justice Research and Statistics Association, the National Center for Victims of Crime, and the Urban Institute.

CVR's Evidence Syntheses

The purpose of CVR's syntheses of knowledge is to assess the state of the field in crime victimization and victim response to help researchers, service providers, and policymakers understand and prioritize what the field needs to improve victim services nationwide. To develop its syntheses, CVR staff focus on addressing a core set of questions, as follows:

1. Prevalence and detection of victims—*How big is each crime victimization problem and how can we identify all crime victims who need help?*
2. Risk and protective factors—*What puts people at risk of each crime victimization and what, if anything, can protect against victimization experiences?*
3. Harms and consequences—*What harms and negative consequences of the crime experience do victims have to navigate?*
4. Preventions, interventions, and victim services—*How can we help victims recover and mitigate the negative consequences of crime experiences? Are there ways to help individuals become resilient to victimization in the first place?*
5. Policy, practice, and research implications—*With what we learn through these syntheses about reaching and serving crime survivors, how can victim researchers, policymakers, and service providers move the field forward to improve the response to crime victimization?*

CVR developed its evidence synthesis framework following the Centers for Disease Control and Prevention's (CDC) evidence project, which recognizes the importance of integrating knowledge from the best available research and experiential knowledge from practice (referred hereinafter as "practice evidence"), along with contextual evidence regarding what we know for each victimization topic. The primary focus of CVR's evidence syntheses has been reviewing materials available in the United States from the years 2000 to present, including journal articles, reports, fact sheets, briefs, and videos found in research databases and on topic-relevant organizations' websites.

Each synthesis summarizes knowledge on the: 1) prevalence and detection of victims, 2) risk and protective factors, 3) harms and consequences, 4) preventions, interventions, and services, and 5) policy, practice, and research implications. More details on the methods CVR followed in building an evidence base for fraud and identity theft victimization and other victimization areas and research products on these victimization topics are provided on CVR's website.

For this synthesis on fraud, CVR researchers initially identified 1,845 potential source documents through database searches and websites of leading victimization organizations. Ultimately, 152 research sources and 278 practice sources met CVR's inclusion criteria and were reviewed for this synthesis (see References for details).

DEFINING IDENTITY THEFT AND FRAUD VICTIMIZATION

This CVR synthesis discusses victimization from a range of identity-related and non-identity related frauds (see Appendix for examples of fraud subtypes). Much of the fraud research to date focuses on fraud against governments and organizations. This emphasis and the lack of a clear definition has allowed fraud against individuals to remain relatively understudied (Beals, DeLiema, & Deevy 2015). In this evidence review, **fraud refers to crimes in which deceptive or false acts are committed for personal, typically financial, gain through misrepresentation** of self and/or promises of goods, services, or financial benefits that do not exist, were never intended to be provided, or were misrepresented (OVC 2019a; OVC 2019b). The review focuses on U.S.-based victims of fraud crimes that could be domestic or transnational in nature.

Identity fraud is a subcategory in which personally identifying information or credentials of others (such as social security number, birthdate, credit card, or online account passwords) are used without authorization (typically for financial gain; Pascual, Marchini, & Miller 2018). Identity fraud can be financial—such as new account fraud (when a perpetrator uses personally identifying information to open new credit, utility, or other accounts in a victim's name)—but it is not always. For instance, medical identity theft involves a perpetrator using a victim's information to receive medical services and criminal identity theft involves a perpetrator using a victim's name during criminal justice processes.

As footnoted previously, identity theft and identity fraud are two terms researchers and practitioners often use interchangeably, yet there are increasing efforts in the field to differentiate the two. According to U.S. federal legislation, identity theft is the knowing transfer or use, without lawful authority, of another person's identity with the intent to commit, aid, or abet unlawful activity (FTC 1998). However, identity theft can occur without an element of fraud (such as in data breaches or mail theft); an incident becomes identity fraud once stolen personal information is used for financial gain (Pascual, Marchini, & Miller 2018). **Accordingly, CVR refers to instances of identity-related fraudulent activity as identity fraud**. However, we refer to specific types of identity fraud with their most commonly used name. For example, child identity theft, medical identity theft, and criminal identity theft are all types of identity fraud.

Other types of identity fraud include unauthorized use or attempted use of an account or of personal information to open an account and the misuse of personal information for a fraudulent purpose (BJS 2018).

CVR treats identity theft that lacks an element of fraud as outside the scope of this review. Acts of identity theft—such as skimming, hacking, data breaches, and mail theft—are often precursors to identity fraud, but are not fraud themselves. Additionally, this synthesis also excludes fraudulent acts targeting organizations and governments; harms of victimization affecting businesses and institutions; evidence focused on victims in countries other than the U.S.; and evidence on fraudulent activity and financial exploitation of older adults by trusted individuals and caregivers (instead, see CVR's forthcoming synthesis on Elder Abuse).

EXAMPLES OF IDENTITY THEFT AND FRAUD

Photo by by Mendenhall Olga/Shutterstock

PREVALENCE AND DETECTION OF VICTIMS

Key Takeaways

- According to the 2016 National Crime Victimization Survey (NCVS), an estimated **25.9 million people in the U.S. aged 16 years and older were victims of misuse or attempted misuse of accounts and personal information for fraudulent purposes—also known as identity fraud**—in the prior year. This was a 3% increase from the 2014 estimates (Harrell 2019).
- An estimated **25.6 million U.S. adults were victims of one or more non-identity frauds** included in Federal Trade Commission's (FTC) 2011 Fraud Survey during the prior year (Anderson 2013). This was a 3% decrease from estimates of the 2005 survey (Anderson 2007).
- Precise fraud prevalence estimates are challenging to generate due to underreporting, the hidden nature of identity fraud, and definitional issues.

Fraud Recording and Reporting Mechanisms

Consumer complaint data, reports to financial institutions, reports to the state and local criminal justice agencies, and surveys are the primary ways that victims of fraud become known to authorities in the U.S. The FTC, Internet Crime Complaint Center (IC3), the National Consumers League's "Fraud.org," and the Identity Theft Resource Center (ITRC) collect reports from consumers nationally about identity theft, fraud, and other consumer protection topics. Victims can also report their experiences to banks, credit issuing agencies, and other financial institutions. Victim reports to state and local criminal justice agencies are less common than reports to national organizations and financial institutions (Newman & McNally 2005). As of 2016, identity fraud data has been collected through the National Incident-based Reporting System (NIBRS), an information system used by law enforcement agencies at all levels across the country. While only 43% of the nation's law enforcement agencies participate in NIBRS (FBI 2019), it can be a helpful source for establishing a baseline prevalence of identity fraud and other fraud (Stamatel & Mastrocinque 2011). In addition, the Bureau of Justice Statistics (BJS), FTC, private for-profit and non-profit organizations, and academics also collect individual- and household-level information on identity fraud and other fraud victimization with national, regional, and local surveys.

Photo by Daisy Daisy/Shutterstock

National Estimates of Victimization and Consumer Complaints

BJS's National Crime Victimization Survey Identity Theft Supplement (NCVC-ITS), FTC's Fraud Surveys, and the private company Javelin Strategy & Research's Identity Theft Reports are the only sources that provide nationally representative annual prevalence estimates for identity fraud and other fraud at the individual level. Other non-random national samples and various national organizations' consumer complaint reports provide further insight into the most common identity frauds and other frauds experienced by victims.

What Do We Know About Individual-Level Prevalence from National Surveys?

Identity Frauds

FTC and the firm Synovate, as a joint effort, conducted the first nationally representative survey on U.S. adults' identity fraud victimization in 2002, followed by a second survey in 2006. These surveys looked at U.S. adults' victimization of identity fraud types defined in federal law: existing credit card fraud, existing non-credit card account fraud, and new accounts and other frauds, including: misuse of the victim's information to misrepresent a person's identity when someone is charged with a crime (criminal identity theft), when renting a house, when obtaining medical care (medical identity theft), for employment, and other situations. The results from these two nationally representative surveys showed that from 2002 to 2006,

U.S. adults' victimization prevalence in these identity fraud categories decreased from 4.6% to 3.7%; however, the decrease was not statistically significant. In both years, misuse of existing accounts was the most frequent victimization category (Synovate 2003; 2007).

12.7%
of survey respondents reported that they were victims of
identity fraud
in the past
five years

According to the 2002 survey, 12.7% of survey respondents reported that they were victims of identity fraud in the past five years (Synovate 2003). The difference between yearly and 5-year estimates demonstrates the importance of collecting data on longer-term victimization experiences for a better understanding of fraud victimization prevalence in the general population. This kind of data collection effort can also allow researchers to control for previous victimization experiences while analyzing future victimization risk.

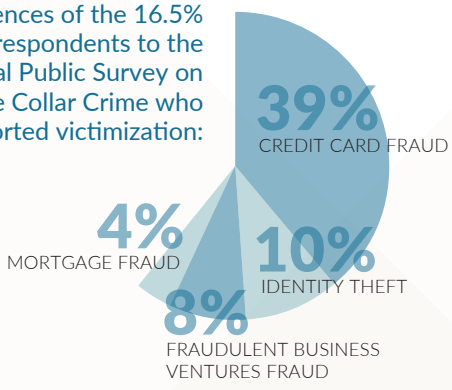
In 2008, BJS collected identity fraud victimization information at the person level from an identity theft supplement to the NCVS. The 2008 iteration of the NCVS-ITS is significantly different than the subsequent iterations in 2012, 2014, and 2016 and is not comparable to the results of subsequent surveys. According to the 2008 ITS, approximately 5% of the U.S. population 16 years and older was victimized by identity fraud in the two years preceding the survey (Langton & Planty 2010). Among these victims, the most frequently experienced victimization type was the fraudulent use of identity information for the unauthorized use of an existing credit card account (53% of all victims).

According to the 2012 and 2014 NCVS-ITS surveys, about 7% of persons aged 16 or older were victims of identity fraud in the year preceding the survey. In 2016, approximately 10% of all U.S. residents age 16 or older were victims of one or more of the three identity fraud categories included in the survey (Harrell 2019). In all iterations of this survey, the most commonly reported identity fraud victimization category was "unauthorized use of an existing account" (Harrell 2019). One limitation of this data collection effort is that NCVS excludes crimes against children 15 or younger; persons living in military bases and in institutions (such as correctional facilities, hospitals, and nursing homes), highly mobile populations, and people experiencing homelessness.

Three other national surveys capture identity fraud at the individual level. In 2010, the National White Collar Crime Center commissioned the nationally representative National Public Survey on White Collar Crime. In this survey, the experiences measured included mortgage fraud; credit card fraud; identity theft; unnecessary home or auto repairs; price misrepresentation; and financial losses occurring due to false stockbroker information, fraudulent business ventures, and internet scams. The survey found that 16.5% of respondents had been a victim of one or more of these white-collar crimes in the past year. Among these victims, credit card fraud constituted 39% of their victimization experiences, identity theft 10%, fraudulent business ventures fraud 8%, and mortgage fraud 4% (Huff & Kane 2010).

AARP's one-time national and multi-state survey of over 11,000 U.S. adults explored the prevalence of and risk factors for internet fraud victimization. Data showed that 65% of all individuals 18 years and older who used the internet received one or more online scam offers in 2013 (Shadel, Pak, & Sauer 2014). Lastly, the Ponemon Institute measured the prevalence of medical identity theft in the U.S. and its impact on consumers with an annual Survey on Medical Identity Theft. In 2013, they surveyed 788 adults regarding their experiences (or close family members) as victims of medical identity theft. The researchers found that an estimated 1.84 million U.S. adults or family members (less than one percent) became victims of medical identity theft at some point in time; this number was 313,000 cases higher than that reported in Ponemon Institute's 2012 survey (Ponemon Institute 2013).

Experiences of the 16.5% of respondents to the National Public Survey on White Collar Crime who reported victimization:



Non-identity Related Frauds

FTC also commissioned three nationally representative surveys in 2003, 2005, and 2011 to capture non-identity related fraud victimization rates among U.S. adults. In these surveys, respondents were asked if they had been victims of the most common fraud crime categories in the complaint reports filed with FTC's Consumer Sentinel Network (Sentinel Network). According to the 2003 FTC Fraud Survey, 11.2% of adults were victims of the 10 fraud categories included in the survey in the preceding year, collectively experiencing 35 million fraud incidents (Anderson 2004). Victimization prevalence increased to 13.5% for the 14 fraud categories included in the 2005 survey (Anderson 2007) for a total of 48.7 million victimization incidents, but fell to 10.8% for the 17 fraud categories included in the 2011 survey for a total of 37.8 million fraud incidents (Anderson 2013).

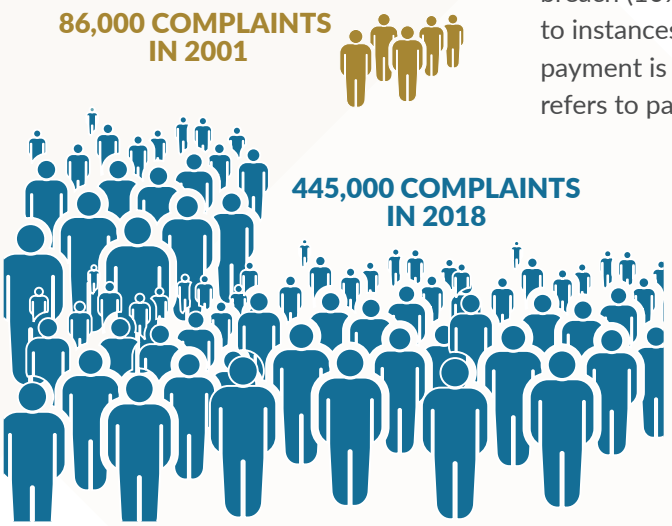
These prevalence figures should, however, be interpreted carefully considering the categories of frauds included in these surveys varied each year. Comparing the percentage of consumers who were victims of 12 categories of fraud included in both the 2005 and 2011 surveys, the prevalence of these frauds in 2011 (9.2%) was slightly lower than in 2005 (10.7%). The top three frauds were advance fee loan scams, buyers' club memberships, credit card insurance frauds, and credit repair frauds in 2003 (Anderson 2004); fraudulent weight loss products, foreign lottery scams, and buyers' club memberships in 2005 (Anderson 2007); and fraudulent weight-loss products, fraudulent prize promotions, and fraudulent buyers' club memberships in 2011 (see Appendix for full descriptions of these fraud types).

What Do We Know About Fraud Incidents from Consumer Complaint Data?

In addition to the national surveys, prevalence estimates come from various fraud reporting mechanisms. It is important to highlight that these estimates only capture victims who knew how to and chose to report, and, as described later, there are many barriers to victims reporting fraud victimization.

FTC's Consumer Sentinel Network received nearly 3 million consumer complaints in 2018, of which 48% were non-identity frauds and 15% were identity-related frauds. Compared to 2001, these numbers represent a five-fold increase in identity fraud complaints (from 86,000 complaints in 2001 to 445,000 complaints in 2018) and a ten-fold increase in non-identity related fraud complaints (from 137,000 complaints in 2001 to 1.4 million complaints in 2018). Imposter scams were the top reported category to the Sentinel Network in 2018. These scams include people falsely claiming to be with the government, a relative in distress, a well-known business, or a technical support expert to get a victim's money. There were nearly 535,000 imposter scam reports to the Sentinel Network in 2018 (FTC 2019a). Credit card fraud was the top identity fraud category for the complaints to FTC in 2018. Out of nearly 167,000 identity fraud reports filed, the majority of complaints were for misuse of an existing account or opening of a new credit card.

IC3 received approximately 300,000 internet crime complaints in 2017, 40,000 more than the number of complaints in 2013. The top complaints were for non-payment/non-delivery (28%) and personal data breach (10%) (IC3 2018). Non-payment refers to instances in which goods are shipped but payment is not sent, whereas non-delivery refers to payment without the delivery of goods or services. According to Fraud.org, in 2017, the top three scams were internet general merchandising (29%), fake check scams (18%), and prizes/sweepstakes scams (18%) (National Consumers League 2018).



Sub-National Estimates of Victimization

In addition to the national studies, we also reviewed state-level and community-level studies that aimed to capture the extent of identity fraud and other fraud. These studies include: state level studies such as surveys by AARP (Burton 2008; Dinger & Sauer 2006; Sauer 2006c; Sauer & Pak 2007; Silberman 2004), a study by Holtfreter and colleagues (2005) that used telephone survey data from a random sample of adult Floridians, another study by Holtfreter and colleagues (2014) which focused on victimization in Arizona and Florida, and other smaller scale local surveys.

According to a random sample of AARP Colorado members 50 years and older, approximately one-third of survey respondents reported being a victim or knowing someone who has been a victim of identity theft or fraud in the last five years. Nearly 65% of these respondents reported that the fraud incident involved stolen credit card information. Approximately one in five members said they would contact the police, State Attorney General Office, or the Better Business Bureau for a fraud complaint or destructive email or Internet problems, but 36% indicated that they were not sure who to contact for help (Burton 2008).

Other AARP surveys of registered voters in Montana and Minnesota residents showed that about a quarter of the survey respondents or someone they know had been the victim of identity theft or fraud within the last five years (Dinger & Sauer 2006; Silberman 2004). Additionally, 9% of respondents to an AARP survey of Washington State residents 18 years and older reported they had been victims of identity fraud in the past five years. Among these victims, 45% contacted police, 29% contacted their bank, and 19% contacted a credit card company for help (Sauer 2005).

A survey of Florida residents found that nearly 16% of adult Floridians were targets of consumer fraud in 2004, and that fraud attempts were successful about a quarter of the time (Holtfreter, Reisig, & Blomberg 2005). Another survey of Florida and Arizona residents 60 years and older found that nearly 6 of every 10 participants had been targeted by a fraud attempt in the year prior to the study (Holtfreter et al. 2015).

Challenges with Identifying Victims and Estimating Scope

Despite the increasing number of surveys and avenues to report these crimes, **researchers and practitioners emphasize that identity fraud and other fraud victimizations are still under-reported** (Newman & McNally 2005; NCVC & FINRA 2013; IACP & Bank of America 2008a; FTC 2017d). Many types of identity fraud go months or years undiscovered (Dixon & Barrett 2013; OVC 2010; Synovate 2007). Victims might not know they are victims or may think they have not been victimized if they did not lose money in the immediate term (Synovate 2003). In some cases—such as imposter or romance scams—a victim may know they have sent money but not realize they were victimized by a scam (Deem & Lande 2018). Detection of child identity theft (identity fraud committed against children) can be especially difficult because usually legal guardians do not check children's credit reports. As such, it often goes undetected for a long time (FTC 2011f).

BJS's 2016 NCVS Identity Theft Supplement confirmed that the way victims discovered identity fraud varied by the type of fraud (Harrell 2019). According to the FTC's 2007 Identity Theft Survey, 52% of all identity fraud victims in the prior year discovered they were victims by monitoring their accounts, whereas 26% were alerted by their financial institutions, and 8% learned about the identity fraud when they applied for credit and were turned down (Synovate 2007). In cases of misuse of existing accounts (existing account fraud), 51% of the victims discovered their victimization after being contacted by their financial institution about suspicious activity on their account. The most common way victims of other types of identity fraud discovered their victimization was by being contacted by a company or agency that was not a financial institution (21%), followed by being contacted by their financial institution about suspicious activity (15%).

Our review of practice evidence further suggests that medical identity fraud could be discovered if: (1) a victim receives a bill for services or debt collection for an unknown bill; (2) an insurance company says a victim has reached an insurance limit; or (3) a victim is denied insurance because of a medical issue they do not have (FTC 2010b; State of California DOJ 2018; Ponemon

2013). Criminal identity theft could be discovered through an arrest, failed background check, or increased auto insurance bill (Pierce 2009).

However, **there are various reasons why victims may not report even if they are aware of their victimization**. Some victims may be embarrassed to accept they have been victims of fraud. Some may not recall the details of the crime, especially if they have memory impairments or have been victimized by a complex fraud (Deem & Lande 2018). Others might doubt a real response from law enforcement, especially if they had past experiences of reporting that resulted in no action (Thorleifson et al. 2009). Further, reporting itself can be a challenging experience, as agencies—such as the police or adult protective services—may not want to receive the report if the victim cannot provide many details. Additionally, practitioners report that some reporting mechanisms are only open during business hours or require victims to spend extensive periods of time on hold (Thorleifson et al. 2009).

Some victims—particularly those who know the perpetrator-- worry about getting the perpetrator into trouble (FTC 2017d; Johnson 2003). In cases of family identity theft (identity fraud perpetrated by a family member), victims might worry about a family member being punished for the crime and they might refrain from reporting, especially if they are a dependent on the perpetrator (NCVC & FINRA, 2013; FTC 2011f). Often, when a family member is involved, victims only report when the legal and financial consequences to themselves are very serious (FTC 2017d).

RISK AND PROTECTIVE FACTORS

Key Takeaways

- While identity fraud and other fraud victimization can impact people of all backgrounds and circumstances, certain traits are associated with vulnerability to subtypes of these crimes.
- Research on risk factors is a primary area of study in the fraud victimization field and focuses on demographic factors of victims, behavioral factors including victims' risk-taking behavior and self-control, and people with specific life circumstances' vulnerability to fraud victimization.
- Risk factors for victimization are different for each type of fraud. Both research and practice evidence demonstrate that different groups have different vulnerabilities, and identity fraud and other fraud are not problems isolated to any population.
- Practice evidence in particular suggests that victims of fraud are likely to be revictimized again.

Age

Practice evidence suggests that **children are likely targets for identity fraud** because of their clean credit histories and the lower likelihood of detection (Idaho Coalition Against Identity Theft 2010b; FTC 2011f). Parents may use their kids' information to get credit without knowing the consequences (Toporoff et al. 2013; OVC 2010), sometimes to meet their family's basic needs (FTC 2011d; FTC 2011f) or out of necessity for access to employment or services, as in the case of some undocumented immigrants (FTC 2011f). Finally, kids in the child welfare system are at particular risk (Toporoff et al. 2013). Personally identifying information of child welfare-involved youth is disseminated among larger numbers of people, including foster parents, caseworkers, case aids, group home providers, and volunteers. This increases the risk of identity fraud for these children (Idaho Coalition Against Identity Theft 2010b; Miller & Robuck 2013), making them the most exposed group among all children (FTC 2011f).

Photo by Pawle/Shutterstock

Among adults, **younger adults are among the most frequent victims of identity fraud** and fraud in general, while older adults are at higher risk of specific other frauds. According to NCVS-ITS, persons ages 25 to 64 had a higher prevalence rate of identity fraud than persons ages 18 to 24 and 65 or older (Harrell 2017; Harrell 2019). A 2005 FTC survey found similar results: persons between ages 65 and 74 years were 32% less likely to report having experienced any of the identity frauds than those between 35 and 44. In the same survey, the likelihood of having experienced any of the frauds was 64% less for those who were 75 and older than for those between 35 and 44 (Synovate 2007).

Furthermore, according to the FTC's 2011 Fraud Survey, people aged 65-74 were less likely to become a victim of fraud in general as well as the special categories of weight-loss product fraud and prize frauds, relative to people who were 35-44 (Anderson 2013). Likewise, although practice evidence suggests that older individuals are more likely to engage in risky investment behaviors (NCVC & FINRA 2013), research evidence suggests that victims of investment fraud are usually male, under 65 years old, have higher than average financial knowledge and income, and are college educated (AARP 2003; NCVC & FINRA 2013).

Evidence from research studies and practice suggests that **older individuals** can be more prone to certain types of fraud, such as sweepstake and lottery scams (AARP 2003; Karp & Kirkman 2016; Holtfreter et al. 2015). According to an AARP national survey of telemarketing fraud, the typical lottery victim is a female over 75 years

old, widowed and living alone, retired, with a household income of less than $30,000 (AARP 2003). Practice evidence further suggests that older adults may be more vulnerable to foreclosure scams (Campbell 2013).

The risks associated with increased age have been termed "**Age-Associated Financial Vulnerability**" by public health researchers Lachs and Han (2015), who suggest that cognitive, medical, psychosocial, and environmental factors can make older adults financially vulnerable. Some of the vulnerabilities may stem from older individuals' worries about independence and financial stability, leading them to take financial risks. Additionally, the higher prevalence of memory or cognitive impairments, like dementia or Alzheimer's, among older individuals can make recognizing and reacting to frauds more challenging. Lastly, isolation and loneliness can contribute to the risk profile of older adults (Karp & Kirkman 2016; CFPB 2014; Johnson 2003; FTC 2013a; Deem & Lande 2018). Isolation can contribute to (as well as result from) what has been termed **"chronic" victimization**, where fraud perpetrators maintain long-standing relationships and frequently steal from the older victim, particularly through an imposter or romance scam (Deem & Lande 2018).

Perpetrators of fraud may also see older individuals as easier targets for several reasons—such as their perception that older targets have money through access to pensions (NCVC & FINRA 2013; DePaul 2010), credit, and real estate (Campbell 2013; Johnson 2003)—and the increased interaction of older adults with the healthcare system resulting in increased medical identity theft risk (FTC 2013a).

As expert practitioners Deem and Lande (2018) describe, "these changes in thinking ability and reasoning make rapid decision-making more difficult. When transnational financial fraud predators rely on creating a sense of urgency to respond, some older victims may be unable to carefully think through what is occurring and recognize the scam."

Race

Among persons with a credit card, non-Hispanic white people have a greater likelihood of experiencing existing credit card misuse than Black and Latinx people and persons of other races (Harrell 2019). On the other hand, Black and Latinx people are approximately twice as likely as non-Hispanic whites to have experienced any surveyed fraud in FTC's 2011 Fraud Survey (Anderson 2013). In addition, practitioners report that Native American people can become targets of fraud due to highly publicized special payout situations like tribal dividend payments from per capita and minor trusts or legal settlements which draw attention (LaCounte et al. 2015).

Income and Education

Research and practice evidence suggest that low-income and high-income individuals might be more susceptible to different types of fraud. While low-income individuals are susceptible to frauds such as debt relief frauds, job scams, prize scams, and weight-loss product scams (Anderson 2013; Rich 2016a; Johnson 2003), high-income individuals might be more likely to become victims of identity fraud, especially in relation to use of existing accounts, and to investment frauds (AARP 2003; Harrell 2017; Harrell 2019). While a higher education reduces the odds of becoming a victim of weight-loss product scams, having a college degree or more is associated with higher odds of experiencing income and investment frauds (AARP 2003; Anderson 2013).

Behavioral Factors

Research evidence further shows that there might be a relationship between behavioral factors and fraud victimization risk. Evidence on the relationship between self-control and fraud victimization is mixed. According to the 2011 FTC Fraud Survey, there is no relationship between levels of self-control and fraud victimization, but people with higher patience have a lower probability of becoming a victim of fraud (Anderson 2013). On the other hand, according to a survey of Arizona and Florida residents (Holtfreter et al. 2015), low self-control is associated with a higher probability of fraud victimization. People who are willing to take risk have a higher risk of victimization to fraud, and, specifically, to income-related fraud such as work-at-home programs, business

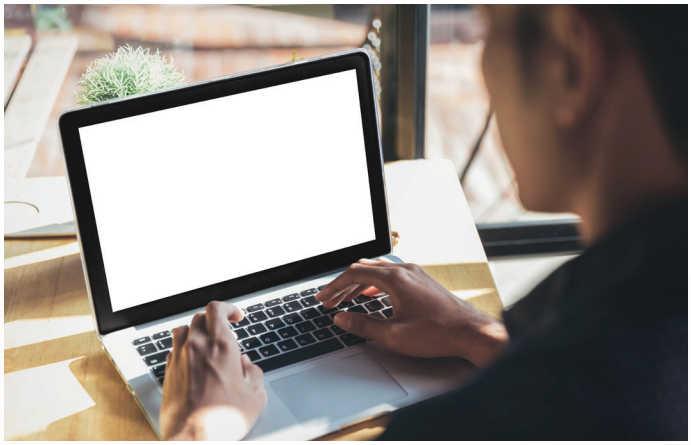


Photo by Suradech Prapairat/Shutterstock

opportunities, pyramid schemes, and government job offers (Anderson 2013).

According to the 2011 FTC Fraud Survey, people who engage in risky purchasing (such as a consumer buying something from a seller about whom the consumer has little information) are more likely to become victims of fraud, specifically weight loss product scams, prize scams, and income fraud (Anderson 2013). According to AARP's 2003 national survey of 11,000 online users, the following behaviors were related to a higher risk of becoming an internet fraud victim:

- clicking on pop-ups;
- opening e-mails from unknown sources;
- selling products on online auction sites;
- signing up for free, limited-time trial offers;
- downloading apps;
- purchasing through an online payment transfer site;
- visiting a website that require one to read a privacy policy or terms of agreement statement; and
- being impulsive (AARP 2003).

Until very recently online safety trainings and education have focused on the "dos and don'ts" of online behavior. The implied relationship between behavioral factors and fraud victimization risk suggests that practitioners should recognize the complex nature of this victimization issue and assist victims in building the skills and habits to reduce victimization risk.

Revictimization

Practitioners widely believe that **people who were former victims of fraud** are likely to be revictimized (FTC 2013b; NCVC & FINRA 2013; Karp & Kirkman 2016).

Victims of identity fraud can be re-victimized because their personally identifying information, passwords, or other sensitive data have been exposed. This information can be reused by the same perpetrator or sold to others and cause the victim to experience identity fraud once again (Pierce 2009; Heckers & O'Brien 2004). According to the NCVS-ITS, many victims experience multiple types of identity fraud. Specifically, about 16% of all victims (1.8 million victims) experienced multiple types of identity fraud during a two-year period (Langton & Planty 2010).

Although their personal information is not necessarily compromised, victims of non-identity frauds can also experience revictimization. Similar to identity frauds, the names of past non-identity fraud victims are sometimes sold on the dark web; these are known as "mooch" or "sucker" lists, and they make victims more likely to be targeted again (Johnson 2003; Deem 2018; NCVC & FINRA 2013). Additionally, sometimes a fraud perpetrator is priming a victim for the next fraud while still scamming them (Karp & Kirkman 2016); for example, some victims of fraud may be directed to fake remediation services that are also scams (Canan & Hume 2016). This revictimization can also occur with victims who have memory impairments, because they may not recognize the crime or remember how to respond; if they continue to be exposed, they may continue to be victimized (Deem 2018). As described above, this can result in what is called "chronic victimization" (see: Age). Notably, victims of non-identity frauds can also become victims of identity frauds through these same channels.

Other Vulnerabilities

Victims of domestic violence may be at risk of identity fraud by their abusers using it as a tactic of coercive control (NCVC & FINRA 2013; Allstate Foundation & NNEDV 2016; Sussman & Shoener 2013; FTC 2017d). **Victims of other crimes**, like sexual assault, burglary, robbery, and elder abuse are at risk of identity fraud if personally identifying information is stolen at the same time (Pierce 2009).

Practitioners suggest that members of marginalized groups sometimes become targets. People may try to exploit **undocumented immigrants'** need to adjust their immigration status (Rich 2016a). **People with cognitive or developmental impairments** may be targeted due to perceptions of them as vulnerable (NCVC & FINRA 2013; Karp & Kirkman 2016). **People experiencing homelessness** might be at heightened risk for identity fraud (Idaho Coalition Against Identity Theft 2010a). **People who have had serious negative experiences** such as death of a loved one, divorce, a serious illness or injury in the family are significantly more likely to experience a variety type of frauds including weight loss product scams, prize scams, unauthorized billing, debt fraud (AARP 2003; Anderson 2013).

Groups that are unable to monitor financial information, like military personnel and incarcerated people, may be prone to identity fraud victimization (George 2018; Treasury Inspector General 2018; CFA 2009). Military consumers filed nearly 114,000 complaint reports to FTC in 2017. Of these, more than 50,000 were fraud reports, including close to 30,000 reports about imposter scams. Identity fraud was the largest single category of reports from military consumers (FTC 2018a). Lastly, **people who indicated that they had more personal debt than they could handle financially in FTC's 2011 Fraud Survey were more likely to become victims of the frauds included in the survey than those with less debt (Anderson 2013).**

Geographic Distribution of Complaints

In 2017, the states with the highest per capita rates of fraud complaints in 2017 were Florida, Georgia, Nevada, Delaware, and Michigan. For identity fraud, the top states in 2017 were Michigan, Florida, California, Maryland, and Nevada (FTC 2018a).

Protective Factors

FTC's 2011 Fraud Survey shows that patience, numerical skills, and a positive outlook on existing debt levels are traits that decrease the likelihood of fraud victimization for individuals (AARP 2003; Anderson 2013). Practitioners further suggest—based on resiliency factors for other crimes—that self-knowledge, insight, hope, and optimism; healthy coping while highly stressed; planning and organizing; getting sleep; strong relationships; and personal meaning and spirituality could make people less susceptible to identity fraud victimization (Texas Identity Theft Coalition 2010d).

Individuals with little oversight of their financial information may not know they are victims

CHILDREN

ELDERLY

MILITARY PERSONNEL

INCARCERATED INDIVIDUALS

HOMELESS INDIVIDUALS

DISASTER VICTIMS

HARMS AND CONSEQUENCES

Key Takeaways:

- Identity fraud and other fraud victimization can cause direct financial losses to victims, as well as indirect economic, mental health, physical health, and social consequences.
- Financial harms are not equally distributed amongst fraud victims. Many victims experience minimal losses that are resolved quickly, while others experience extensive losses that may never be recovered.
- The financial and even non-financial harms of fraud victimization can be exacerbated when the crime goes undiscovered or unaddressed for long periods of time.

Financial Consequences

Victims of all types of fraud can be affected by a range of harms that impact their financial situations in direct and indirect ways. *Direct* financial harms—the victims' monetary losses acquired by the perpetrator of fraud—are the most thoroughly understood. However, victims may also have associated harms to their financial circumstances from remediation costs, legal fees, damaged credit, or barriers to finding employment as a result of their victimization, referred to here as indirect financial harms.

Direct Financial Harms

Direct financial harms can occur through a range of methods. Victims of tax fraud lose their refunds to perpetrators of fraud who filed the return first, victims of existing account fraud (account takeover) have money from their bank accounts used by someone else, and victims of a broad range of frauds are tricked into giving up their money over the phone, through a wire transfer, in the mail, or over the internet under false pretenses. Among reports of fraud in 2017 (excluding identity fraud), wire transfers were the most frequently reported to the FTC as the vehicle for financial losses, with a total of $333 million cumulatively lost from all victims (FTC 2018a).

Collectively, fraud creates large financial losses for victims in the U.S. The 2008 NCVS-ITS estimated $17.3 billion was lost in the previous two-year period to identity fraud (Langton & Planty 2010). Reports to the Federal Trade Commission's Consumer Sentinel Network produced an estimate of $905 million lost to fraud (excluding identity fraud) in 2017 alone (FTC 2018a).

For individual victims, fraud usually results in financial loss but the amount differs by type of fraud. For non-identity frauds, the most recent estimate of median loss was $60; however, the costliest fraud – work-at-home scams – resulted in a median loss of $200 (Anderson 2007). For identity fraud victims, the median value of goods and services lost was $500 as of 2005 (Synovate 2007), but these values differed among different types of identity fraud. For example, for victims of new account fraud the median value lost was $1,350 as of 2005 (Synovate 2007) and $900 in 2016 (Harrell 2019). For existing account fraud, including both credit and non-credit card fraud, the median value was less than $500 in 2005 and, similarly, $200 in 2016 (Synovate 2007; Harrell 2019). Likewise, NCVS reported that the median loss for new account frauds was $1,900, whereas fraud in existing accounts had a median loss of $200.

The percentage of victims who experience losses also differs by victimization type. NCVS also reported that, including both direct and indirect costs (such as legal fees or overdraft charges), 67% of identity fraud victims reported a financial loss in 2016, with a median average loss of $300 (Harrell 2019). The percentage of victims who experienced financial loss due to existing account fraud (68%) was higher than the percentage of victims who had a financial loss due to new account fraud (40%), for example. Furthermore, among victims who experienced multiple identity fraud victimizations, 73% reported a direct financial loss.

Notably, the initial loss of money does not always result in a personal financial loss to the victim. For some types of identity fraud—existing and new account fraud in particular—an individual has limited financial liability. The **Fair Credit Billing Act** (FCBA) limits an individual's liability for credit card fraud and places limits on liability for debit card fraud, which depend on the reporting timeframe. Moreover, many state laws preclude an individual being held responsible for accounts opened in their name without permission (FTC n.d.b).

As a result of these legal liability limitations, the actual personal financial loss from identity fraud and other fraud can be considerably less than the amount stolen by the perpetrator. According to the NCVS, for example, in 2016 only 12% of identity fraud victims experienced direct or indirect out-of-pocket losses greater than a dollar, in contrast with the 67% that had some initial financial loss (Harrell 2017). According to Javelin's 2017 Identity Theft Survey, the victims of account takeover paid an average of $290 out of pocket (Pascual, Marchini, & Miller 2018). In the specific case of identity-theft related tax fraud, once an individual's victimization experience has been confirmed by the victim and the IRS, if the victim is due a refund, the funds are typically released to them (IRS 2019).

However, these direct financial losses are not equally distributed amongst all victims of frauds, due to the varied types of frauds (of which only some have limited liability) and the variances of individual experiences. Additionally, victims of certain types of fraud have higher financial losses. The FTC reported that, while in 2017 the median loss of fraud reports was $429, victims of Travel/Vacation Scams lost a median of $1,710, victims of Mortgage Foreclosure Relief/Debt Management Scams lost $1,200, and victims of Business/Job Opportunity Scams lost $1,063 (FTC 2018a). Moreover, in a small percentages of cases, victims experience much higher losses than the median average. For example, for new account fraud victims, while the median amount lost in 2005 was $1,350, ten percent of cases involved initial losses of $15,000 and the top five percent lost $30,000 in goods or services (not necessarily out-of-pocket losses) (Synovate 2007).

Notably, as will be discussed later, some victims never recover their financial losses, because a perpetrator may dispose of the funds immediately and there are barriers to accessing remediation and victim compensation (NCVC & FINRA n.d.c). For example, receiving the benefits of legal protection often requires extensive and complicated communication with the creditors and financial institutions that can be beyond the capabilities of some victims.

Indirect Financial Harms

The economic impact to an individual victim of fraud can extend beyond the money lost to the perpetrator of the fraud. In the short-term, victims can incur costs of remediation of the harms, including notary costs, legal fees, copying costs, lost wages while dealing with problems, and postage. Other immediate consequences can include the fees associated with bounced checks or overdraft fees from compromised accounts or payment of fraudulent debts (Synovate 2007; Harrell 2017; Harrell 2019). According to the 2005 FTC Identity Theft Survey, fewer than half of identity fraud victims incurred financial losses from this type of indirect financial harm (Synovate 2007). However, a 2013 study of medical identity theft showed that the financial loss associated with medical identity theft can be particularly severe and significantly more than the losses from credit card frauds. According to this study, 65% of the medical identity theft victims paid on average $13,500 to resolve the crime. Their costs included payments to the healthcare provider, payments to the insurer for services obtained by the fraud perpetrator, or costs to engage an identity service provider or legal counsel (Ponemon Institute 2013).

Indirect costs also extend beyond easily quantifiable dollar amounts, and these harms are not typically captured in the national survey research. First, identity fraud in particular can result in a damaged credit score. This can hinder a victim's ability to secure housing, loans or credit, or employment, as these often require a credit background check and/or a minimum credit score (OVC TTAC n.d.b; Dixon 2006; Synovate 2007). Victims of criminal identity theft may face further barriers to employment, as an erroneous criminal record coming up in a background check could prevent them from obtaining new employment (OVC TTAC n.d.c; Givens 2005; FTC 2017d; Pierce 2009).

Photo by Suphaksorn Thongwongboot/Shutterstock

Research and practice sources indicate a number of additional harms, including: harassment by collections agencies, utilities being cut off, being forced to declare bankruptcy, increased health insurance premiums (from medical identity theft in particular), having to relocate to reduce expenses, having to sell belongings, and missing work or other hobbies to resolve problems (Synovate 2007; ITRC 2017; Ponemon Institute 2013). Victims of housing-related scams, such as foreclosure rescue scams and mortgage refinancing scams that either charge homeowners for ineffectual assistance or transfer the deed of the home from the owner through trickery, can end up losing the equity of their homes (Saunders, Pizor, & Twomey 2009).

The prevalence of these hard-to-measure indirect financial harms is not entirely clear. FTC's 2006 Identity Theft Survey reports that 37% of identity fraud victims experienced these types of problems, with victims of new account frauds twice as likely as victims of existing non-credit card account fraud and four times as likely as victims of existing credit card fraud to do so (Synovate 2007). According to ITRC's 2017 Aftermath Study, denial of credit is the most common challenge facing victims of identity fraud, followed by challenges securing loans, debt, barriers to finding housing, and declaring bankruptcy (ITRC 2017).

Mental and Emotional Health Consequences

Experts in fraud victimization emphasize that the mental and emotional consequences of fraud victimization can resemble those of victims of violent crimes (NCVC & FINRA 2013). The emotional and mental response can include shame, fear, paranoia, disbelief, hopelessness, anger, loss of ability to trust, questioning of spiritual beliefs, perception of lack of justice, and even depression, anxiety, psychological disorders, and suicidality (Heckers & O'Brien 2014; NCVC & FINRA 2013; Texas Identity Theft Coalition 2010b; Texas Identity Theft Coalition 2010c; Golladay & Holtfreter 2017). Researchers even developed the term "Fraud Trauma Syndrome" to describe the emotional experience of victims of fraud (Goldstein, Goldstein, & Fornaro 2010).

Estimates of the extent of these negative mental and emotional responses to fraud victimization range from 20% to more than half of victims. Results of the 2008 NCVS-ITS suggest that 20% of identity fraud victims

Photo by Twin Design/Shutterstock

perceived the experience as "severely distressing" (Langton & Planty 2010). The 2014 NCVS-ITS found that 36% of victims experienced moderate or severe emotional distress (Harrell 2017) and in 2016, one in ten respondents reported that they were severely distressed as a result of the crime (Harrell 2019). That year, severe stress was most prevalent among victims whose information was used to open a new account or for fraudulent purposes (Harrell 2019). Further, among 172 victims of the Bernie Madoff Ponzi Scheme surveyed through an online convenience study for 8-10 months following the revelation of the scam, the majority of respondents met the criteria for post-traumatic stress disorder (Freshman 2012). Additionally, 61% of respondents reported high levels of anxiety and 58% reported symptoms of depression (Freshman 2012). The ITRC Aftermath Study reported that 56% of identity fraud victims experienced rage and 37% reported fear about their future (ITRC 2017).

Practitioners hypothesize about the reasons many victims of identity fraud and other fraud experience emotional responses to a financial crime. One potential contributing factor is the fear and perceived risk of revictimization (Texas Identity Theft Coalition 2010b; FTC 2017f). As described previously, victims of identity fraud and other fraud may experience revictimization due to their already compromised personally identifying information or the presence of their names on lists of supposedly susceptible targets available on the dark web. The realistic fear of revictimization may leave victims in a heightened emotional state. Additionally, practitioners note that non-responsive legal and law enforcement systems can make victims feel revictimized in instances when their cases go uninvestigated or unprosecuted (OVC 2010).

Physical Health Consequences

Fraud victims may experience physical health consequences related to the mental, emotional, and stress responses to their victimization, as they may miss out on rest, food, or social activities (OVC TTAC n.d.c). For example, the ITRC Aftermath Study found that, in 2017, 48% of identity fraud victims experienced sleep disturbances, 35% had fatigue, and 34% experienced headaches following their victimization (ITRC 2017).

Medical identity theft, where an individual's identity is used by a thief who obtains health services in their name (potentially with their health insurance), can also be the source of unique physical health consequences. As a result of medical identity theft, a victim's medical records can be incorrect, including blood type and medical history. In the worst-case scenario, this can be very dangerous, especially if information like blood type or allergies is only discovered in an emergency (Dixon 2006; Ponemon Institute 2013). Practitioner sources suggest that 20% of medical identity theft victims experience negative health outcomes including mistreatment, misdiagnosis, or delayed care (FTC 2017d).

> ***"Not only am I getting bills for hundreds of thousands of dollars, but operations, pregnancies, substance abuse treatment—even an extended stay in an in-patient mental health hospital—are all showing up on my child's medical history. He is only 5! And what happens if we get in a car accident or something and I can't tell them in the emergency room? Will this kill my baby?"***
>
> – A mother of a medical identity theft Victim served by the Colorado Bureau of Investigation
> *(Source: Heckers & O'Brien 2014)*

Legal Consequences

Civil and criminal legal troubles can also result from fraud victimization (Synovate 2007). For example, victims of many types of identity fraud can end up being sued for debts that they did not incur themselves (Pierce 2009).

Victims of **criminal identity theft** can face especially consequential legal troubles. In criminal identity theft, an identity thief uses another person's name at arrest when committing a crime or violating a law. In some cases, such as for traffic violations or misdemeanor crimes, the thief will be summoned for a court appearance and will not show, resulting in a warrant for the arrest of the victim. If the victim comes in contact with law enforcement, this can result in a false arrest (Givens 2005; Synovate 2007). Furthermore, the victim can incur a false criminal record. This can impact employment, housing, and other aspects of life for the victim (Heckers & O'Brien 2014).

> ***"I travel for my business. Now that this has happened, I have turned down jobs out of state because I'm afraid I might still be on a No-Fly List and end up in prison. The police told me the person using my ID has made terrorist threats against the President. That is really scary!"***
>
> – a victim helped by the Colorado Bureau of Investigation
> *(Heckers & O'Brien 2014)*

Housing Problems

Fraud victimization can create problems for victims seeking housing. First, as described above, victims of property-related frauds, such as mortgage refinancing scams, are sometimes tricked out of the deeds of their homes and can end up losing them, and thus losing their housing (Saunders, Pizor, & Twomey 2009). Second, as a result of lowered credit and/or erroneous criminal records, victims of fraud can be denied rental housing as a result of their background checks (OVC TTAC n.d.b).

Photo by Olivier Le Queinec/Shutterstock

Other Consequences

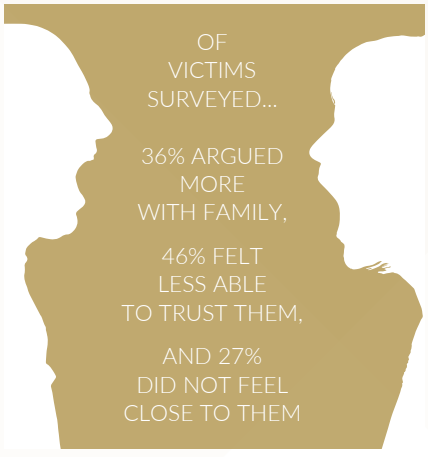
The harms of identity fraud and other fraud victimization can extend beyond the financial, health, legal, and housing problems to other realms of a victim's life.

First, the **time burden** of recovering from fraud can be substantial. On one hand, research shows that one-third to half of identity fraud victims are able to resolve

problems stemming from their victimization within one day (Synovate 2007; Harrell 2017, 2019; Langton & Planty 2010). However, some victims with more complicated cases can have protracted problems. One survey showed that one-third of victims had problems lasting at least a month (Harrell 2017) and two other surveys showed that one to three percent of victims still had problems after six months (Langton & Planty 2010; Harrell 2019). Practitioners emphasize that sometimes the problems, especially the fear associated with revictimization, may never entirely be resolved (FTC 2017d; FTC 2011f).

The total amount of time spent resolving these problems is thus uneven among victims; while the median number of hours spent resolving identity fraud problems was four, the top five percent of victims of identity fraud spent more than 130 hours addressing the crime (Synovate 2007). This time burden can also prevent victims from taking advantage of other opportunities (ITRC 2018a). As a result of the time cost to recovery, victims may have to take time away from their other life experiences, hobbies, vacations, and jobs. **It is important for service providers to prepare victims of identity fraud in particular that their recovery period may be protracted.**

Moreover, victims' **social relationships** can be strained or damaged as they may have to borrow money from friends or family, relocate to reduce life expenses, or suffer from a general lack of trust (Harrell 2019; ITRC 2017; Ponemon Institute 2013). The Identity Theft Resource Center's 2018 Aftermath Study found that 36% of victims surveyed argued more with family, 46% felt less able to trust them, and 27% did not feel close to them (ITRC 2018a). In some cases—particularly for victims of "imposter" or romance schemes—victims may become isolated from friends and family in favor of the fraud perpetrator (Deem & Lande 2018). Victims of certain types of identity fraud, such as social media impersonation, can also experience reputational damage as a result of their victimization (FTC 2017d). Likewise, victims may worry that friends and family will judge or lose respect for them as a result of their victimization (Deem & Lande 2018).



Lastly, victims of fraud can experience a variety of other harms specific to the unique type and circumstances of their victimization. For example, some victims of criminal identity theft could face challenges renewing their driver's license (OVC 2010) and victims of medical identity theft often suffer from a loss of privacy as their medical records are circulated between law enforcement, courts, and other agencies while attempting to resolve issues (Dixon 2006; Ponemon Institute 2013).

Aggravating Factors of Harms and Consequences

As described above, the harms and consequences of identity fraud and other fraud victimization are not evenly spread among all victims. The reasons that certain victims experience more severe consequences are not entirely clear and may include the type of victimization and characteristics of the victims themselves.

Research and practice propose several mechanisms that may increase the harms resulting from identity fraud and other fraud victimization. First, research suggests that the harms and consequences associated with fraud are compounded by the length of proceedings and the amount of time burden on the victim (Harrell 2017; Langton & Planty 2010; Ponemon Institute 2013; Synovate 2007). Relatedly, the inability to monitor financial information can lengthen the time to discovery and exacerbate the consequences of identity fraud victimization. For example, children, incarcerated people, and military members may not have access to, or think to check, their credit scores, which can result in problems going undetected as they deepen (FTC 2011f; OVC 2010).

As described previously, chronic victims can be repeatedly revictimized by the same perpetrator and may require early intervention to prevent additional victimization (Deem & Lande 2018). As a result, **it can be helpful for victim services providers to intervene as early as possible when working with victims of fraud**. Lastly, release of victims' private information to the public (especially false information such as health records) can intensify the negative impact of victimization on medical identity fraud victims (Dixon 2006; FTC 2017d; Ponemon Institute, 2013)

PREVENTION, INTERVENTION, AND VICTIM SERVICES

Key Takeaways

- Few interventions and services for identity fraud and other fraud victims have been evaluated. Most evaluated services focus on prevention and education, though other services include financial recovery assistance, hotlines, and case management.
- No programs were identified that address the mental health concerns of identity fraud and other fraud victims.
- Providing services for victims of identity fraud and other fraud can be challenging because the multiple types of crimes often require distinct paths to financial recovery.
- Victims of identity fraud and other fraud face barriers to recovery, including the lack of service providers, little cooperation from law enforcement or financial institutions, and prohibitive costs.

Given the many economic, legal, social, and health harms that victims of identity fraud and other frauds face, service providers must be prepared to help victims recover and also prevent future victimization. Practice evidence encourages advocates and others working with victims to have broad **knowledge about identity fraud and other fraud** (OVC 2010; IACP & Bank of America 2008b) and use a victim-centered, trauma-informed, and culturally sensitive approach that is tailored to each victim's needs (NCVC & FINRA 2013; Deem & Lande 2018). Service providers should also set **realistic expectations for victims** about what a normal trauma response looks like, that assets might not be recovered, potentially limited communication from agencies and law enforcement (NCVC & FINRA 2013; FTC 2011f; OVC TTAC 2018b; Texas Identity Theft Coalition n.d.a), the low likelihood of an investigation or prosecution (Deem & Lande 2018), and the possibility of revictimization (Heckers & O'Brien 2014; NCVC & FINRA 2013). Additionally, practitioners recommend tapping existing resources and services—especially multidisciplinary ones—to serve fraud victims (Deem & Lande 2018); this could be Adult Protective services or Financial Abuse Specialist Teams for older adults, child welfare services, or domestic violence service centers (Deem 2018; Thorleifson et al. 2009).

Prevention

Efforts to prevent fraud victimization center around education on warning signs, reporting, and help-seeking (O'Brien et al. 2012; Johnson 2003; FTC 2017d; FTC 2013a). There are also several fee-based services available to potential victims of identity frauds in particular.

Education programs are among the only programs for fraud victims that have been evaluated in research and are also among the limited set of programs oriented towards victims of frauds other than identity fraud. Prevention-focused educational efforts include awareness campaigns about recognizing frauds and preventing victimization amongst the general public or in specific groups that are particularly targeted or are typically underserved (NCVC 2014). Educational outreach about recognizing fraud can occur through a range of methods including community gatherings, door-to-door outreach, and social media (HUD Center for Faith-Based and Neighborhood Partnerships n.d.; Thorleifson et al. 2009). Outreach should occur regularly to update potential victims of new forms of scams or frauds (Thorleifson et al. 2009).

Preventative measures widely encouraged through educational campaigns include monitoring credit accounts and bills, protecting personal information, using strong passwords for accounts, reporting and ignoring spam or phishing emails and popups, and hanging up the phone on possible telephone fraud perpetrators, though the effectiveness of these practices is generally still unknown (NCVC & FINRA 2013; Schaffer et al. 2016; ITRC 2013; FTC 2000; IACP n.d.a; AARP 2003). One program, for example, sends out postcards that resemble prize scams and subsequently shares information about recognition and prevention of fraud to those who respond (Johnson 2003). Another intervention uses trained peer counselors to reach out by telephone to telemarketing fraud victims or potential victims of similar ages and backgrounds. The peer counselors share information about recognizing and not responding to these fraudulent calls, which has been found to be effective at reducing vulnerability to fraud victimization (AARP 2003).

Practice evidence emphasizes that consistent follow up is important for all preventative messaging, including about reporting, warning signs, and help-seeking (OVC 2010). One program, for example, provides fraud victimized seniors with volunteers who provide one-on-one contact to help victims avoid fraud by looking at mail and reviewing telemarketing calls together (Johnson 2003). Other sources suggest having support staff on-call for victims to contact when they're unsure of how to proceed after a contact from a fraud perpetrator (Thorleifson et al. 2009). Ongoing programs like this, however, are expensive, and are not widely available.

Research has also examined training programs that are designed to increase secure internet behavior and decease vulnerability to internet-based frauds like phishing attacks. One study found that training children could improve their ability to reject phishing, but that their newly acquired skills only lasted in the short term (Lastdrager 2017). Some studies of anti-phishing training programs show that they can be successful in raising subjects' self-perceived susceptibility, but that this has very little impact on changing actual behavior (Davison & Sillence 2010). Generally, research suggests that programs designed to prevent computer-based frauds still have progress to make in improving fraud prevention behavior.

Education and training efforts may also focus on **reporting** identity fraud and other fraud victimization, which plays an important role in connecting victims to services. However, as mentioned earlier, victims of fraud may not report due to embarrassment of being victimized or fears that their concerns will not be taken seriously by authorities (Cross et al. 2016). Therefore, programs have been developed to build communication between frequently targeted populations—such as older adults—and law enforcement (Nerenberg 2005). Research shows that victims of fraud in particular need clear and simple channels to report, including staff trained specifically in fraud victimization and connections to counseling and support services for their recovery (Cross et al. 2016). Additionally, victims of fraud report wanting respect from police and other authorities, non-judgmental listening, and acknowledgement of the crime committed against them (Cross et al 2016). To alleviate issues with embarrassment in reporting, practitioners suggest highlighting high-profile people who have experienced fraud to make victims feel more comfortable reporting themselves (Thorleifson et al. 2009).

In addition to educational measures aimed at preventing various types of fraud, preventative services for identity frauds in particular include credit and identity monitoring, which are usually provided by for-profit companies for a fee, either to the client or to a third party footing the cost, such as a company providing the service to customers after a data breach.

Credit Monitoring

Credit monitoring is a service provided to victims or potential victims of new account identity fraud only. People who suspect or know they have been victims of identity theft (meaning their personal information has been obtained by someone else) use it as a preventative measure, while those who have already been victimized by identity fraud use it to prevent revictimization. In this intervention, a for-profit victim service provider monitors a person's credit for the opening of new accounts and notifies the victim if that occurs (GAO 2017).

Credit monitoring is designed to protect against the negative consequences of new account fraud, because practice suggests that it can potentially detect identity fraud earlier and allow a victim to take action. However, credit monitoring itself does not prevent, stop, or remedy new account fraud (GAO 2017; Givens 2014; CFA 2009). Furthermore, credit monitoring is not a method to prevent other forms of identity fraud, such as existing account fraud, medical identity theft, or tax fraud, unless those frauds are so extensive that they draw attention in a credit report (GAO 2017; CFA 2009).

Given the costs associated with this service, some practitioners suggest free or low-cost alternatives, such as obtaining a credit freeze, placing a fraud alert with the

Photo by Andrey_Popov/Shutterstock

credit reporting agencies, or accessing free credit reports. These alternatives are usually provided to victims at no or low cost and can also enable a victim to monitor the potential presence of new accounts in their name (GAO 2017; CFA 2009).

Identity Monitoring

Identity monitoring involves a third party looking at sources other than credit reports for a victim's or potential victim's personally identifying information. Sources include public records, arrest records, sex offender registries, United States Postal Service change of address registries, black market websites, the dark web, and proprietary databases (GAO 2017). Like credit monitoring, identity monitoring neither prevents nor remedies identity fraud, and a victim of identity fraud would need to consider taking further corrective action to protect themselves. Also, similar to credit monitoring, identity monitoring is usually provided by for-profit companies. However, unlike credit monitoring, this is usually a service that a potential victim could not provide themselves (GAO 2017). The impact of identity monitoring is unknown because, to date, it has not been evaluated (GAO 2017).

Even with strong messaging, consistent follow-up, and the use of monitoring and fraud prevention service offerings, **the impact of preventative measures by individuals may be limited**, especially for identity related frauds. Although personally identifying information can be compromised by an individual—through a lost social security card or tax documents left in a mailbox for too long—it is often lost at the institutional level, though data breaches at companies or medical providers (Givens 2000c; Dixon & Barrett 2013; Breyault 2013). Further, practice evidence emphasizes that in order for personally identifying information to be used for identity fraud, it also needs to be reviewed and approved by a creditor. As a result, there are many opportunities for prevention that are available and necessary at the institutional level that should be explored further to prevent fraud victimization.

Interventions and Services

Once someone has experienced identity fraud or other fraud victimization – and potentially some or all of the myriad economic, mental health, social and legal consequences outlined above – the field has a limited array of services to help them recover and prevent further victimization. Primarily, those **services are targeted towards the victims of identity frauds**, for whom they usually focus on the direct, rather than indirect, **economic costs of victimization**. While interventions for victims of other frauds are more limited, the field has several suggested and promising practices for those victims, particularly for older adult victims.

Photo by Monkey Business Images/Shutterstock

A number of the services for victims of identity and non-identity related fraud involve **direct, hands-on supports** by a non-profit or private provider, which can be crucial to the recovery of victims with certain limitations, such as victims who are children, or victims with limited English proficiency, developmental delays, or memory challenges. These hands-on supports are also important for victims with complicated cases, such as those who are victimized by non-financial identity frauds (like medical or criminal identity theft), those who are being sued or harassed by creditors or debt collectors, those who are encountering uncooperative creditors or other agencies, or those who are chronic victims (Deem 2018; FTC 2013b). Practitioners agree that, in these cases, providers should expect to provide long-term services over multiple sessions (Deem 2018; OVC TTAC n.d.b; OVC 2010). However, practice evidence supports the idea that sharing detailed self-help materials can provide financial recovery to the majority of victims of identity frauds especially, which the FTC refers to as a "**guiding approach**" (FTC 2013b; OVC 2010; CFA 2015).

Most of those services target financial recovery for victims of frauds, and outside of that there are **only very limited legal services and mental health supports targeted specifically for fraud victims.**

Identity Restoration

Identity restoration services are the supports provided to victims of identity fraud designed to help them recover from mainly the financial harms of victimization. Typically, this involves a service provider directly reaching out to creditors, credit reporting agencies, and other financial institutions for or with a victim. The steps taken by a service provider mirror those typically offered in self-help materials for victims who can reach recovery through the "guiding approach" (FTC 2013b). Importantly, the practice-supported steps to identity recovery frequently change, as the field gains understanding and the laws surrounding identity fraud and other frauds change. The protections and requirements reflected below are true at the time of writing, but practitioners should consult local and federal laws and guidance to provide the current and most accurate information and support to victims.

Practice evidence sources generally recommend a few general responses to move toward financial remediation of the harms of identity frauds, particularly those involving credit accounts. These options should be approached differently depending on each individual case and type of identity fraud involved. Notably, these responses have not been evaluated, but are supported by key practitioner organizations and authorities in the space, like the FTC. One response area is **reporting to the FTC and/or law enforcement**. The FTC both tracks fraud complaints and can provide victims with documentation of their victimization to share with creditors and financial institutions. Law enforcement most likely will not be able to investigate the crime, but in some instances a police report can be used in conjunction with FTC documentation to confirm that one is a victim of identity fraud (Heckers & O'Brien 2014; OVC 2010).

IDENTITY RESTORATION REQUIRES VICTIMS TO CONNECT WITH NUMEROUS AGENCIES

Another response is communicating with creditors, financial institutions, and credit reporting agencies (CRAs) to cancel the compromised accounts and to repair the victim's credit score (FTC 2016f; FTC 2013b).

Third, victims and the service providers supporting them can **utilize a number of legal and other protections to prevent further victimization**. Practice evidence emphasizes that revictimization is always a real possibility for victims of identity fraud; once personally identifying information has been stolen, the perpetrator could attempt to use it again or sell it through mediums on the dark web, for example (Heckers & O'Brien 2014; Pierce 2009). As such, remaining vigilant and taking steps to prevent revictimization is crucial. Examples of such preventative steps include **initial fraud alerts**, which require creditors to take additional identity verification steps for a limited amount of time (FTC 2018c; FTC 2016f; FTC n.d.c; IACP n.d.b; FTC 2013b); extended fraud alerts, which last for several years (CFA 2009; FTC 2013b); credit or security freezes, which prevent potential creditors from accessing one's credit report and, thus, granting new credit (FTC 2013b; FTC 2018b; FTC 2018d; CFA 2009; GAO 2017); and changing the victim's Social Security Number (SSN).

Fair and Accurate Credit Transactions Act of 2003 (FACTA). FACTA is the federal law that protects victims of credit-related identity frauds. Its main provisions dictate that victims can place fraud alerts on their credit reports, can dispute inaccurate information on their report, and that credit reporting agencies and creditors must take steps to clear erroneous information (OVC 2010).

These strategies all have strengths and benefits that must be weighed for each victim. For example, credit freezes only protect against credit-related identity frauds and extended fraud alerts do not prevent fraud in existing accounts (GAO 2017; CFA 2009; FTC 2016f). Changing a social security number can be particularly complex, as so many aspects of one's life are linked to the SSN, and, further, the Social Security Administration holds the power to approve or reject a change (FTC 2011f; FTC 2012l).

Importantly, practice evidence highlights that cases of non-credit-related financial identity frauds—such as tax identity

fraud, student loan identity fraud, or employment fraud—may be more complicated and require additional help (FTC 2016f). For example, addressing the financial harms of student loan identity fraud (when someone else takes out student loans in a victim's name) can be challenging, because the victim must take extra steps to inform the U.S. Department of Education. In some cases, they may need a court verdict that proves victimization to substantiate their claim, which is not typical or easy to obtain (Heckers & O'Brien 2014; FTC 2013b; OVC TTAC n.d.j; FTC 2013b). Likewise, tax and employment identity fraud can involve additional steps of contacting the Internal Revenue Service (IRS) and/or the Social Security Administration (SSA) and following their remediation processes (FTC 2016f; OVC TTAC n.d.h; Pierce 2009).

Although identity restoration services and self-help materials typically focus on identity frauds related to credit or bank accounts (GAO 2017), **there are distinct response options to support victims of other identity frauds, like medical or criminal identity theft**. Generally, practice evidence is less robust in addressing these types of identity fraud, and research evidence is sparse. For criminal identity theft, for example, recovery steps are piecemeal and vary by state. Generally, victims must get a letter of clearance from law enforcement; communicate with the criminal records agency, courts, and possibly motor vehicle departments in their state; and in some cases even carry the clearance letter with them at all times (ITRC 2000; Pierce 2009). Some states have developed **Identity Theft Passports** for victims of criminal identity theft to carry and present to law enforcement for this purpose (Pierce 2009). Criminal identity theft victims may have to continue to clear their name by communicating with potential employers, landlords, and background check companies over time (ITRC 2018b). Similarly, **medical identity theft** recovery involves very different steps than typical identity fraud recovery. Generally, victims must report their victimization to authorities and communicate with medical providers and insurance companies to add information to their files about the fraud (Pierce 2009).

The steps towards identity restoration for victims of identity fraud are crucial to financial recovery, whether completed by the victim themselves of by a service provider. In addition to identity restoration services, a number of other intervention services exist to meet the needs of victims of identity fraud (and other fraud as well).

Case Management

Crisis and long-term case management services have been identified by practitioners as crucial to the recovery of some fraud victims. In particular, these services have been identified as helpful to chronic victims of non-identity related frauds, especially older adults, who require ongoing support (Deem 2018; Deem & Lande 2018). Crisis case management services—designed for immediately after an incidence of victimization—include planning for the victim's safety; addressing critical emotional needs; and finding resources to fill in financial gaps, such as emergency funds for rent or food bank access (Deem & Lande 2018).

In the longer term, case management can include supports to find work/financial resources; assistance making new, positive connections and activities instead of maintaining contact with the perpetrator; and long-term education on identifying frauds, knowing how to respond, and understanding where to report them (Deem 2018; Deem & Lande 2018). Although crisis and case management services for fraud victims are uncommon, practitioners have successfully leveraged existing resources for these victims; for example, some domestic violence service providers and Area Aging Centers in California have allowed certain fraud victims to access crisis management services (Deem 2018).

Hotlines

Telephone hotlines are typically available 24-hours a day to receive reports and answer questions about identity fraud and other fraud victimization. Some hotlines, like that run by the Colorado Bureau of Investigation, are available to victims of identity-related frauds, other frauds, and even other cybervictimizations, while others, like the U.S. Department of Justice's Disaster Fraud Hotline or the National Telemarketing Victim Call Center, are more targeted. Although the impact of this intervention on fraud victims has not yet been evaluated, hotlines aim to provide a hub for education of the public, an outlet for reporting, connections between victims and services, and advice on recovery for fraud victims (O'Brien et al. 2012; OVC 2010; IACP & Bank of America 2008a; Deem & Lande 2018).

Legal Services

Legal services are a key resource for victims of identity fraud and other fraud to address the potential civil or criminal legal needs outlined above. Outside of victims of criminal identity theft—who may require additional services—most victims of identity fraud and other fraud require legal services to respond to lawsuits from creditors or debt collectors, get court orders to prove their victimization, clear public records, prepare a victim impact statement, or recuperate financial losses (OVC 2010; FTC 2013b). Private civil legal services can be expensive, so services offered through Pro Bono opportunities or legal aid agencies are essential. In some cases, an existing attorney could be used to support civil legal needs from fraud, such as the Guardian ad Litem (court assigned legal representative) for a child in the child welfare system (NCVC & FINRA 2013; OVC 2010; FTC 2011f).

Legal services play a particularly important role in recuperating direct financial losses from victimization (Pierce 2009; NCVC 2017). While identity theft insurance (a paid service) can compensate a victim for the direct and time costs associated with recovery, navigating the legal system is often the only way to get stolen money back. This could entail filing a lawsuit, arbitration, or mediation through the civil legal system (NCVC & FINRA n.d.a). Settlements can include damages to compensate for the direct losses and the emotional/health/non-economic harms and sometimes even punitive damages (Andres 2015).

Despite this potential, civil legal services for victims of fraud still face a number of problems. First, although some states allow attorney's fees to be recovered in a settlement, not all states do. This disincentivizes private attorneys from working these cases and leaves them to legal aid or Pro Bono providers that are often already overburdened (NCVC 2014; NCVC 2017; Andres 2015). Additionally, even when a judgment is awarded in the victim's favor, the perpetrator may have already spent the money and may be unable to pay what is owed (Pierce 2009). As a result, though promising, civil legal services are by no means a guarantee that a victim will recover their direct financial losses.

The criminal justice system, on the other hand, is rarely able to help victims recover their financial losses.[2] First, prosecution of identity fraud and other fraud perpetrators is rare. Reasons for this include the relatively low financial losses that characterize many frauds and the challenging nature of investigating and prosecuting crimes that may be nationwide or international in scope (Deegan 2018). Second, even with a successful prosecution where restitution is ordered, victims do not always receive the ordered payments. Additionally, restitution orders do not cover any financial costs beyond the money directly stolen. Third, victim compensation is often not available to victims of fraud, because many state's compensation systems are exclusively open to victims of violent crimes (NCVC 2017; Pierce 2009). Accordingly, practice evidence suggests that victims are more likely able to recover financially with civil legal services, despite the challenges that lie there.

Mental Health Services

Lastly, mental health services are important for victims of identity fraud and other fraud (FTC 2011f). Although research evidence on mental health interventions for fraud victims is underdeveloped, practice evidence offers limited information on the specific practices of value to these victims. For example, for those victims who experience trauma responses to their victimization, trauma-focused therapy can play an important role in recovery (Texas Identity Theft Coalition 2010b). This therapy should include education about prevention of revictimization, which can counter a victim's sense of lack of control; exercises to help develop social supports and address the sense of mistrust a victim may feel; psychoeducation; and coping strategies (Texas Identity Theft Coalition 2010b).

2 There are some notable exceptions to this. For example, victims of various frauds related to the Enron corporation were collectively awarded over $40 million in restitution (DOJ 2017) and prosecutors at various levels of government pursue cases of identity theft and fraud each year (IRS 2016).

Practitioners recommend in-home counseling, when possible, to mitigate potential embarrassment victims could face in seeking services (Deem 2018). They have also highlighted the utility of peer support groups for victims of fraud. These groups can be led by professional social workers or therapists and can take place online, over the phone, or in-person (Deem 2018).

Barriers to Services

Despite the variety of services and interventions that exist to meet the needs of victims of fraud, victims can face barriers to reaching these services and recovering. These challenges include the cost of accessing services, lack of supports, failure to cooperate on the part of institutions, and lack of legal protections.

First, victims seeking care for the mental and physical health consequences are often prevented by the **cost of these services**. The ITRC's 2017 Aftermath Study found that more than 15% of survey respondents who did not seek health services for physical symptoms failed to do so because they could not afford it, and 13% of respondents who did not seek mental health supports similarly cited the prohibitive cost (ITRC 2017). As another example, legal services can be prohibitively expensive; although many low-income people (approximately 20% of the U.S. population) qualify for legal aid or Pro Bono attorneys, many middle-income victims above the qualifying income threshold are also challenged to afford legal counsel (DOJ 2014).

Second, victims can be prevented from receiving support when there is a lack of trained service providers prepared to help fraud victims, especially with long-term case management services (Deem 2018; FTC 2011f; Thorleifson et al. 2009). Practice evidence sources, including those from the Office for Victims of Crime, have expressed concern that VOCA-funded programs have historically not included victims of fraud, and that many service providers do not have the training, funding, and capacity to recognize the severity of fraud's harms (OVC 2010). Victims who are unable to access these services may then feel blamed for their circumstances, unsupported, or that they have to prove their own case and recover on their own (Deem & Lande 2018; OVC TTAC n.d.b; OVC 2010).

Third, victims may face challenges in reaching recovery because of a lack of cooperation from the necessary institutions and agencies, including law enforcement, creditors, and banks. First, practice evidence suggests that historically law enforcement agencies have not been supportive of fraud victims. For example, victims that filed complaints sometimes meet resistance from police to filing an official report (Pierce 2009; Givens 2000a). Practitioners attribute this lack of cooperation to a dearth of training on the topic for law enforcement and communication gaps between communities and law enforcement on how to discuss the crimes (IACP & Bank of America 2008b; OVC 2010). Law enforcement may also lack the capacity or knowledge to handle crimes that are transnational or cyber in nature (Deem & Lande 2018). Further, victims may face challenges communicating with their creditors—who may be incredulous of their claims—or credit reporting agencies—which may be hard to reach (Givens 2000a).

Lastly, victims of certain frauds face additional challenges because of a lack of legal protections. Medical identity theft victims do not have comparable protections to victims of other types of identity fraud. For example, at the time of writing, while victims of financial identity fraud are legally permitted to correct their credit reports when impacted by fraud, medical identity theft victims are not. A victim cannot even insist that a medical provider use their correct information over that of the fraud perpetrator (Dixon 2006). As such, the challenges with uncooperative institutions can be exacerbated; for example, some providers won't share or correct medical records, in order to protect the imposter's privacy (Pierce 2009; OVC 2010; Dixon 2006). Further aggravating these difficulties is the fact that medical records are not centralized in the way that financial records are (via credit reporting agencies), making it even more difficult to monitor and prevent revictimization (FTC 2017d). As another example, not all states include identity fraud in their state victims' rights amendment. This affects the ability of victim compensation programs to offer support to those victims.

Overall, victims of identity fraud and other fraud can face challenges receiving services because of a lack of understanding of the crime. In particular, the variations in victimization—from the type of fraud to the type of victim—require particularly knowledgeable service provision (FTC 2017d). To respond to victims of fraud effectively, the field must be educated on the variety of harms and consequences and the available services to remedy those harms.

IMPLICATIONS FOR RESEARCH, POLICY, AND PRACTICE

CVR's review of research, practice, and contextual evidence on identity fraud and other fraud victimization points to four key implications for victim-centered research, policy, and practice, as follows:

(1) The field needs more research on identity fraud and other fraud victimization.

This includes a need for clarification on language about identity theft, identity fraud, and other frauds; particular attention to different stages of identity-related crimes; and the completion of more studies to capture lifetime prevalence, harms of victimization, and effectiveness of prevention efforts and services for victims.

Research studies and agencies collecting data on fraud often fail to distinguish between the types of frauds. For example, many studies combine different crimes (such as criminal fraud, account takeover, Ponzi schemes, etc.) under the umbrella terms of identity theft, identity fraud, and fraud. Researchers and agencies collecting data on these crimes should better distinguish between the detailed categories of crimes in order to understand the differences between specific fraud types. This is especially important in understanding certain emerging fraud types, such as synthetic identity theft—where pieces of personally identifying information from different victims are used to create new, fake identities—frauds affecting individuals in disaster regions, and internet auction frauds. Understanding the prevalence, risk factors, and specific consequences of each type of fraud is crucial for the field; victim service providers must have access to the details of each in order to best respond to victims.

In addition to disaggregating fraud types, it is important for the field to begin to distinguish between the stages of the crime, especially for identity-related crimes. Researchers and agencies collecting data on identity theft should pay specific attention to 1) the acquisition of identity information, 2) the use of identity information to commit fraud, and 3) the outcomes of identity theft. This kind of a staged approach to identity-related crime estimation will better allow researchers to explore the different motivations to commit identity-related crimes, the profiles of those who commit identity and other fraud, and the losses associated with fraud (Newman & McNally 2005).

Additionally, more research studies are needed to capture (1) lifetime prevalence of fraud victimization and the impact of prior victimization on subsequent victimizations and (2) state- and regional-level identity fraud and other fraud trends; (3) services, programs for addressing emotional and mental health outcomes of identity theft and other fraud; (4) the impact of training and awareness campaigns on victimization, re-victimization, and secure behavior; and (5) impact of legal services on post-fraud outcomes. Furthermore, very few studies focus on the views that victims and practitioners have of victims' needs.

(2) It is important for service providers and policymakers to expand victim services to reach all fraud victims and to address their varied needs.

Because the harms of identity fraud and other fraud can be extensive and can include not only financial consequences but negative impacts on physical, mental, legal, and social standing, it is important for the field to be equipped with interventions to meet all these needs. However, the most established services are targeted towards remedying the financial harms of financial identity frauds, such as existing or new account fraud. Services meeting the needs of victims of other types of frauds and meeting other harms—such as stress, mental trauma, physical health consequences, and legal needs—are not as robust.

In contrast to the lack of evidence around the effectiveness of those services, there is a well-established research base addressing non-financial harms faced by fraud victims. These findings should guide the development of interventions and services tailored to the needs of victims of fraud. Further, the field should continue to strive to reduce barriers to victims receiving these services through methods such as expanding the eligibility of victim compensation, providing low-cost services to a wider variety of income levels, and continuing outreach to communities and groups typically underserved by victim services.

(3) More knowledge about, and awareness of, identity fraud and other fraud is needed amongst the general public and within the victim services field.

Widespread educational campaigns are needed to promote preventative measures, encourage reporting, and facilitate help seeking of existing victims. These campaigns should reach the entire public and also include targeted messaging to communities vulnerable to certain types of fraud (Holftreter et al. 2005).

Organizations and professionals working with victims of identity fraud and other fraud—from service providers, law enforcement officers, and employees of creditors and banks—also require more understanding of the wide range of needs and experiences that victims of different types of frauds face. Understanding the variety of fraud types and the variety of victims can promote cooperation from these entities and facilitate useful skills for promoting recovery. For example, knowing that different populations are likely to be victims of different types of scams and frauds can allow service providers to communicate this to victims, thus alleviating embarrassment and increasing victims' willingness to report the crime (NCVC & FINRA 2013).

(4) Efforts within the victim services field to address the needs of individual victims must be complemented by policy and practice solutions to prevent exposure of personally identifying information at the business- and institutional-levels, especially for identity fraud.

Given the likelihood of revictimization and limited nature of recovery from certain forms of identity fraud—for example, medical identity theft and new account fraud resulting from a data breach—greater preventative efforts are required at the business and institutional levels. This regulation could come from legislative response or industry self-regulation (Shoudt 2002). Although institutional regulation and responses are outside the scope of the review, it is an important contextual note that the victim services field would benefit from such preventative efforts.

Overall, the prevalence of identity fraud and other fraud, its varied and wide-reaching harms, and the complicated nature of victims' recovery processes point to the importance of these crimes to the victim services field. Fraud can affect victims' finances, relationships, justice-system status, and health. However, prevalence efforts lack specificity on fraud subtypes, risk factors remain relatively un-investigated by research, and few intervention and preventive services have been evaluated by researchers. As the field continues to develop, the knowledge base and availability of services for fraud victims must expand to better respond to fraud victims' needs.

This document was produced by the Center for Victim Research (CVR) under grant number 2016-XV-GX-K006, awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this document are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice. The primary authors of this document were CVR researchers, **Yasemin Irvin-Erickson, PhD** and **Alexandra Ricks, BA**. The CVR also acknowledges thoughtful contributions from subject matter experts, Eva Velasquez, Dr. Kristy Holtfreter, and Hazel Heckers, who reviewed earlier drafts of this synthesis.

REFERENCES

AARP Foundation. (2003). *Off the Hook: Reducing Participation in Telemarketing Fraud*. Retrieved Jun 2019 from https://assets.aarp.org/rgcenter/consume/d17812_fraud.pdf

Allstate Foundation and National Network to End Domestic Violence (NNEDV). (2016). *Module One: Understanding Financial Abuse.* Retrieved from https://nnedv.org/mdocs-posts/module-one-understanding-financial-abuse/

Anderson, K.B. (2004). *Consumer Fraud in the United States: An FTC Survey.* Retrieved Jun 2019 from https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-ftc-survey/040805confraudrpt.pdf

Anderson, K.B. (2007). *Consumer Fraud in the United States: The Second FTC Survey.* Retrieved Jun 2019 from https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-second-federal-trade-commission-survey-staff-report-federal-trade/fraud.pdf

Anderson, K.B. (2013). *Consumer Fraud in the United States, 2011: The Third FTC Survey.* Retrieved Jun 2019 from https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf

Andres, M. N. (2015). Making elder financial exploitation cases part of a sustainable practice: Tips from the experiences of the University of Illinois College of Law's Elder Financial Justice Clinic. *Elder Law Journal*, *23*, 297.

Beals, M., DeLiema, M., & Deevy, M. (2015). Framework for a taxonomy of fraud. *Financial Fraud Research Center at Stanford Center on Longevity and FINRA Investor Education Foundation.* Retrieved Jun 2019 from http://longevity3.stanford.edu/framework-for-a-taxonomy-of-fraud/

Breuer, L. (2011). *Disaster Fraud Task Force: Report to The Attorney General for Fiscal Year 2011*. Washington, DC: Department of Justice. Retrieved from https://www.justice.gov/sites/default/files/criminal-disasters/legacy/2013/04/04/ReportDFTF2011.pdf

Breyault, J. (2013). *The State of Identity Theft In 2013: A National Consumers League White Paper Examining Fifteen Years of Federal Anti-Identity Theft Consumer Protection Policies.* National Consumers League. Retrieved from https://www.slideshare.net/nationalconsumersleague/breyault-id-theftwhitepaper-final-2

Bureau of Justice Statistics (BJS). (2018). *Identity Theft.* Retrieved from: BJS 2018. Identity Theft. Retrieved from: https://www.bjs.gov/index.cfm?ty=tp&tid=42

Burton, C. (1998). *Consumer Fraud: A 2008 Survey of AARP Colorado Members' Experiences and Opinions*. Washington, DC: AARP Foundation.

California Department of Justice. (2018). *First Aid for Medical Identity Theft: Tips for Consumers.* Retrieved from https://oag.ca.gov/privacy/facts/medical-privacy/med-id-theft

Campbell, J. (2013). *Fraud on The Elderly: A Growing Concern for A Growing Population.* Washington, DC: US Department of Justice, Federal Bureau of Investigation, Criminal Investigation Division. Retrieved from https://www.justice.gov/iso/opa/ola/witness/05-16-13-fbi-campbell-testimony-re-fraud-on-the-elderly--a-growing-concern-for-a.201385141.pdf

Canan, S. & Hume, C. (2016). *Older Consumers Targeted by Fraudsters Not Once, But Twice!.* Consumer Financial Protection Bureau. Retrieved from https://www.consumerfinance.gov/about-us/blog/older-consumers-targeted-by-fraudsters-not-once-but-twice/

Consumer Federation of America (CFA). (2009). *To Catch a Thief: Are Identity Theft Services Worth the Cost?*. Retrieved from https://consumerfed.org/wp-content/uploads/2016/09/3-1-09-To-Catch-A-Thief_Report.pdf

Consumer Federation of America (CFA). (2015). *Best Practices for Identity Theft Services, Version 2.0.* Retrieved from https://consumerfed.org/pdfs/CFA-Best-Practices-Id-Theft-Services.pdf

Consumer Financial Protection Bureau (CFPB). (2014). *Protecting Residents from Financial Exploitation: A Manual for Assisted Living and Nursing Facilities.* Retrieved from https://files.consumerfinance.gov/f/201406_cfpb_guide_protecting-residents-from-financial-exploitation.pdf

Cross, C., Richards, K., & Smith, R.G. (2016). *Improving Responses to Online Fraud Victims: An Examination of Reporting and Support.* Retrieved Jun 2019 from http://crg.aic.gov.au/reports/1617/29-1314-FinalReport.pdf

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior, 26*(6), 1747.

Deegan Jr., P.E. (2018). Elder financial fraud schemes: The case for federal investigation and prosecution. *US Att'ys Bull.*, *66*, 31.

Deem, D. (2018). *International Financial Crimes: How Do We Turn the Tide and Help Older Victims?* Federal Bureau of Investigations. Retrieved from https://www.elderjusticecal.org/uploads/1/0/1/7/101741090/debbie_deem-elder_justice_ca_aug1_with_sbaker_7.29.18-1.pdf

Deem, D., & Lande, E. S. (2018). Transnational scam predators and older adult victims: Contributing characteristics of chronic victims and developing an effective response. *US Att'ys Bull.*, *66*, 177.

DePaul, S. (2010). *The Hallmarks of Consumer Fraud Targeting Senior Victims: A Primer on How to Identify, Deter, And Defend Against Consumer Fraud.* National Consumer Law Center and the Administration on Aging. Retrieved from http://www.nclc.org/images/pdf/conferences_and_webinars/webinar_trainings/presentations/2010/presentation_april14.pdf

Dinger, E.L., & Sauer, J.H. (2006). Protecting your name: A survey of Montanans on identity theft. *AARP Knowledge Management, AARP Research.* Retrieved Jun 2019 from https://www.aarp.org/money/scams-fraud/info-2006/mt_id.html

Dixon, P. (2006). *Medical Identity Theft: The Information Crime That Can Kill You.* World Privacy Forum. Retrieved from http://www.worldprivacyforum.org/wp-content/uploads/2007/11/wpf_medicalidtheft2006.pdf

Dixon, P. & Barrett, T. (2013). *Medical Identity Theft.* Office for Victims of Crime's National Identity Theft Network. Retrieved from https://www.youtube.com/watch?v=sOa6AWzHSEs

Federal Bureau of Investigation (FBI). (2019). *National Incident-Based Reporting System (Nibrs).* Retrieved from https://www.fbi.gov/services/cjis/ucr/nibrs

Federal Trade Commission (FTC). (1998). *Identity Theft and Assumption Deterrence Act (ITADA).* Retrieved from: https://www.ftc.gov/node/119459

Federal Trade Commission (FTC). (2000). *ID Theft: When Bad Things Happen to Your Good Name.* Retrieved from https://archives-financialservices.house.gov/banking/91300ftc.pdf

Federal Trade Commission (FTC). (2005). *Fraud and ID Complaints Received by the FTC from Consumers Age 50 and Over.* Retrieved Jun 2019 from https://www.ftc.gov/sites/default/files/documents/reports_annual/fraud-and-id-complaints-received-ftc-consumers-age-50-and-over-cy-2004/fraud-idtage50-cy2004.pdf

Federal Trade Commission (FTC)(2010b). *Medical Identity Theft.* Retrieved from https://www.ovcttac.gov/downloads/identitytheftnetwork/toolkit/TrainingMaterials/FTC-FactsForConsumersMedicalIDTheft.pdf

Federal Trade Commission (FTC). (2011d). *Prepared Statement of The Federal Trade Commission Before the Subcommittee on Social Security of The House Committee on Ways and Means on Child Identity Theft.* Retrieved from https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-child-identity-theft/110901identitythefttestimony.pdf

Federal Trade Commission (FTC). (2011f). *Stolen Futures: A Forum on Child Identity Theft.* Retrieved from https://www.ftc.gov/news-events/events-calendar/2011/07/stolen-futures-forum-child-identity-theft

Federal Trade Commission (FTC). (2012l). *Scams Against Immigrants.* Retrieved from https://www.ftc.gov/news-events/audio-video/video/scams-against-immigrants

Federal Trade Commission (FTC). (2013a). *FTC Senior Identity Theft Workshop.* Retrieved from https://www.ftc.gov/sites/default/files/documents/videos/senior-identity-theft-workshop-part-1/130507senioridtheft_sess1.pdf

Federal Trade Commission (FTC). (2013b). *Guide for Assisting Identity Theft Victims.* Retrieved from https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf

Federal Trade Commission (FTC). (2014e). *Pass It On: Imposter Scams.* Retrieved from https://www.consumer.ftc.gov/articles/pdf-0180-imposter-scams.pdf

Federal Trade Commission (FTC). (2016f). *Identity Theft: A Recovery Plan.* Retrieved from https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf

Federal Trade Commission (FTC). (2017a). *Businesses Must Provide Victims and Law Enforcement with Transaction Records Relating to Identity Theft.* Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/businesses-must-provide-victims-law-enforcement-transaction

Federal Trade Commission (FTC). (2017d). *Identity Theft: Planning for The Future, Parts 1, 2, and 3.* Retrieved from https://www.ftc.gov/news-events/audio-video/video/identity-theft-planning-future-part-1

Federal Trade Commission (FTC). (2018a). *Consumer Sentinel Network Data Book 2017.* Washington, DC: Federal Trade Commission. Retrieved from https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf

Federal Trade Commission (FTC). (2018b). *Extended Fraud Alerts and Credit Freezes.* Retrieved from https://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes#Why

Federal Trade Commission (FTC). (2018c). *Free Credit Freezes Are Here.* Retrieved from https://www.consumer.ftc.gov/blog/2018/09/free-credit-freezes-are-here

Federal Trade Commission (FTC). (2018d). *New Credit Law FAQs.* Retrieved from https://www.consumer.ftc.gov/blog/2018/10/new-credit-law-faqs

Federal Trade Commission (FTC). (2019a). *Consumer Sentinel Network Data Book 2018.* Washington, DC: Federal Trade Commission. Retrieved from https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018_0.pdf

Federal Trade Commission (FTC). (2019b). *Pyramid Schemes.* Retrieved: https://www.ftc.gov/public-statements/1998/05/pyramid-schemes

Federal Trade Commission (FTC). (n.d.b). *Know Your Rights.* Retrieved from https://www.identitytheft.gov/Know-Your-Rights

Federal Trade Commission (FTC). (n.d.c). *Statement of Rights for Identity Theft Victims.* Retrieved from https://www.ovcttac.gov/downloads/identitytheftnetwork/toolkit/TrainingMaterials/IDTheftVictimStatementOfRights.pdf

Freshman, A. (2012). Financial disaster as a risk factor for posttraumatic stress disorder: Internet survey of trauma in victims of the Madoff Ponzi scheme. *Health & Social Work*, *37*(1), 39-48.

George, J. (2018). *The Man with The Stolen Name*. The Marshall Project. Retrieved from https://www.themarshallproject.org/2018/05/14/the-man-with-the-stolen-name?utm_medium=email&utm_campaign=newsletter&utm_source=opening-statement&utm_term=newsletter-20180515-1052

Givens, B. (2000a). *Identity Theft: How It Happens, Its Impact on Victims, And Legislative Solutions*. Privacy Rights Clearinghouse. Retrieved from https://www.privacyrights.org/blog/identity-theft-how-it-happens-its-impact-victims-and-legislative-solutions

Givens, B. (2000c). *ID Theft: A Rapidly Growing Crime That Scars Its Victims*. Consumer Action. Retrieved from https://www.consumer-action.org/news/articles/2000_identity_theft_issue#Topic_01

Givens, B. (2005). *Criminal Identity Theft in California: Seeking Solutions to the "Worst Case Scenario"*. Privacy Rights Clearinghouse. Retrieved from https://www.privacyrights.org/blog/criminal-identity-theft-california-seeking-solutions-worst-case-scenario

Givens, B. (2014). *Senate Judiciary and Banking Committee Hearing on Data Breaches, Panel One: Data Breach Law and Identity Theft Prevention*. Privacy Rights Clearinghouse. Retrieved from https://www.privacyrights.org/blog/senate-judiciary-and-banking-committee-hearing-data-breaches-panel-one-data-breach-law-and

Glodstein, D., Glodstein, S.L., & Fornaro, J. (2010). Fraud trauma syndrome: The victims of the Bernard Madoff scandal. *Journal of Forensic Studies in Accounting and Business*, *6*, 1-9.

Golladay, K.A., & Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders*, *12*(5), 741-760.

Government Accountability Office (GAO). (2017). *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud*. Retrieved from https://www.gao.gov/assets/690/683842.pdf

Harrell, E. (2017). *Victims of Identity Theft, 2014*. Washington, DC: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. Retrieved Jun 2019 from https://www.bjs.gov/content/pub/pdf/vit14.pdf

Harrell, E. (2019). *Victims of Identity Theft, 2016*. Washington, DC: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. Retrieved April 2019 from: https://www.bjs.gov/content/pub/pdf/vit16.pdf

Heckers, H. & O'Brien, M. (2014). *Advanced Identity Theft Responses: Financial Identity Theft*. The National Center for Victims of Crime & The Financial Industry Regulatory Authority Investor Education Foundation. Retrieved from https://victimsofcrime.org/top-links/events/2014/09/10/default-calendar/advanced-identity-theft-responses

Holtfreter, K., Reisig, M.D., & Blomberg, T.G. (2005). Consumer fraud victimization in Florida: An empirical study. *Thomas L. Rev.*, *18*, 761.

Holtfreter, K., Reisig, M. D., Mears, D. P., & Wolfe, S. E. (2014). *Financial Exploitation of the Elderl IIn A Consumer Context*. Washington, DC: US Department of Justice, Office of Justice Programs, National Institute of Justice.

Holtfreter, K., Reisig, M. D., Pratt, T. C., & Holtfreter, R. E. (2015). Risky remote purchasing and identity theft victimization among older Internet users. *Psychology, Crime & Law*, *21*(7), 681-698.

Huff, R., & Kane, J. (2010). Differentiating identity theft: An exploratory study of victims using a national victimization survey. *Journal of Criminal Justice*, (5), 1045.

Idaho Coalition Against Identity Theft. (2010a). *Identity Theft: A Training for Financial Institution Employees*. Retrieved from https://www.ovcttac.gov/downloads/identitytheftnetwork/toolkit/TrainingMaterials/TrainingForBankEmployees.pdf

Identity Theft Resource Center (ITRC). (2000). *ITRC Fact Sheet 110 Criminal Identity Theft: A Guide to The Crime*. Retrieved from https://www.idtheftcenter.org/Fact-Sheets/fs-110.html

Identity Theft Resource Center (ITRC). (2013). *Identity Theft Resource Center Predicts 2014 Identity Theft Climate for Tax Season and Beyond*. Retrieved from https://www.idtheftcenter.org/images/surveys_studies/ITRC_TAXSEASONIDTHEFT_2014.pdf

Identity Theft Resource Center (ITRC). (2017). *The Aftermath: The Non-Economic Impacts of Identity Theft*. Retrieved Jun 2019 from: https://www.idtheftcenter.org/wp-content/uploads/2018/09/ITRC_Aftermath-2018_Web_FINAL.pdf

Identity Theft Resource Center (ITRC). (2018a). *The Aftermath: The Non-Economic Impacts of Identity Theft*. San Diego, CA: Identity Theft Resource Center. Retrieved from: https://www.idtheftcenter.org/wp-content/uploads/2018/09/ITRC_Aftermath-2018_Web_FINAL.pdf

Identity Theft Resource Center (ITRC). (2018b). *Clearing Criminal Identity Theft*. Retrieved from https://www.idtheftcenter.org/knowledge-base/clearing-criminal-identity-theft/

Internal Revenue Service (IRS). (2016). *IRS's Top Ten Identity Theft Prosecutions: Criminal Investigation Continues Efforts to Halt Refund Fraud*. Retrieved from https://www.irs.gov/newsroom/irss-top-10-identity-theft-prosecutions-criminal-investigation-continues-efforts-to-halt-refund-fraud

Internal Revenue Service (IRS). (2019). *Identity Theft Victim Assistance: How It Works*. Retrieved from https://www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works

International Association of Chiefs of Police (IACP). (n.d.a). *Prevention Toolkit: Keep Your Good Name*. Retrieved from http://www.theiacp.org/portals/0/pdfs/prevention_toolkit.pdf

International Association of Chiefs of Police (IACP). (n.d.b). *Recovery Toolkit: Get Back Your Good Name.* Retrieved from http://www.theiacp.org/portals/0/pdfs/recovery_toolkit.pdf

International Association of Chiefs of Police (IACP) and Bank of America. (2008a). *Identity Crime Update: Part I.* Retrieved from http://www.theiacp.org/portals/0/pdfs/616IdentityCrimeUpdatePartI.pdf

International Association of Chiefs of Police (IACP) and Bank of America. (2008b). *Identity Crime Update: Part Ii.* Retrieved from http://www.theiacp.org/portals/0/pdfs/617IdentityCrimeUpdatePartII.pdf

Internet Crime Complaint Center. (2018). *2017 Internet Crime Report.* Retrieved Jun 2019 from https://pdf.ic3.gov/2017_IC3Report.pdf

Johnson, K. (2003). *Financial Crimes Against the Elderly.* Washington, DC: U.S. Department of Justice Office of Community Oriented Policing. Retrieved from https://ric-zai-inc.com/Publications/cops-w0768-pub.pdf

Karp, N. & Kirkman, D. (2016). *Financial Frauds and Scams Against Elders: Government Responses and Resources.* National Consumer Law Center. Retrieved from https://www.nclc.org/national-elder-rights-training-project/consumer-fraud-scams/financial-frauds-scams-against-elders.html

Lachs, M. S., & Han, S. D. (2015). Age-associated financial vulnerability: An emerging public health issue. *Annals of internal medicine*, *163*(11), 877-878.

LaCounte, C., Gray, J., & Dewees, S. (2015). *Financial Fraud in Indian Country.* Financial Crime Resource Center, National Center for Victims of Crime, & Financial Industry Regulatory Authority. Retrieved from https://victimsofcrime.org/top-links/events/2015/08/25/default-calendar/financial-fraud-in-indian-country

Lastdrager, E., Gallardo, I.C., Hartel, P., & Junger, M. (2017). *How Effective is Anti-Phishing Training for Children?* Paper presented at Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), Santa Clara, CA.

Miller, J. & Robuck, R. (2013). *Youth and Credit: Protecting the Credit of Youth in Foster Care.* Baltimore, MD: Annie E. Casey Foundation. Retrieved from http://www.aecf.org/m/resourcedoc/AECF-YouthAndCredit-2013.pdf

National Center for Victims of Crime (NCVC). (2014). *White Paper: Roundtable on Serving Victims of Elder Financial Exploitation.* Retrieved from http://victimsofcrime.org/docs/default-source/financial-fraud/final-efe-white-paper---with-participant-list.docx?sfvrsn=2

National Center for Victims of Crime. (2017). *Model Civil Provisions on Elder Financial Exploitation.* Retrieved from http://victimsofcrime.org/docs/default-source/financial-fraud/model-civil-provisions-on-elder-financial-exploitation.pdf?sfvrsn=2

National Center for Victims of Crime & Financial Industry Regulatory Authority Investor Education Foundation (NCVC and FINRA). (2013). *Taking Action: An Advocate's Guide to Assisting Victims of Financial Fraud.* Retrieved from https://www.saveandinvest.org/sites/default/files/Taking-Action-An-Advocates-Guide-to-Assisting-Victims-of-Financial-Fraud.pdf

National Center for Victims of Crime & Financial Industry Regulatory Authority (NCVC & FINRA). (n.d.a). *Taking Action: Identity Theft Victim Recovery Checklist.* Retrieved from https://victimsofcrime.org/docs/default-source/financial-fraud/recoverychecklist_idtheft.pdf?sfvrsn=4

National Center for Victims of Crime & Financial Industry Regulatory Authority Investor Education Foundation (NCVC & FINRA). (n.d.c). *Taking Action: Mass Marketing and Other Fraud- Victim Recovery Checklist.* Retrieved from https://victimsofcrime.org/docs/default-source/financial-fraud/recoverychecklist_otherfraud.pdf?sfvrsn=2

National Consumers League. (2018) *Top Scams of 2017.* Fraud!org Retrieved from https://d3n8a8pro7vhmx.cloudfront.net/ncl/pages/4567/attachments/original/1517428302/2017_top_scams_report.pdf?1517428302

National White Collar Crime Center (NWC3). (2017). *Disaster Fraud.* Retrieved from: https://www.nw3c.org/docs/research/disaster-fraud.pdf

Nerenberg, L. (2005). *Identity Theft and Related Crimes: The Critical Role of Intervention, Education and Assistance to Victims.* Outline of presentation from the NW3C's 2005 Economic Crime Summit, Minneapolis, MN.

Newman, G.R., & McNally, M.M. (2005). *Identity Theft Literature Review.* Retrieved Jun 2019 from https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf

O'brien, M., Heckers, H., Rusch, J., Coats, S., Zalenski, C., & Pedley, E. (2012). *Disaster Related Identity Theft Victimization and Fraud.* Office for Victims of Crime's National Identity Theft Victims Assistance Network. Retrieved from https://www.youtube.com/watch?v=vZRPCT-tei4"

Office for Victims of Crime (OVC). (2010). *Expanding Services to Reach Victims of Identity Theft and Financial Fraud.* Retrieved from https://www.ovc.gov/pubs/ID_theft/pfv.html

Office for Victims of Crime (OVC). (2019a). *Crime Victimization Glossary.* Retrieved from https://www.ovc.gov/library/glossary.html

Office for Victims of Crime (OVC). (2019b). *Fraud and Identity Theft.* Retrieved from https://ovc.ncjrs.gov/topic.aspx?topicid=29

Office for Victims of Crime Training and Technical Assistance Center (OVC TTAC). (2018b). *Resources for Law Enforcement.* Retrieved from https://www.ovcttac.gov/identitytheftnetwork/resource-map/resources-for-law-enforcement/

Office for Victims of Crime Training and Technical Assistance Center (OVC TTAC). (n.d.b). *Credit Card Issuer Obligations Under the Fair Credit Billing Act.* Retrieved from https://www.ovcttac.gov/downloads/identitytheftnetwork/toolkit/TrainingMaterials/FTC-GuidebookCreditCardObligations.pdf

Office for Victims of Crime Training and Technical Assistance Center (OVC TTAC). (n.d.c). *Disputing Errors in Credit Reports Using Sections 611, 623(b), and 623(a)(1)(B).* Retrieved from https://www.ovcttac.gov/downloads/identitytheftnetwork/toolkit/TrainingMaterials/FTC-GuideToAssisting-ObtrainingCopiesOfCreditReports.pdf

Office for Victims of Crime Training and Technical Assistance Center (OVC TTAC). (n.d.h). *Identity Theft Involving the Social Security Administration.* Retrieved from https://www.ovcttac.gov/downloads/identitytheftnetwork/toolkit/TrainingMaterials/FTC-GuidebookSSA.pdf

Office for Victims of Crime Training and Technical Assistance Center (OVC TTAC). (n.d.j). *The Primary Tools to Minimize Further Fraud.* Retrieved from https://www.ovcttac.gov/downloads/identitytheftnetwork/toolkit/TrainingMaterials/FTC-GuidebookPrimaryToolsForVictims.pdf

Pascual, A., Marchini, K., & Miller, S. (2018). *2018 Identity Fraud: Fraud Enters a New Era of Complexity.* Javelin Strategy & Research.

Pierce, P. (2009). *Identity Theft.* Office for Victims of Crime Training and Technical Assistance Center. Retrieved from http://www.ncdsv.org/images/OVCTTAC_IdentityTheftResourcePaper_2012.pdf

Pizor, A. (2010). *Mortgage Assistance Relief Scams: What Advocates Should Know & Updates on Regulation.* National Consumer Law Center. Retrieved from https://www.nclc.org/images/pdf/conferences_and_webinars/webinar_trainings/presentations/2010/presentation_march10.pdf

Ponemon Institute. (2013). *2013 Survey on Medical Identity Theft.* Retrieved Jun 2019 from https://www.ponemon.org/local/upload/file/2013%20Medical%20Identity%20Theft%20Report%20FINAL%2011.pdf

Rich, J. (2016a). *Combating Fraud in African-American And Latino Communities.* Federal Trade Commission. Retrieved from https://www.consumer.ftc.gov/blog/2016/06/combating-fraud-african-american-and-latino-communities

Sauer, J.H. (2005). Stealing your good name: A survey of Washington state residents 18+ on identity theft incidence and prevention. *AARP Knowledge Management, AARP Research.* Retrieved Jun 2019 from https://assets.aarp.org/rgcenter/post-import/wa_id.pdf

Sauer, J.H. (2006c). *Investor Protection: A Survey of AARP Wyoming Members.* AARP Knowledge Management, AARP Research. Retrieved Jun 2019 from https://www.aarp.org/money/investing/info-2006/wy_ipt_2006.html

Sauer, J.H., & Pak, K. (2007). Stolen futures: An AARP Washington survey of investors and victims of investment fraud. *AARP Knowledge Management, AARP Research.* Retrieved Jun 2019 from https://www.aarp.org/money/scams-fraud/info-2007/wa_fraud_07.html

Saunders, L., Pizor, A., & Twomey, T. (2009). *Desperate Homeowners: Loan Mod Scammers Step in When Loan Services Refuse to Provide Relief.* National Consumer Law Center. Retrieved from https://www.nclc.org/images/pdf/pr-reports/report-loan-mod-scams-2009.pdf

Schaffer, P., Velasquez, E., Fiorentino, N., Dwyer, K., Hamilton, A., Barney, K., Brown, D., Laluk, L., & Dwoskin, M. (2016). *Identity Theft and The Holiday Season: Understanding and Managing Risk During a Time of Increased Travel and Spending.* Generali Global Assistance and the Identity Theft Resource Center. Retrieved from https://cdn2.hubspot.net/hubfs/524149/Gated_Content/Identity%20Theft%20and%20the%20Holiday%20Season.pdf

Shadel, D., Pak, K., & Sauer, J.H. (2014). Caught in the scammer's net: Risk factors that may lead to becoming an internet fraud victim, AARP survey of American adults age 18 and older. *AARP Research.* Retrieved Jun 2019 from https://www.aarp.org/research/topics/economics/info-2014/internet-fraud-victimization-attitudes-behavior-national.html

Shoudt, E.M. (2002). Identity theft: Victims 'cry out' for reform. *American University Law Review,* (1), 339.

Silberman, S.L. (2004). AARP Minnesota identity theft survey: A study of residents 18+. *AARP Knowledge Management.* Retrieved Jun 2019 from https://assets.aarp.org/rgcenter/consume/mn_identity_theft.pdf

Stamatel, J.P., & Mastrocinque, J.M. (2011). Using national incident-based reporting system (NIBRS) data to understand financial exploitation of the elderly: A research note. *Victims and Offenders, 6*(2), 117-136.

Sussman, E. & Shoener, S. (2013). *The Use of Identity Theft by Domestic Violence Perpetrators.* Office for Victims of Crime's National Identity Theft Network. Retrieved from https://www.youtube.com/watch?v=IdGTKfAHvYc

Synovate. (2003). *Federal Trade Commission – Identity Theft Survey Report.* Retrieved Jun 2019 from https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-identity-theft-program/synovatereport.pdf

Synovate. (2007). *Federal Trade Commission – 2006 Identity Theft Survey Report.* Retrieved Jun 2019 from https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-2006-identity-theft-survey-report-prepared-commission-synovate/synovatereport.pdf

Texas Identity Theft Coalition. (2010b). *Mental Health Issues of Identity Theft Victims.* Retrieved from https://www.ovcttac.gov/downloads/identitytheftnetwork/toolkit/TrainingMaterials/TipsForProfessionalTherapists_doc.pdf

Texas Identity Theft Coalition. (2010c). *Module 2: Emotional Impact of Identity Theft*. Retrieved from https://www.ovcttac.gov/downloads/identitytheftnetwork/toolkit/TrainingMaterials/Module_2_EmotionalImpactOfIdentityTheft.pdf

Texas Identity Theft Coalition. (2010d). *Module 3: Strengthening Resilience in Identity Theft Victims*. Retrieved from https://www.ovcttac.gov/downloads/identitytheftnetwork/toolkit/TrainingMaterials/Module_3_StrengtheningResilience.pdf

Texas Identity Theft Coalition. (n.d.a). *Action Plan for Victims of Identity Theft*. Retrieved from https://www.ovcttac.gov/downloads/identitytheftnetwork/toolkit/TrainingMaterials/Module1_handout.pdf

Thorleifson, T., Anderson, K., Greenberg, S., Fisher, L., Szuchman, D., Carpenter, N., & Deem, D. (2009). *Quantifying Fraud and Under-Reported Fraud: Identifying the Fraud That Is Not Reported and Exploring Ways to Reach Vulnerable Consumers* [PowerPoint Presentation]. Retrieved from https://www.ftc.gov/sites/default/files/documents/public_events/fraud-forum/b.day1panel2.ppt

Toporoff, S., Gargano-Ahmed, A., Heckers, H., & Ayers, S. (2013). *Identity Theft and Children in The Foster Care System*. Office for Victims of Crime National Identity Theft Network. Retrieved from https://www.youtube.com/watch?v=3h4TcjFKBBM

Treasury Inspector General for Tax Administration. (2018). *Results of the 2017 Filing Season*. Washington, DC: Treasury Inspector General for Tax Administration. Retrieved from https://www.treasury.gov/tigta/auditreports/2018reports/201840012fr.pdf

Tripoli, S. & Renuart, E. (2005). *Dreams Foreclosed: The Rampant Theft of Americans' Homes Through Equity Stripping Foreclosure "Rescue Scams"*. Boston, MA: National Consumer Law Center. Retrieved from https://www.nclc.org/images/pdf/foreclosure_mortgage/scam/report-foreclosure-rescue-scams-2005.pdf

US Department of Housing and Urban Development Center for Faith-Based and Neighborhood Partnerships (HUD Center for Faith-Based and Neighborhood Partnerships). (n.d.). *Toolkit on Foreclosure Prevention & Scam Awareness for Faith-Based and Community Organizations*. Retrieved from https://www.hud.gov/sites/documents/TOOLKIT_HYPERLINKS_2.PDF

US Department of Justice (DOJ). (2014). *Civil Legal Aid 101*. Retrieved from https://www.justice.gov/atj/civil-legal-aid-101

US Department of Justice (DOJ). (2017). *Department of Justice vs. Jeffery K Skilling*. Retrieved from https://www.justice.gov/criminal-vns/case/skillingjk

US Securities and Exchange Commission (US SEC). (2013). *Affinity Fraud: How to Avoid Investment Scams That Target Groups*. Retrieved from https://www.sec.gov/investor/pubs/affinity.htm

World Privacy Forum. (2012). *Medical ID Theft: How to Recover If You're a Victim and What to Do If You Are Worried About Becoming a Victim*. Retrieved from https://www.worldprivacyforum.org/2012/04/faq-victims-of-medical-id-theft/

APPENDIX: COMMON TYPES OF IDENTITY FRAUD AND OTHER FRAUDS

Type	Definition	Source
Identity Frauds		
Criminal identity theft	An imposter gives law enforcement another person's name and personal information (such as a driver's license, date or birth, or Social Security Number (SSN)) upon arrest or during another type of interaction with law enforcement or the justice system.	Pierce 2009
Existing account fraud/ credit card fraud/account takeover	The perpetrator makes unauthorized charges to a bank, credit card, utility, phone, or other accounts.	Pierce 2009
Medical/insurance identity theft	The perpetrator uses a victim's identity or insurance to receive medical care. This can also include financial fraud. It is not the same as healthcare fraud, which is committed against organizations.	World Privacy Forum 2012; Dixon and Barrett 2013
New account fraud	An imposter uses the victim's information to open new accounts (bank, credit card, utility, phone, brokerage, loans, mortgages, etc.).	Pierce 2009
Social Security Number-related identity theft (includes tax and benefit fraud)	**Tax fraud:** Someone uses the victim's SSN to file for a tax return OR for employment. **Benefits fraud:** An individual uses the victim's SSN to get government benefits (such as food stamps, disability payments, or social security payouts).	OVC TTAC n.d.h; FTC 2017d; FTC 2018a
Synthetic identity theft	Fraud that results from using pieces of multiple people's personally identifying information to create a fake, new identity.	GAO 2017; Pierce 2009
Other Fraud, Scams, and Schemes		
Advance fee scams	Someone targets victims to make advance or upfront payments for goods, services and/or financial gains that do not materialize.	National Consumers League 2018
Affinity fraud	Affinity fraud is when someone defrauds members of a group they are—or pretend to be—a part of to gain more trust.	US SEC 2013
Buyer's Club Membership/Internet Service Fraud	Being billed for a buyer's club membership or internet service not signed up for	Anderson 2013
Charity fraud	Individuals use deception to get money from people who believe they are making donations to charities.	FTC 2018a
Credit card insurance/Credit repair fraud	**Credit Card Insurance:** Victims unnecessarily purchase insurance against the misuse of a loss or stolen credit card. **Credit card repair:** Victims pay someone who has promised to remove negative, but accurate, information from their credit report or who has promised to help them create a new credit record without the negative information.	FTC 2005

Type	Definition	Source
Disaster/home-repair fraud	Fraudsters take advantage of needs following a natural disaster, such as contractors collecting money to repair damaged property without completing the project or creating false disaster-related charities.	Breuer 2011; NW3C 2017
Imposter scams	Someone contacts a victim and pretends to be a family member in distress or government figure that requires money.	FTC 2014e
Job scams/business fraud	**Job scams:** Someone promises victims help finding a job for a fee but does not provide this service. **Business Fraud:** Victims purchase a business opportunity but do not earn even half as much as promised or do not receive promised assistance.	FTC 2005
Foreclosure scams /mortgage scams/ loan scams	**Loan modification scams** occur when an individual requests up-front payment to negotiate with the victim's loan servicer but does not. **Loan audits** involve an individual claiming to review the victim's loan documents for a fee, under the pretense that it could help them avoid an impeding foreclosure. **Short sales scams** involve a false claim that the individual can convince a mortgage servicer to sell the victim's house for less than amount due on the loan. **Sale leasebacks** involve someone tricking a victim into giving up the deed to their home and becoming a renter instead of an owner. **Foreclosure rescue scams** involve advertisements to property-owners at risk of losing their homes but result in the individual owning the property instead or the victim being foreclosed on.	Saunders, Pizor, and Twomey 2009; Pizor 2010; Tripoli et al. 2005
Investment fraud	Individuals use deceptive messaging to convince victims to invest in false or poor investments.	NCVC and FINRA 2013
Merchandising scams	These scams (including weight-loss product scams) involve the victim purchasing products that they do not receive or are of extremely low quality.	National Consumers League 2018; FTC 2005
Ponzi/pyramid schemes	**Pyramid schemes:** Individuals promise victims profits based solely on recruiting others to invest too, without real profits from any real investment or product. **Ponzi schemes:** The individual convinces victims to pay into fictitious business and pays initial investors with investments of new investors.	FTC 2019b
Phishing scams	Individual convince victims to provide their personally identifying information through online or emailed falsifications of actual websites.	FTC 2018a
Prize scams/sweepstakes scams / lottery scams	Individuals send notices to victims claiming they won a prize or lottery but must submit a small fee to claim the winnings.	National Consumers League 2018
Romance scams	Individuals typically use a fake persona to persuade a victim to have romantic feelings for them and then ask for money.	FTC 2005