Crime Science

SYSTEMATIC REVIEW Open Access

Identity fraud victimization: a critical review of the literature of the past two decades

Yasemin Irvin-Erickson[1*]

Abstract

This study aims to provide an understanding of the nature, extent, and quality of the research evidence on identity fraud victimization in the US. Specifically, this article reviews, summarizes, and comments on the state of empirical research of identity fraud victimization in the US based on a narrative review of 52 published empirical studies. Studies included in this review suggest that the prevalence of identity fraud in the US has increased over the years and existing account frauds is the most prevalent type of identity fraud. There is a pressing need for more research on the prevalence of identity fraud victimization among minors, institutionalized individuals, and individuals from minority groups; long-term prevalence of identity fraud victimization; and emerging forms of identity fraud such as synthetic identity fraud victimization. Studies included in this review further suggest that identity fraud risk factors vary based on the fraud type considered. Identity fraud victims can experience a variety of harms. Longitudinal studies following identity fraud victims are essential for reliably estimating the risk factors for identity fraud victimization and the impact of identity fraud victimization on individual victims. The research on services for identity fraud victims is limited and suggests the positive impact of trauma-informed services for serious identity fraud victims. The overwhelming lack of research on the impact of programs and services for identity fraud victims necessitates more attention from scholars to study the impact of programs, interventions, and services for identity fraud victims on reporting of victimization, prevention of victimization, experiences of victims, and victim-centered cost benefit analysis of services. Policy and practice implications of these findings are discussed.

Keywords Identity theft, Identity fraud, Review, Victim

Background

Identity theft and associated frauds have increasingly attracted public attention in the United States (US) with highly publicized data breaches and millions becoming victims of this crime every year. Efforts to educate the public about identity theft have raised attention to the risks of identity theft and fraud, however, an in-depth exploration of identity fraud victimization is needed to further the field's and the public's understanding of this crime.

Despite the comparatively scant evidence on identity theft in the field of criminology, the research on identity theft in the US has started picking up speed in the past decade with the availability of nationally representative data on this topic through the Bureau of Justice Statistics'(BJS) National Crime Victimization Survey Identity Theft Supplement (NCVS-ITS). The NCVS is the US's primary data source on victimization since 1972. The NCVS is administered to non-institutionalized individuals who are 12 years old or older from a nationally representative sample of households in the US. The ITS is a supplemental survey to the NCVS which is administered to the respondents to the NCVS survey who are 16 years old or older. The ITS was first implemented in

*Correspondence:
Yasemin Irvin-Erickson
YIrviner@gmu.edu
[1] George Mason University, 354 Enterprise Hall, 4400 University Drive, MS 4F4, Fairfax, VA 22030, USA

2008 and gets fielded approximately every two years. This leading national level data source on identity theft victimization asks respondents if they had been victims of different forms of identity theft in the past 12 months and beyond the past year and the characteristics and consequences of victimization and help-seeking behavior if respondents indicate they had been victims of identity theft.

There has been a few review studies on the state of the US literature on identity theft through funding by the Department of Justice offices. For instance, the first literature on identity theft by Newman and McNally (2005) funded by the National Institute of Justice explored what is known about identity theft and the knowledge gaps based on their review of publications of different organizations, complaint data, less than 10 surveys conducted by different organizations, and a handful of research studies published at the time of that review. Another review study by Irvin-Erickson and Ricks (2019) funded by the Office for Victims of Crime examined the state of the literature on fraud victimization based on research evidence from academic and non-academic sources and practice evidence sources (such as fact sheets, podcasts, and other sources that are not traditionally considered in reviews) published between 2000 and 2018. This study expands upon the aforementioned reviews by considering not only the scope of the literature on identity theft victimization published in the past two decades but also the quality of conduct of these studies to provide a broad yet nuanced understanding of the state of the literature on this topic and the knowledge gaps. Although the aforementioned reviews provided invaluable information about the opportunity structure, risks, and consequences of identity theft victimization and the needs of identity theft victims, similar to other traditional narrative reviews of the literature in the grey literature, these reviews did not include risk of bias and quality assessments of the sources of evidence included in these reviews. The current study fills this critical knowledge gap in our understanding of the state of the literature on identity fraud victimization through consideration of the risk of bias and the quality of each study included in this review.

Despite the increase in the number of studies on the topic of identity theft victimization over the past decade, the evidence base on identity theft victimization is still limited. Accordingly, this review did not follow the format of a systematic review and instead followed steps similar to a scoping review to gain an understanding of the nature, extent, and quality of the research evidence on identity fraud victimization. Specifically, this review aimed to answer the following questions to present the size, scope, and quality of the emerging evidence base on identity fraud victimization:

1) What are the trends in the US literature on identity fraud victimization?
2) What do we know from the US literature on identity fraud victimization?

    a. What are the topics most and least commonly studied in the literature on identity fraud victimization?
    b. What are the risks of bias associated with existing studies?
    c. What do studies with lower risk of bias and/or higher quality demonstrate about key concepts studied by these studies?

3) What are the knowledge gaps in the US literature on identity fraud victimization?

By answering these questions, this review primarily aims to provide suggestions for future research on identity fraud victimization including potential research questions for future systematic reviews as the evidence base on this topic becomes denser at which point researchers can conduct larger knowledge syntheses. Accordingly, although risk of bias and quality of studies are assessed for each study included in this review, a meta-analysis or statistical pooling of studies has not been performed.

Definitional issues regarding identity theft

There is an increased interest in the field to differentiate between the terms of identity theft and identity fraud because not all identity theft incidents involve a fraudulent act at the time of theft of personal information. Javelin Strategy and Research (2021) defines identity theft as “unauthorized access of personal information” and identity fraud as identity theft incidents in which there is an element of financial gain. The Federal Trade Commission (FTC) and the BJS define identity theft as “fraud that is committed or attempted using a person’s identifying information without authority” (FTC, 2004; Harrell, 2019, p. 18). The acts considered by the BJS under this definition include unauthorized use or attempted use of an existing account, unauthorized use or attempted use of personal information to open a new account, and misuse or attempted misuse of personal information for a fraudulent purpose (Harrell, 2019).

Researchers differentiated between three stages of identity theft: acquisition of personal information, use of personal information for illegal financial or other gain, and discovery of identity theft (Newman & McNally, 2007). Personal information can be acquired through different means ranging from simple physical theft to more complex and even legal ways such as scams, cyber, or mechanical means and purchasing the information from data brokers. The acquired personal information is used for financial gain or other criminal purposes (Newman & McNally, 2007). However, fraudulent use of information might not happen at the time of acquiring of information and once personal information is exposed, a person can become an identity theft victim multiple times.

Another important stage of identity theft is the discovery of theft of personal information and associated frauds because the longer the discovery period is the less likely it is for victims to contact law enforcement (Randa & Reyns, 2020) and the more likely it is for them to experience aggravated consequences (Synovate, 2007). Police reports are critical for victims to pursue an identity theft case (OVC, 2010). For victims of certain forms of identity theft, the discovery of victimization can take as long as 6 months or more (Synovate, 2003, 2007). In cases where personal information is exposed due to data breaches, victims might have greatly varying experiences of when and what they learn about this exposure (if at all) and the services available to them. Currently, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have laws requiring businesses, and in most states, government organizations to notify individuals of security breaches involving personal information (National Conference of State Legislatures, 2022). However, the decisions of organizations on whom to notify (such as the victims, the FTC, or law enforcement), when to notify, and how to notify can drastically vary from one geography to another based on laws. Two groups can become targets of identity fraud: individuals whose personal information is stolen and organizations which are in care of the stolen personal information or which become targets of fraud. Law enforcement might be more likely to put emphasis on organizations as visible and collective targets of identity theft (Newman & McNally, 2005).

In recognition of the stages and targets of identity theft, there has been an interest in the field to differentiate between the terms of identity theft and identity fraud. In popular knowledge, the terms "identity theft" and "identity fraud" have been used interchangeably considering the interrelated nature of acts considered under these terms. However, it is acknowledged that these terms legally refer to different things (Newman & McNally, 2005).

In statute, identity theft was legally defined at the federal level with the Federal Identity Theft and Assumption Deterrence Act (ITADA) of 1998 (Newman & McNally, 2005). ITADA made it a federal offense to "knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law" (the Identity Theft Act; U.S. Public Law 105-318). Prior to this legal definition of identity theft in the US, the terms "identity theft" and "identity fraud" were used to primarily distinguish between the individual victims and collective victims with the former being referred to as victims of identity theft and the latter as victims of identity fraud (McNally & Newman, 2008). In later years, these terms have been used to differentiate between the act of unlawful acquisition of identity information and the fraudulent use of personal information.

Over the years, different research and practice sources have generally considered the following acts under identity theft and identity fraud: criminal identity theft in which individuals use others' personal information during interactions with law enforcement or for committing other crimes (Button et al., 2014); existing account frauds where an individual makes unauthorized charges to existing accounts such as bank, credit card, and other existing accounts; medical/insurance identity theft in which an individual fraudulently uses somebody else's personal information to receive medical care; new account frauds in which an individual's personal information is used unlawfully to open a new account; social security number (SSN) related frauds in which an individual uses the victim's SSN to file for a tax return, for employment, or to receive government benefits; and synthetic identity theft in which different pieces of real and fake identity information are combined together to create an identity and to commit frauds (Dixon & Barrett, 2013; FTC, 2017, 2018; GAO, 2017; Pierce, 2009).

The opportunity structure for identity theft

Earlier research on perpetrators of identity theft, using a conceptual framework informed by Cornish and Clarke's (1986) *Rational Choice Theory* and the methodology of crime script analysis, has focused on the motivations and methods of committing identity frauds (see Copes & Vieraitis, 2009, 2012) and the impact of experiences of perpetrators' on their criminal involvement and criminal event decisions (Vieraitis et al., 2015). Regarding the organizational level of identity frauds, research has shown that perpetrators of identity theft and fraud might range from individuals to street-level and more advanced criminal organizations (Copes & Vieraitis, 2009, 2012; Newman & McNally, 2007). Although earlier research has shown that perpetrators of identity theft used low-technology methods (Copes & Vieraitis, 2009, 2012), perpetrators of identity theft have started using more complex schemes and relying more heavily on the internet to acquire identity information over the years (Pascual et al., 2018).

The number of identity fraud victims who know the perpetrators has decreased over the years. For instance, in 2008, about 40% of identity fraud victims knew how the incident happened, and from those, about 30% believed that their information was stolen during a purchase or other interaction and 20% believed that their personal information was stolen from their wallet, 14% believed the information was stolen from files at an office, and another 8% believed that the information was stolen by friends or family (Langton & Planty, 2010). In 2012, about 32% of identity victims in the US knew how their personal information was stolen and 9% knew the identity of the perpetrator (Harrell & Langton, 2013). Comparatively, in 2018, 25% of identity fraud victims knew how the offender obtained the information and 6% of victims knew something about the perpetrator (Harrell, 2021). This unknown status of how the information is obtained or who the perpetrator is sometimes interpreted as the technology-facilitated nature of the acquisition of information (Newman & McNally, 2005). However, victims of instrumental identity theft in which an individual's information is stolen to commit other frauds and crimes, and individuals who have been victims of multiple types of identity theft in the recent past, are more likely to know how their information was stolen and the perpetrator (Harrell, 2019). New research examining the impact of the pandemic on identity fraud further suggest an increase in identity fraud scams and loan fraud in which perpetrators directly target consumers and a significant portion of victims of identity fraud scams and loan fraud (about 3 in every 4 victims) knowing their perpetrators (Buzzard & Kitten, 2021).

The most frequent way identity theft victims become known to authorities in the US is complaints to financial institutions (Harrell, 2021). The other ways victims report their victimization include complaints to federal institutions [such as the FTC and the Internet Crimes Complaint Center (IC3)] and non-governmental organizations [such as the Identity Theft Resource Center (ITRC) and the National Consumers League (NCL)] and crime reports to law enforcement.

In the past decade, federal and non-profit organizations increased their efforts to educate consumers on risks and reporting of identity theft and how to deal with the ramifications of fraud victimization. Several federal and other organizations provide information for services victims can receive such as reporting and assistance hotlines, civil and criminal legal services, and trauma informed counseling. Other available responses to identity theft include credit and identity theft monitoring, identity theft insurance, and identity theft restoration; however, these responses are typically provided by for-profit companies. Depending on who the victim contacts, victims might not be uniformly informed about all options available to them. Many victim service providers working in organizations funded by the Victims of Crime Act do not have the resources to recognize and respond to fraud's harms (OVC, 2010). Furthermore, even when services are available, there might be significant barriers against victims' access to these resources including financial barriers. Currently, majority of services available to identity theft victims are geared towards handling out-of-pocket expenses.

At the time of this review, there was a fast evolving opportunity structure for identity theft and identity fraud due to the hardships inflicted on individuals by the economic and health crises. Direct stimulus payments, increased loan applications, and the overall increase in online activities during the pandemic have provided increased opportunities for identity frauds such as account takeovers (Tedder & Buzzard, 2020) and identity frauds in relation to scams (Buzzard & Kitten, 2021). Furthermore, low-income individuals, older individuals, individuals who depend on others for their care, and individuals who might not have control over their finances can experience aggravated harms as a result of identity fraud victimization. Furthermore, some victims might experience a significant damage to their reputations (Button et al., 2014). All of these conditions necessitate more scientific inquiry and a better understanding of existing research evidence base on identity fraud.

Scope of review

This review focuses only on identity fraud victimization and excludes studies that focus on theft of personal information but not the fraud aspect of identity theft. As an example, although skimming, intentional data breaches, and mail theft are acts of identity theft, if a research study focused solely on these acts but not the fraud aspect, that study was excluded from the review. The review further excluded research on identity frauds targeting organizations and governments, harms of identity fraud to businesses and institutions, and research studies focusing on victims in countries other than the US. The review also excluded sources in which no data collection and analysis was attempted, paid research content, and research summaries with limited or no information about methodology.

The current review included empirical research studies that focus on identity fraud victimization in the US which were published in English and between January 2000 and November 2021. The resources that were reviewed included journal articles, PhD dissertations, government reports, and other reports found in major social science research databases and on websites of organizations focusing on identity theft. This review adopted a broad definition of "empirical" research focusing on studies using both quantitative and qualitative data analysis methods including descriptive analysis.

In this review, a comprehensive search strategy was used to search the literature for relevant studies. The search strategy was consisted of (1) a formal search of academic databases using search strings based on Boolean operators[1] and (2) an informal search of grey literature using keyword searches and searches on the websites of organizations focusing on identity fraud. Searches were conducted in the following academic databases: Proquest Social Sciences Collection, Web of Science Social Sciences Citation Index, Wiley Online, JSTOR, Criminal Justice Abstracts, SocIndex Full text, and Violence and Abuse Abstracts. Additional searches were completed on the websites of the BJS, the Internet Crime Complaint Center (IC3), the FTC, the ITRC, Javelin, the National White Collar Crime Center (NW3C), and the Ponemon Institute.

299 potential studies were identified through database searches (excluding duplicate records) and 37 publicly available empirical studies were identified from websites of leading organizations on identity fraud. Ultimately, 29 sources from these database searches and 23 sources from the aforementioned organizations met the inclusion criteria for this review (see Appendix 1 for the screening process). These included articles are denoted with an asterisk (*) in the references section.

Appraisal of quality of studies

Studies included in this review were appraised for methodological quality. Quality appraisal was conducted after deeming a study eligible for the review based on the inclusion criteria specified earlier. Appendix 2 and Appendix 3 show the two quality appraisal tools that were adapted from Hoy et al. (2012) and Mays and Pope (2020). Each quantitative study was assigned into one of three categories based on the evaluation of risk of study bias: low, moderate, or high risk of bias. Each qualitative study was assigned into one of three categories based on the evaluation of quality: low, medium, or high quality. For the only mixed-method study in this review, risk of bias and study quality were evaluated separately for qualitative and quantitative elements of the study. More information about quality rating process and quality ratings of studies can be found in Appendix 4 and notes on bias and quality assessments for included studies can be found in Appendix 5.

Trends of identity fraud victimization research

Of the 52 studies included in this review, the majority were NGO reports (n = 22) followed by journal articles (n = 18), government reports (n = 7), and PhD dissertations (n = 5). Almost all of the white papers from government organizations and NGOs (n = 28) were descriptive quantitative studies. All of the white papers included in this review (n = 29) were based on survey data. Of the 23 academic studies (i.e., journal articles and dissertations) included in the review, 19 quantitative studies used surveys and 4 qualitative studies used interviews or focus groups discussions as their data source. Among these 23 academic studies, the primary data analysis method was regression analysis (n = 15) followed by descriptive quantitative data analysis (incidence, correlation, ANOVA analyses (n = 4), narrative analysis (n = 3), and phenomenological analysis (n = 1). Only one quantitative study included in this review used a quasi-experimental design with propensity score matching, and none of the quantitative studies included in the review had random assignment. The earliest journal article included in this review was published in 2006 and half of the journal articles included in this review (n = 9) were published between 2019 and 2021 (n = 9).

The studies in this review thematically fell into one or more of the following four areas of identity fraud victimization research: (1) prevalence, incidence, and reporting, (2) risk factors, (3) harms, and (4) prevention, programs, and services. From the 52 studies included in this review, 31 focused on harms, 22 focused on prevalence, incidence, and reporting, and 15 focused on risk factors. Notably, only 3 studies included in this review focused on services for identity fraud victims and among these studies there were no experiments with random assignment focusing on the effectiveness of specific programs or interventions for identity fraud victims (see Table 1 for subtopics and citations of identity fraud studies included in this review).

Prevalence, incidence, and reporting of identity fraud victimization

A significant number of studies included in this review (n = 22) focused on the extent and reporting of identity fraud victimization, however the majority of these publications (n = 13) were evaluated to have a high risk of bias.

[1] The following search string was used in all databases with the exception of JSTOR: ("identity theft" OR "identity fraud" OR "social security fraud" OR "credit card fraud" OR "account fraud" OR "internet fraud" OR "cyber fraud") AND (victim*). For JSTOR database the following truncated search string was used due to word limitations: ("identity theft" OR "identity fraud") AND (victim*). These search strings were applied to the title or abstracts of the sources included in these databases.

Table 1 Subtopics of Identity Fraud Studies with Citations

1. Prevalence, incidence, and reporting of identity fraud victimization	Binette (2004); Burton (2008); Dinger and Sauer (2006); Golladay (2017); Gray (2010); Harrell (2017, 2019, 2021); Harrell and Langton (2013); Langton and Planty (2010); Marcum et al. (2016); Navarro and Higgins (2017); Ponemon Institute (2011, 2012, 2013, 2015); Reyns and Randa (2017); Sauer (2005, 2010); Silberman (2004); Synovate (2003, 2007)
2. Risk factors of identity fraud victimization	Anderson (2006); Betz (2012); Burnes et al. (2020); Copes et al. (2010); Cornelius (2016); Harrell (2017, 2019, 2021); Harrell and Langton (2013); Holtfreter et al. (2015); Kpaduwa (2010); Langton and Planty (2010); Navarro and Higgins (2017); Ponemon Institute (2011); Reyns et al. (2019)
3. Harms and consequences of identity fraud victimization	Betz (2012); DeLiema et al. (2021); Golladay and Holtfreter (2017); Green et al. (2020); Harrell (2019, 20212017); Harrell and Langton (2013); Langton and Planty (2010); Li et al. (2019); ITRC (2003, 2005, 2007, 2008, 2009, 2010, 2014, 2015, 2017, 2018a, 2018b, 2021); Ponemon Institute (2011, 2012, 2013, 2015); Pryor (2009); Randa and Reyns (2020); Reynolds (2020); Synovate (2003, 2007)
4. Prevention, programs, and services	Gies et al. (2021); Green et al., (2020, 2021)

Nine of the 22 publications in this area which were evaluated to have lower risk of bias (i.e., low or moderate risk of bias), were based on nationally representative surveys by the BJS and the FTC.

Prevalence, incidence, and types of identity fraud victimization

National estimates

Seven lower bias studies included in this review uniformly demonstrated that the incidence and prevalence of identity fraud victimization have increased between early 2000s and 2018, and misuse or attempted misuse of an existing account has been the most common type of identity fraud victimization over the years (Harrell, 2017, 2019, 2021; Harrell & Langton, 2013; Langton & Planty, 2010; Synovate, 2003, 2007).

The FTC, the first organization that collected national survey data on identity fraud based on phone surveys of US adults aged 18 and older in 2003 and 2006 estimated that approximately 10 million, or 4% of US adults, experienced identity fraud in the year preceding data collection (Synovate, 2003, 2007). As indicated earlier, BJS has been collecting individual-level data on identity fraud since 2008. The 2008 iteration of the NCVS-ITS was significantly different than the later iterations of the NCVS-ITS conducted in 2012, 2014, 2016, and 2018. Results from the 2008 NCVS-ITS are not comparable to the results from the subsequent surveys. One important limitation of the NCVS-ITS is that it does not include individuals younger than 16 and individuals living in institutional and transient settings in its sample (Harrell, 2021). Another limitation of the NCVS-ITS is that although it was designed to distinguish between victims of attempted identity fraud and victims of successful frauds, the 2008 NCVS survey couldn't successfully distinguish between the two (Langton & Planty, 2010). Accordingly, reports based on the NCVC-ITS fielded between 2008 and 2018 do not provide disaggregated statistics on these two groups.

The 2008 NCVS-ITS, despite being different than the 2003 and 2006 surveys of the FTC with regards to its shortest prevalence and the age interval of its study participants, similarly found that 11.7 million, or 5% of all persons aged 16 or older in the US, have been victims of at least one type of identity fraud in the two years preceding the survey (Langton & Planty, 2010). Later iterations of the NCVS-ITS highlighted a significant increase in the share of identity theft victims among persons aged 16 and older, especially after 2015. While the 2012 and 2014 NCVS-ITS estimated that approximately 7% of all persons aged 16 or older in the US had been victims of identity fraud in the past year (Harrell, 2017; Harrell & Langton, 2013), the 2016 and 2018 iterations of the NCVS-ITS estimated that approximately 10% and 9% of persons aged 16 or older in the US had been victims of at least one form of identity fraud in the past 12 months, respectively (Harrell, 2019, 2021).

In the FTC and the BJS identity theft surveys, three main subcategories of identity fraud are captured: existing account frauds, new account frauds, and use of personal information to commit other frauds. The FTC and the BJS surveys over the years have showed that existing credit card frauds are the most prevalent form of identity fraud victimization (Harrell, 2017; Harrell & Langton, 2013; Langton & Planty, 2010; Synovate, 2003, 2007). Notably, neither the FTC nor the BJS surveys captured synthetic identity frauds.

In the FTC and the BJS surveys, more detailed forms of identity frauds are captured under the main subcategories of existing account, new account, and other frauds.

The FTC reports included in this review provided estimates on identity theft victims who had been affected by these detailed identity fraud categories (see Synovate, 2003, 2007). For instance, according to the 2006 FTC identity theft survey, fraudulent use of credit cards (existing account frauds), opening of new credit cards (new account frauds), and use of personal information to commit other crimes (other frauds) were the most frequently experienced detailed fraud types under the three broad subcategories of identity fraud (Synovate, 2007). Although the NCVS-ITS also collects data on detailed forms of frauds under these three categories, neither the BJS reports nor the academic studies in this review based on the NCVS-ITS provided disaggregated information on detailed categories of identity fraud considered under "new account" and "other fraud" categories. However, publications based on the NCVS-ITS showed that, existing credit card frauds is the most prevalent existing account fraud subcategory followed by bank account and other existing account frauds (Harrell, 2017, 2019; Harrell & Langton, 2013; Langton & Planty, 2010).

Currently, surveys from the Ponemon Institute, which were classified to have high risk of bias, provide the most in-depth insights into medical identity fraud. In Ponemon surveys, medical identity fraud is defined as the use of an individual's personal identity to fraudulently receive medical service or prescription drugs and goods, including attempts to commit fraudulent billing (Ponemon Institute, 2011). The number of US adult individuals who experienced medical identity fraud at some point in time increased from 1.49 million in 2011 to 2.32 million in 2014 (Ponemon Institute, 2011, 2012, 2013, 2015). Lastly, another study with high bias risk by Navarro and Higgins (2017) found that among victims of familial identity fraud (identity frauds committed by family members), the most frequent type of identity fraud experienced was misuse of personal information for instrumental frauds such as government benefit frauds.

Although there is a recall bias associated with using cross-sectional surveys to capture distant past experiences, data from the FTC and the BJS surveys also provide important information about individuals' exposure to multiple forms of identity theft and their repeat victimization. In 2003, the FTC estimated the 5-year prevalence rate of identity fraud victimization among US adults to be 12.7% (Synovate, 2003). In 2012 and 2014, the NCVS-ITS estimated that about 14% of individuals aged 16 and older experienced at least one incident of identity fraud in their lifetime (Harrell, 2017; Harrell & Langton, 2013). Analyses based on the two most recent iterations of the NCVS-ITS further show that nearly 1 in 5 persons aged 16 and older experienced identity fraud in their lifetime (Harrell, 2019, 2021).

Data from the NCVS-ITS further show that number of identity fraud victims who experienced multiple types of identity fraud victimization in a single incident decreased between 2016 and 2018 and majority of multiple identity fraud victims in a given year experienced fraudulent use of a combination of existing accounts (Harrell, 2017, 2019, 2021; Harrell & Langton, 2013; Langton & Planty, 2010). According to the 2008 NCVS-ITS, about 18% identity fraud victims experienced multiple types of identity fraud during their most recent victimization in the past year. Studies based on the 2012, 2014, 2016 iterations of the NCVS-ITS estimated that approximately 8% of victims experienced multiple types of identity fraud during a single incident (Harrell, 2017, 2019; Harrell & Langton, 2013). According to the 2018 NCVS-ITS, only 6% of the identity fraud victims experienced multiple identity victimization in the past year (Harrell, 2021).

Subnational estimates

Publications by the AARP included in this review, which were evaluated to have a high risk of bias due to several design issues (see Appendix 5), showed that 15% to 30% of individuals who participated in the AARP surveys in Colorado, Minnesota, Montana, Oklahoma, Washington, and West Virginia have been victims of identity fraud or knew someone who has been victim of identity fraud in the past 5 years (see Binette, 2004; Burton, 2008; Dinger, 2006; Sauer, 2005, 2010; Silberman, 2004).

Discovery of identity fraud victimization

Although majority of identity fraud victims discover their victimization quickly, some victims, and especially victims of new account frauds and other frauds, might be more likely to have a long discovery period (Synovate, 2003, 2007). FTC surveys estimated that for 33% to 40% of all identity fraud victims, it took less than one week to discover that their personal information was misused (Synovate, 2003, 2007). The same surveys further found that the discovery period was the quickest for victims of existing account frauds; and, victims of new account and other frauds were the least likely to discover their victimization within one week (Synovate, 2003, 2007). Furthermore, for 24% to 27% of new account and other fraud victims, it took them 6 months or more to discover their victimization as opposed to less than 5% for existing credit card and other existing account victims (Synovate, 2003, 2007). In parallel with these findings, the 2014

Ponemon medical identity fraud study found that most victims of medical identity fraud did not learn about their victimization until 3 months after the incident (Ponemon Institute, 2015). Surveys by the BJS over the years have consistently shown that the most common way identity fraud victims discover their victimization was through contact from a financial institution for victims of existing account frauds and contact from a non-financial institution for other types of identity fraud (Harrell, 2017, 2019, 2021; Harrell & Langton, 2013).

Reporting of identity fraud victimization

The studies included in this review demonstrated that there is a considerable risk of underreporting of identity fraud victimization to authorities (especially to law enforcement) and to organizations which can provide the necessary information and services to handle the aftermath of victimization.

Looking at studies from early 2000s, the 2003 and 2006 FTC surveys show that, 38% of identity fraud victims did not report their victimization to any organization. In both surveys, 43% of the victims reported their victimization to the company that issued an existing credit card/account or the company that issued the new account and close to 75% of survey participants did not report their victimization to law enforcement (Synovate, 2003, 2007). According to the 2008 NCVS-ITS, the majority of victims (68%) contacted a credit bureau or a bank to report their victimization. The 2008 NCVS-ITS estimated the reporting of identity fraud victimization to law enforcement at 17% (Langton & Planty, 2010), which is lower than the FTC surveys' estimates of 25% in 2003 and 2006 (Synovate, 2003, 2007). The later iterations of the NCVS-ITS confirmed the findings from earlier surveys by showing that not only identity fraud is underreported to law enforcement but reporting of identity fraud to law enforcement decreased significantly after 2008 with less than 10% of victims reporting their most recent victimization to law enforcement in 2012, 2014, 2016, and 2018 (Harrell, 2017, 2019, 2021; Harrell & Langton, 2013). However, the same NCVS-ITS surveys also showed an uptick in reporting of identity fraud to non-law enforcement agencies. According to the 2012, 2014, 2016, and 2018 NCVS-ITS surveys, about 9 in 10 identity fraud victims reported their victimization to a non-law enforcement agency (Harrell, 2017, 2019, 2021; Harrell & Langton, 2013) with credit card companies and banks being the most frequently contacted organizations and non-law enforcement victim service organizations being the least contacted organizations by the victims.

BJS reports based on all 5 iterations of NCVS-ITS further suggest that victims of existing account frauds are less likely than victims of new account frauds and other frauds to report their victimization to law enforcement (Harrell, 2017, 2019, 2021; Harrell & Langton, 2013; Langton & Planty, 2010). The most common reason for victims to not report their victimization to law enforcement was victims handling the incident in a different way such as reporting their victimization to another non-law enforcement agency (Harrell, 2017, 2019, 2021; Harrell & Langton, 2013; Langton & Planty, 2010). Other reasons for victims to not report their victimization to law enforcement include victims not suffering any monetary loss; victims thinking law enforcement cannot help them; victims thinking their victimization is not important enough; victims not knowing they can report their identity fraud victimization to police; victims being embarrassed, afraid, or burdened to report their victimization; and perpetrator being a family member or an acquaintance (Harrell, 2017, 2019, 2021; Harrell & Langton, 2013; Langton & Planty, 2010). The 2014 Ponemon Institute study similarly found that victims of comparatively more serious identity fraud cases are more likely to contact law enforcement. Ponemon surveys found reasons similar to those identified by the NCVS-ITS for victims not reporting their victimization to legal authorities (Ponemon Institute, 2012, 2013, 2015).

Two academic studies by Golladay (2017) and Reyns and Randa (2017), both based on the 2012 iteration of the NCVS-ITS, provide additional insight into reporting of identity frauds. According to Golladay (2017), higher income victims are more likely to report their victimization to a credit card company or financial institution whereas people of color, individuals who know the perpetrator, and individuals who did not have prior identity fraud victimization or who had a lower number of identity fraud victimization experiences in the past year were more likely to contact law enforcement. The Golladay (2017) finding on the positive relationship between knowing the offender and the likelihood of contacting organizations is surprising considering, the descriptive analysis of the NCVS-ITS suggest that individuals knowing the offender is a reason for not contacting law enforcement (Harrell & Langton, 2013). This discrepancy might be due to the increasingly technological nature of identity fraud cases where victims who know anything about the offender contacting the police or the omission of some variables in relation to the severity of identity fraud (such as discovery time or time spent trying to resolve issues in relation to victimization) from the regression models.

According to the same study (Golladay, 2017), people of color (in comparison to individuals who identify as White), individuals who knew the perpetrator (in comparison to people who did not know), individuals with a higher monetary loss as a result of their victimization, and victims who experienced a higher number of identity frauds in the past year were more likely to report their victimization to a credit bureau.

Another study by Reyns and Randa (2017) compared the factors affecting reporting of victimization among victims of credit card fraud, bank fraud, any existing account fraud, and new accounts fraud. According to this study, seriousness of the offense (which the authors describe as incidents in which victims experienced more emotional distress and had more out of pocket losses and perpetrators obtained more money) appears as the only common factor affecting the decision to report victimization to law enforcement among all identity frauds considered. Other factors such as knowing how the personal information was obtained and a shorter time period between the fraud incident and the discovery of victimization were associated with increased odds of contacting law enforcement for credit card and bank fraud victims. According to the same study (Reyns & Randa, 2017), reporting the incident to a non-law enforcement agency was associated with increased odds of contacting law enforcement among victims of existing account frauds, however a sub-analysis of reporting patterns among bank fraud and credit card fraud victims showed that, while bank fraud victims who contacted other agencies were more likely to contact law enforcement, victims of credit card fraud who contacted other agencies were not as likely to contact law enforcement. This study further showed that income and sex were significant predictors of reporting when subcategories of identity fraud were considered. Victims of credit card fraud with higher incomes and female victims of new account frauds were less likely to report their victimization to law enforcement.

Other academic studies, which were evaluated to have a high risk of bias, provide additional insight into reporting behavior of identity fraud victims. A study by Gray (2010) found that individuals who knew which law enforcement agency to contact for reporting identity fraud were most likely to contact law enforcement (Gray, 2010). Another online survey of school counselors by Marcum et al. (2016) found that counselors who are White, who have a higher level of education, and who work in urban school settings were less likely than their counterparts to complete an incident report about identity fraud victimization reported by students.

Risk factors for identity fraud victimization

From the 52 publications included in this review, 15 focused on risk factors of identity fraud victimization. According to the evaluation of risk of bias among these 15 studies, 6 were classified to have a low risk of bias; 3 to have a moderate risk of bias and 6 to have a high risk of bias. The 9 studies with low and moderate risk of bias ratings suggest several individual-level risk factors for identity fraud victimization. Among these studies, demographic factors were the most commonly studied individual-level predictors of identity fraud victimization. The biggest takeaway from these studies is that predictors of identity fraud victimization vary significantly based on the identity fraud victimization type considered.

Among all demographic factors studied, the findings from different studies on the relationship between age, income, and identity fraud risk were in most agreement. In the broader victimology literature, victims and especially victims of violent crime have been shown to be younger (Turanovic & Pratt, 2019). The studies included in this review generally suggest that victims of identity fraud are older than victims of other crimes. However, as indicated in the earlier section, minors under the age of 16 who might be at increased risk of identity fraud victimization due to their clean credit histories and lack of control over their finances (FTC, 2011), have not been included in identity fraud data collection efforts in the studies that were reviewed. Accordingly, this exclusion should be taken into consideration in the comparison of age patterns among identity fraud victims and victims of other crimes. Although victims of existing bank account frauds tend to be slightly younger than victims of existing credit card frauds and new account frauds, overall, lower bias studies included in this review show that the victims of existing account frauds and new account frauds tend to be in older age categories (35–64 years of age) (see Anderson, 2006; Burnes et al., 2020; Copes et al., 2010; Harrell & Langton, 2013; Harrell, 2017, 2019, 2021; Langton & Planty, 2010). Another important finding from lower bias studies included in this review was that identity fraud victimization risk decreases after age 65 and individuals who are aged 75 and older have a lower risk of identity fraud victimization in comparison to other age groups (Anderson, 2006; Harrell & Langton, 2013).

High income was another common predictor of identity fraud among the majority of studies included in this review. Several lower bias studies not only showed that among all identity fraud victims, individuals with a household income of $75,000 or more are more likely to be an identity fraud in the general victim population (Anderson, 2006; Harrell, 2017, 2019, 2021; Langton

& Planty, 2010; Reyns, 2013) but this pattern also holds for the subcategory of existing credit card/bank account fraud (Burnes et al., 2020, 2017, 2019). One exception to this finding was a study by Copes et al. (2010), which was evaluated to have a moderate level of bias, which showed that although the typical identity fraud victim earned $50,000 to $75,000, victims of non-credit card identity frauds were majority low-income individuals.

The relationship between racial/ethnic minority status and identity fraud victimization risk was another commonly studied topic. Based on the lower bias studies included in this review, the evidence on this relationship was mixed. Findings from the most recent studies based on the NCVS-ITS demonstrate the clear need for differentiating between credit card frauds and other types of identity frauds for exploring the nature of this relationship. A study by Anderson (2006) based on a regression analysis of data from the 2003 FTC survey showed that, when all identity fraud types are taken into consideration, individuals who identity themselves in the "Other" race/ethnicity group, which included individuals who do not identify as African American/Black, Asian, Hispanic, or non-Hispanic White, were more likely to become victims of identity fraud in comparison to individuals who identify with these racial/ethnic categories. On the other hand, later descriptive analyses based on NCVS-ITS showed that non-Hispanic White individuals were more likely to be victims of identity fraud in the general victim population and this pattern also held true for victims of existing credit card fraud (Burnes et al., 2020; Harrell, 2017, 2019, 2021; Harrell & Langton, 2013; Langton & Planty, 2010). Some of the lower bias studies included in this review showed that there were no differences between different racial/ethnic categories in their risk of experiencing existing bank account frauds (Harrell, 2017; Harrell & Langton, 2013), new account frauds, and other frauds (Burnes et al., 2020). One notable exception to this finding was results from the Copes et al. (2010) study which showed that victims of non-credit card frauds were more likely to be Black.

Similar to the relationship between racial/ethnic identity and victimization risk, the evidence on the relationship between sex and identity fraud victimization risk was mixed. While some of the lower bias studies included in this review suggested that there was no significant relationship between an individual's sex and their identity fraud victimization risk (even when different subcategories of identity fraud were considered; see Burnes et al., 2020; Harrell, 2019; Harrell & Langton, 2013; Langton & Planty, 2010), other studies found that females have a higher victimization risk in general (Anderson, 2006; Copes, 2010; Harrell, 2021) and especially for non-credit card frauds (Anderson, 2006; Copes, 2010).

Lower bias studies included in this review further showed that other less commonly studied demographic factors such as education, marital status, number of children in the household, and number of adults in the household can be related to risk of identity fraud. While earlier studies found no relationship between marital status and identity fraud risk (Anderson, 2006; Copes, 2010), a recent regression study by Burnes et al. (2020), which was based on the 2012 and 2014 iterations of the NCVS-ITS, found that married people were more likely to be victims of instrumental identity frauds. The same study (2020) further showed that individuals who have attended at least some college degree have a higher likelihood of becoming a victim of an existing or new account fraud. The study by Copes (2010) also found that individuals with more than a high school education were more likely to become identity fraud victims. Although far less commonly studied, a higher number of children in the household (three or more) and having only one adult in the household were also found to be associated with a higher identity fraud victimization risk (see Anderson, 2006).

Burnes et al. (2020) further showed that individuals who experience multiple instances of identity fraud in a short amount of time and individuals who chronically experience identity fraud victimization are more likely to experience identity fraud victimization later. Repeat victimization is a particularly understudied topic within the literature on identity fraud and has important implications considering stolen personally information can be used over the years and the conditions that enable victimization in the first place can predict further victimization.

Lastly, a few of the lower bias studies included in this review examined the relationship between individuals' protective behavior, routine online activities, and self-control and their risk of identity fraud victimization. For instance, Copes et al.'s (2010) study found that victims of identity fraud did not engage in any more risky behavior than non-victims and spent about the same time online as average Americans. Other more recent studies on the other hand found a significant relationship between lifestyles, routine activities, self-control and identity fraud victimization. For instance, Holtfreter et al. (2015) conducted a phone survey with individuals aged 60 and older living in Arizona and Florida and found that individuals who have a lower level of self-control were more likely to engage in risky online purchases and subsequently more likely to become identity fraud victims. Burnes et al. (2020) further found that some protective behaviors employed by individuals such as changing online passwords and shredding and destroying documents reduced the risk of identity fraud victimization.

Other studies that were evaluated to have a higher risk of bias also provided support for the findings discussed above and provided additional insights into predictors of identity fraud victimization. However, the findings from these studies should be considered carefully considering each study's limitations (see Appendix 5). For instance, a study by Cornelius (2016) based on an online survey found that the higher an internet user's knowledge of phishing risks, the higher likelihood that the user was victimized by online theft. In another study, Holt and Turner (2012) administered a survey to students, faculty, and staff at a university and found that females and individuals who update their protective computer software were more resilient against identity fraud. Kpaduwa (2010) conducted a survey with university students and found no significant correlation between students' knowledge of identity fraud and their risk of identity fraud victimization. Another study by Navarro and Higgins (2017) found that victims of familial identity theft, younger victims, and repeat victims of identity fraud were more likely to experience non-account identity frauds. Ponemon Institute (2011) provided further support for the findings from lower bias studies by showing that victims of medical identity fraud tend to be older. Lastly, in another college sample, Reyns et al. (2019) found that the time spent sending e-mailing was positively correlated with identity fraud victimization risk.

Harms and consequences of identity fraud victimization

From the 52 publications included in this review, 31 focused on harms of identity fraud victimization. Studies based on the NCVS-ITS once again provide the most robust evidence on both economic and non-economic harms of identity fraud.

Economic consequences of identity fraud victimization

The studies included in this review focused on both direct costs of identity fraud for victims, which can include out-of-pocket and reimbursed losses to the victim and indirect costs such as monetary costs associated with dealing with the aftermath of the victimization experience (such as legal costs, bounced checks, and other expenses), lost wages, difficulty finding jobs, being denied loans, and damaged credit scores. The lower bias quantitative studies included in this review based on national samples revealed the following main findings: (1) the majority of identity fraud victimizations result in direct financial loss; (2) the initial money lost does not always result in out of pocket loss; (3) certain demographic factors might predict the likelihood of experiencing out of pocket losses; (4) the indirect and direct loss amount differs by the type of identity fraud victimization; and (5) victims whose personal information is used for other fraudulent purposes are most likely to experience direct and indirect losses, credit related problems, and other financial problems (Green et al., 2020; Harrell, 2017, 2019, 2021; Harrell & Langton, 2013; Langton & Planty, 2010; Reynolds, 2020; Synovate, 2003, 2007).

For instance, the most recent statistics based on the 2018 iteration of the NCVS-ITS show that 68% of victims experienced a direct loss of $1 or more as a result of their most recent victimization (with a median loss of $200) but from these victims only 12% experienced an out of pocket loss of $1 or more (with a median out of pocket loss of $100) (Harrell, 2021, p. 9). According to the same survey, among all victims, only 5% experienced an indirect loss that was $1 or more (with a median loss of $30) (Harrell, 2021, p. 10). The same survey further showed that victims of existing account frauds were least likely to experience direct and indirect costs whereas individuals whose personal information was stolen for other fraudulent purposes were most likely to experience direct and indirect costs (Harrell, 2021). Another important trend is that victims who have a long discovery time had more severe economic consequences. For instance, the 2006 FTC survey found that while 30% of victims who discovered that their personal information was being misused 6 months or more after the incident spent $1000 or more to handle the aftermath of their victimization, only 10% of those who found the misuse within 6 months spent $1000 or more.

A recent study by Reynolds (2020) further found a relationship between economic costs and demographics. Individuals with lower income and educational attainment and unmarried individuals are at higher risk of experiencing out of pocket losses as a result of their identity fraud victimization. Another study by DeLiema et al. (2021) based on the 2014 and 2016 iterations of the NCVS-ITS also found that, among older adults, individuals who live at or below the federal poverty level were most likely to experience out of pocket losses.

Other high bias studies included in this review provide further support for the lower bias studies included in the review. For instance, studies by the Ponemon Institute found that medical identity fraud victims can experience distinct indirect costs such as increased insurance premiums and lost medical coverage (Ponemon Institute, 2011, 2012, 2013, 2015). ITRC surveys further showcased the aggravated economic harms experienced by victims of comparatively more serious cases of identity fraud (i.e., non-account frauds) (see ITRC, 2003, 2005, 2007, 2008, 2009, 2010, 2014, 2015, 2017, 2018a, 2018b, 2021).

Non-economic consequences of identity fraud victimization

The lower bias studies included in this review which are based on national surveys showed that a significant number of identity fraud victims (estimates ranging from 80 to 90%) experience some level of distress as a result of their victimization. Victims of new account frauds and other frauds (in comparison to victims of existing account frauds), victims of multiple types of identity fraud (in comparison to victims of one type of identity fraud), and victims who spend a longer time resolving problems associated with their victimization are much more likely to experience severe distress as a consequence of their victimization (Harrell, 2017, 2019; Harrell & Langton, 2013; Langton & Planty, 2010). National studies further suggest that a small group of identity fraud victims might experience physical problems, legal problems, and problems with family, friends, work, and school in relation to their identity fraud victimization (Langton & Planty, 2010; Harrell, 2017, 2019, 2021; Harrell & Langton, 2013; Reyns & Randa, 2020).

Looking deeper into the time burden aspect of identity fraud, national studies over the years revealed that, unsurprisingly, victims who discovered their victimization later spent a longer amount of time resolving the ramifications of their victimization (Synovate, 2003). These surveys further estimated that between 25 and 50% of victims resolved any issues experienced as a result of their victimization within 1 day of discovering they were victims (Harrell 2017, 2019, 2021; Harrell & Langton, 2013; Synovate, 2007) but for a smaller group of victims (less than 10% of the victims) resolving issues took 6 months or more (Harrell 2017, 2019, 2021; Harrell & Langton, 2013). National surveys also showed that new account and other fraud victims spent a longer amount of time resolving their problems in the aftermath of their victimization in comparison to victims of existing account frauds (Harrell 2017, 2019, 2021; Harrell & Langton, 2013; Synovate, 2007). According to the 2006 FTC survey, the top 10% and 5% of victims spent more than 100 h and 1000 h respectively to resolve their problems (Synovate, 2007).

Other lower bias regression studies and higher quality qualitative studies included in this review support these descriptive findings from national surveys and further suggest other individual and situation-specific factors that can predict who is more likely to experience these negative outcomes (Betz, 2012; Golladay & Holtfreter, 2017; Pryor, 2009; Randa & Reyns, 2020). For instance, a qualitative study based on in-depth interviews with identity fraud victims showed that individuals who experienced identity fraud as a minor but discovered the victimization as an adult can experience negative emotional consequences and these consequences might be aggravated if the victims do not have support from law enforcement and their families (Betz, 2012). Another study by Golladay & Holtfreter based on the 2012 NCVS-ITS suggested that individuals who have prior victimization experiences and individuals who are not White might be more likely to experience a higher level of negative emotional consequences. Another low bias study by Randa and Reyns (2020) found that while being older, being a female, spending more time resolving the ramifications of victimization, and higher amount of net loss as a result of victimization were all correlated with higher distress level; being married and having a higher education level were correlated with less distress reporting. The authors (2020) similarly found that while the net monetary loss and the time to clear the incident were positively correlated with the level of negative physical outcomes experienced by the victims; education level and being married were negatively correlated with the level of negative physical outcomes.

Green et al. (2020) conducted qualitative analyses based on data from interviews with 16 individuals who contacted the ITRC after experiencing a serious identity fraud victimization (defined by authors as victims who experienced identity frauds other than existing credit card fraud and who contacted the ITRC). According to this study, among victims of serious identity fraud, victims of criminal identity fraud (and especially identity frauds involving government-based services) had the most complicated and time-consuming cases with the most substantial indirect economic and legal consequences and the majority of victims of serious identity frauds attempted to investigate their own cases (despite being discouraged to do so). The study further showed that victims who strictly follow the best practices to document in detail their interactions and conversations with others during the remediation process, experienced a significant time burden and had a hard time in managing their daily routines. This study suggested that the experiences of victims of serious identity frauds trying to prove their situations to legal authorities is similar to those of survivors of sexual assault (Green et al., 2020).

Other studies that were rated to have a high risk of bias due to issues with the sampling frame and size, nonresponse rate, and missing data nevertheless provided strong support for the findings on the negative emotional and physical outcomes, legal problems, time burden, and other problems faced by the victims in the aftermath of their victimization (see ITRC, 2005, 2007, 2008, 2009, 2010, 2014, 2015, 2017, 2018a, 2018b, 2021; Li et al., 2019; Ponemon Institute, 2011, 2012, 2013, 2015).

Prevention, programs, and services

From the 52 studies included in this review, prevention of victimization and programs and services for victims was the least researched topic. Notably, all of the three articles included in the review under this topic were published between 2020 and 2021 and by the same group of authors.

One of these studies by Green et al. (2020), which was rated to have a moderate risk of bias, found that victims of serious identity fraud, despite the increasingly online nature of this crime, still use internet search engines as the main method to learn about remediation options. The authors further found that victims of serious identity fraud who expressed a higher level of satisfaction with services provided to them were individuals who had a representative from an organization whom they felt was a partner in their pursuit of recovery from their victimization.

Another study by Green et al. (2021), which was rated to have medium quality, explored the needs of identity fraud victims from the viewpoint of a diverse group of professionals providing services for identity fraud victims. An important finding from this study was that organizations serving identity fraud victims are not equipped to respond to the long-term needs of victims of synthetic identity fraud in which perpetrators generally combine real and fake identity information to create new identities and victims do not become aware of victimization for years. The study findings further suggested that the field need to better understand the relationship between data breaches and subsequent identity fraud victimization to better educate and provide services to individual victims based on the nature of the stolen personal information.

Another quantitative study by Gies et al. (2021) examined the effect of using services provided by the ITRC on experiences of serious identity fraud victims (defined by authors as victims of any identity fraud other than misuse of existing credit card). The authors combined data from the ITRC's 2017 Aftermath Survey and the 2016 NCVS-ITS to compare experiences of three groups of victims of serious identity frauds that have been matched on key demographic variables: (1) respondents to the NCVS-ITS who did not report their victimization to any entity (*no report*), (2) respondents to the NCVS-ITS who reported their victimization to one or more entities and received standard services from these entities (*treatment as usual*), and (3) individuals who contacted the ITRC and received specialized services which involves receiving caring and compassionate advice from specially trained (trauma-informed) employees of the ITRC including a continuity of care upon request of the victim (*ITRC treatment*).

First, this study showed that individuals who contacted the ITRC had a longer time period between the victimization incident and the discovery of victimization and spent a longer amount of time resolving the incident. Accordingly, it is reasonable to argue that although the groups were matched on key variables, individuals in the *ITRC treatment* group had comparatively more serious cases of identity fraud victimization. The study found significant differences between the three groups regarding the key outcomes measured. The respondents in the *ITRC treatment* group reported significantly more general problems, financial problems, employment/educational problems, family/friend problems, and physical health problems and more money loss in comparison to the individuals in the *no report* and *treatment as usual* groups. This finding is not surprising considering the victims in the *ITRC treatment* group had a longer discovery time and spent more time dealing with the ramifications of their victimization. However, surprisingly, the victims in the *ITRC treatment group* reported fewer health problems as a result of their victimization experience than the individuals in the *no report* and *treatment as usual* groups. This finding provides support for the model of services provided by ITRC (i.e., the trauma-informed focus of these services and the continuity of care in the long term if requested by the victims). However, these findings should be interpreted carefully considering some limitations of this study (see Appendix 5 for a detailed description) including the cross-sectional nature of data collection on which this quasi-experimental study was based on.

Discussion

For this study, 52 studies were reviewed for their results on different aspects of identity fraud victimization. So, what does this emerging literature on identity fraud tell us about identity fraud victimization and what we can do as researchers and practitioners to narrow the gaps in the existing literature and to better identify, reach, and serve victims and to prevent victimization?

Cross-sectional national data collection efforts show that the incidence and prevalence of identity fraud victimization increased over the years and the misuse of an existing account is the most common type of identity fraud victimization. However, national identity fraud surveys likely underestimate the number of victims due to underreporting, the discovery period of identity frauds, and exclusion of certain groups and from survey samples. There is a pressing need for further analysis of existing data and collection and analysis of new data to explore the following: (1) the prevalence of identity fraud victimization among minors, individuals in institutional settings, and individuals in transient living settings; (2) long-term prevalence of identity fraud victimization; (3) prevalence of victimization to detailed subcategories of new account and instrumental frauds; (4) disaggregated analysis of prevalence of attempted and successful identity frauds; (5) subnational trends in identity fraud victimization; and (6) prevalence of synthetic identity fraud victimization.

The reluctance of victims to report identity frauds in general, and to law enforcement and victim service organizations in particular, suggest a pressing need to educate the public, the law enforcement, and victim service providers about stages of identity theft, forms of identity theft, and seriousness of this crime. As discussed earlier identity theft and identity fraud are two terms that are used interchangeably although acquiring of information precedes the fraudulent acts committed with the acquired information and theft of information does not have a monetary harm (Gies et al., 2021). The lack of distinguishing between these two stages of identity theft and not knowing about different forms of identity theft might result in individuals not fully understanding the potential long-term harms of exposure of their personal information.

Furthermore, in addition to public's reluctance to report identity fraud victimization to law enforcement; the often cross-jurisdictional nature of identity theft and fraud, the interrelatedness of identity theft with other crimes, the lack of knowledge about the perpetrator, and the frequent handling and investigation of financial frauds by financial agencies make it hard for law enforcement agencies to identify and record identity theft and even disincentivize them to handle identity theft cases (Newman & McNally, 2005). The reluctance of victims to report their victimization and the reluctance of law enforcement to respond the cases of identity theft can: reduce victims' access to criminal justice processes, affect investigation and prosecution of these crimes, increase victims' sense of helplessness, and reduce victims' chances of accessing critical information and resources to prevent victimization and revictimization and recover from the aftermath of their victimization. Accordingly, there is a need for individuals, law enforcement, victim service providers, and policymakers to put as much emphasis on the acquisition of personal information as the subsequent frauds (Gies et al., 2021) and to better understand the nature of this crime including stages, types, victims, perpetrators, and consequences of identity theft and the evolving opportunity structure for identity theft.

The research evidence on the lower likelihood of identity fraud reporting among individuals who had negative interactions with law enforcement further suggest that there is a need for making it easier for victims to report their victimization, increasing public outreach to encourage reporting, commitment of leadership to a victim-centered approach, training of police officers on the nature of identity theft and fraud and different forms of identity fraud. However, similar to the experiences of victim service providers, budget limitations can prohibit local law enforcement from putting in place organizational inputs (such as establishing an identity theft unit, having victim advocates, and providing continuous training) to ensure these outcomes. Collaboration between federal and local law enforcement organizations in training of officers and increasing state funding for police departments to have cybercrime and identity theft units and employ identity theft analysts and investigators can lift some of these barriers. There is also a need to better educate the employees of banks and financial institutions about the nature of identity theft and to use this communication between identity theft victims and these organizations as an opportunity to direct victims to government and nonprofit organizations specialized in helping identity theft and identity fraud victims.

Studies on risk factors of identity fraud victimization further show that risk factors for victimization vary by identity fraud types. Studies in this review further showed that people of color, individuals from lower socio-economic backgrounds, individuals with chronic identity fraud victimization experiences, and individuals with multiple identity fraud victimizations at a short amount of time in the near past might be more likely to experience more serious forms of identity fraud and might be at heightened risk of experiencing aggravated harms. However, these studies exclude critical groups and do not provide information about the risk factors for detailed subcategories of identity fraud such as various subcategories of instrumental frauds. The research on protective behavior of individuals against identity fraud is not conclusive and is not able to temporally differentiate the impact of protective behaviors on identity fraud victimization due to the cross-sectional design of studies. Longitudinal studies of protective behavior and more detailed data collection and analysis on risk factors for victimization can provide critical insight for public education about risk factors and targeting of this information through different means to groups at risk.

Longitudinal studies following identity fraud victims are also essential for reliably estimating the true impact of identity fraud victimization on victims and the effectiveness of services and programs offered to identity fraud victims. There is also a need to better distinguish the impacts of identity fraud victimization for detailed categories of identity fraud.

The overwhelming evidence on the differential impact of identity fraud for victims of different identity frauds and victims of different circumstances reiterate the importance of recognizing that not every identity fraud is the same and not every identity fraud victim will experience severe trauma and other negative consequences. Considering the limited funding and resources for victims of crime in general, and victims of identity frauds in particular, better identification of victims who are in need of extended services and triage of services and resources between different organizations are essential to provide holistic and long-term services to victims who are at highest risk to experience chronic victimization and aggravated harms as a result of their victimization.

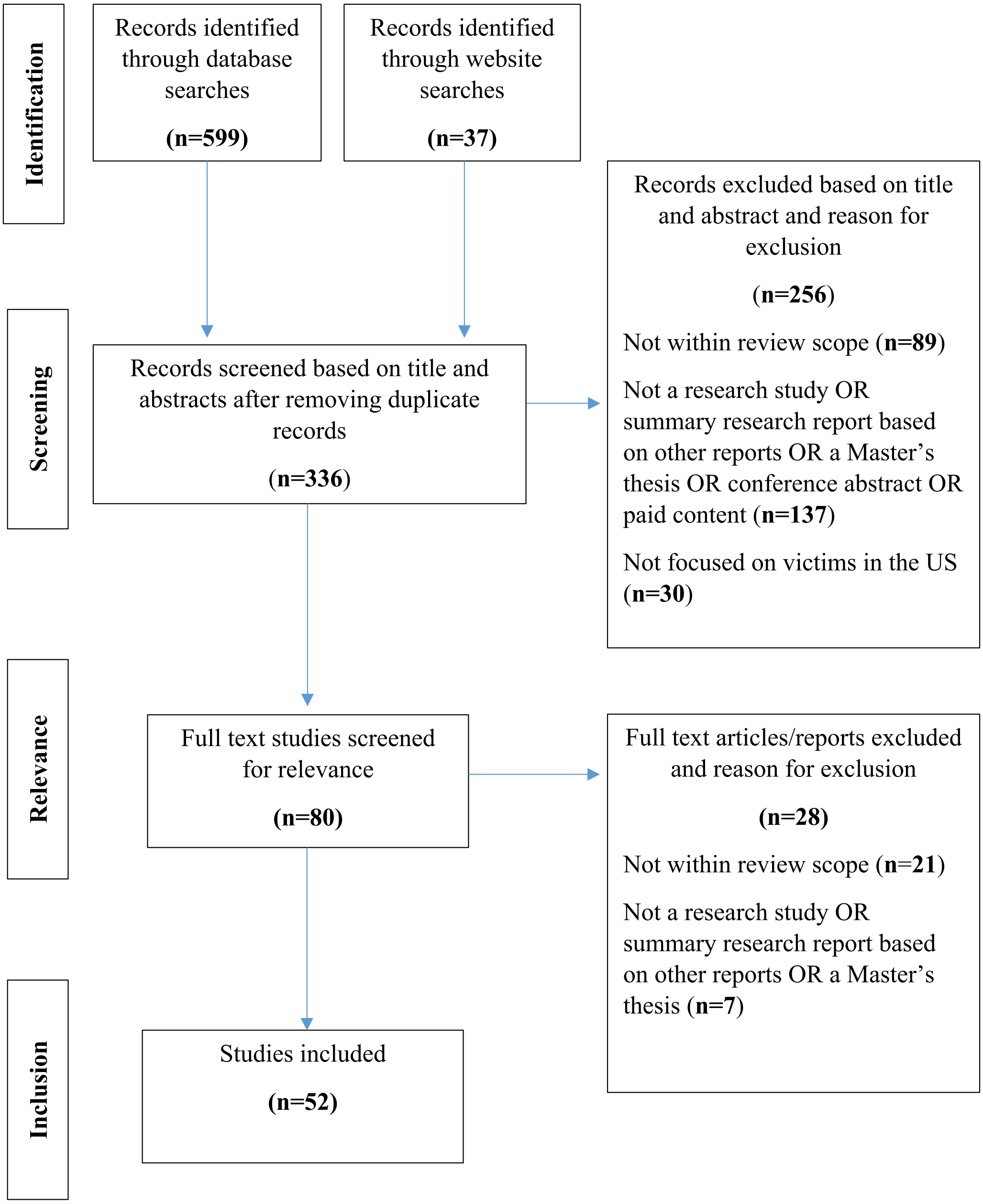
The overwhelming lack of research on the impact of programs and services for identity fraud victims necessitates more attention from scholars and practitioners to study the impact of programs, interventions, and services for identity fraud victims on reporting of victimization, prevention of victimization, experiences of victims, and victim-centered cost benefit analysis of services. The empirical evidence on the more positive outcomes experienced by victims of identity fraud who have a meaningful and satisfactory experience with victim service professionals and who are receiving specialized services suggest the promising potential of trauma informed services and continuity of services for a specific group of victims experiencing more serious forms of identity frauds. However, more research is needed to identify which characteristics and components of specialized services that are more likely to produce positive outcomes for identity fraud victims.

Although phishing and vishing (i.e., voice phishing) has not been included in the scope of this review, another emerging important topic in relation to the understanding individuals' vulnerability to identity fraud and other types of frauds is the use of artificial intelligence (AI) in fraudulent activities. Recently, the ITRC (2019) reported the first case of the use of artificial intelligence in AI-related fraud in which AI was used to impersonate the head of a German company to successfully request money from the CEO of the UK branch of the company.

Lastly, although this review focused on individual victims of identity fraud, and not organizational victims, considering the increasing number of data breaches; greater preventative efforts are required at the organizational level to secure operations, to fix vulnerabilities, and to better notify involved parties (FTC, 2022). Establishment of uniform data security and data breach notification standards across the US and federal enforcement of these standards can simultaneously reduce identity theft and identity fraud risk by targeting both collective and individual targets of identity theft.

Appendix 1

Flow chart diagram of search results and identification of studies


Identification
Records identified through database searches
(n=599)
Records identified through website searches
(n=37)
Screening
Records screened based on title and abstracts after removing duplicate records
(n=336)
Records excluded based on title and abstract and reason for exclusion
(n=256)
Not within review scope (n=89)
Not a research study OR summary research report based on other reports OR a Master's thesis OR conference abstract OR paid content (n=137)
Not focused on victims in the US (n=30)
Relevance
Full text studies screened for relevance
(n=80)
Full text articles/reports excluded and reason for exclusion
(n=28)
Not within review scope (n=21)
Not a research study OR summary research report based on other reports OR a Master's thesis (n=7)
Inclusion
Studies included
(n=52)

Appendix 2

Hoy et al. (2012) risk of bias tool

Note: If there is insufficient information in the article to permit a judgment for a particular item, please answer No (HIGH RISK) for that particular item.

Risk of bias item	Criteria for answers
External validity	
1. Was the study's target population a close representation of the national population in relation to relevant variables?	• Yes (LOW RISK): The study's target population was a close representation of the national population • No (HIGH RISK): The study's target population was clearly NOT representative of the national population
2. Was the sampling frame a true or close representation of the target population?	• Yes (LOW RISK): The sampling frame was a true or close representation of the target population • No (HIGH RISK): The sampling frame was NOT a true or close representation of the target population
3. Was some form of random selection used to select the sample, OR, was a census undertaken?	• Yes (LOW RISK): A census was undertaken, OR, some form of random selection was used to select the sample (e.g., simple random sampling, stratified random sampling, cluster sampling, systematic sampling) • No (HIGH RISK): A census was NOT undertaken, AND some form of random selection was NOT used to select the sample
4. Was the likelihood of non-response bias minimal?	• Yes (LOW RISK): The response rate for the study was >/=75%, OR, an analysis was performed that showed no significant difference in relevant demographic characteristics between responders and nonresponders • No (HIGH RISK): The response rate was <75%, and if any analysis comparing responders and non-responders was done, it showed a significant difference in relevant demographic characteristics between responders and non-responders
Internal validity	
5. Were data collected directly from the subjects (as opposed to a proxy)?	• Yes (LOW RISK): All data were collected directly from the subjects • No (HIGH RISK): In some instances, data were collected from a proxy
6. Was an acceptable case definition used in the study?*	• Yes (LOW RISK): An acceptable case definition was used • No (HIGH RISK): An acceptable case definition was NOT used
7. Was the study instrument that measured the parameter of interest shown to have reliability and validity (if necessary)?	• Yes (LOW RISK): The study instrument had been shown to have reliability and validity (if this was necessary), e.g., test–retest, piloting, validation in a previous study, etc • No (HIGH RISK): The study instrument had NOT been shown to have reliability or validity (if this was necessary)
8. Was the same mode of data collection used for all subjects?	• Yes (LOW RISK): The same mode of data collection was used for all subjects • No (HIGH RISK): The same mode of data collection was NOT used for all subjects
9. Was the length of the shortest prevalence period for the parameter of interest appropriate?*	• Yes (LOW RISK): The shortest prevalence period for the parameter of interest was appropriate (e.g., point prevalence, one-week prevalence, one-year prevalence) • No (HIGH RISK): The shortest prevalence period for the parameter of interest was not appropriate (e.g., lifetime prevalence)
10. Were the numerator(s) and denominator(s) for the parameter of interest appropriate?*	• Yes (LOW RISK): The paper presented appropriate numerator(s) AND denominator(s) for the parameter of interest • No (HIGH RISK): The paper did present numerator(s) AND denominator(s) for the parameter of interest but one or more of these were inappropriate
11. Summary item on the overall risk of study bias	• LOW RISK OF BIAS: Further research is very unlikely to change our confidence in the estimate • MODERATE RISK OF BIAS: Further research is likely to have an important impact on our confidence in the estimate and may change the estimate • HIGH RISK OF BIAS: Further research is very likely to have an important impact on our confidence in the estimate and is likely to change the estimate

*All descriptive quantitative studies were evaluated based on items 1–5, 7(if necessary), and 8. Items 6, 9, and 10 were only used to assess the risk of bias within prevalence studies

Appendix 3

Mays and Pope (2020) framework for assessing quality of qualitative studies

Features/processes of the study	Appraisal questions	Quality indicators (i.e., possible features of the study for consideration)
Findings	1. How credible are the findings?	Findings are supported by data/study evidence Findings 'make sense'; i.e., have a coherent logic Findings are resonant with other knowledge Corroborating evidence is used to support or refine findings (other data sources or other research evidence)
Findings	2. How has knowledge or understanding been extended by the research?	Literature review summarizing previous knowledge and key issues raised by previous research Aims and design related to existing knowledge, but identify new areas for investigation Credible, clear discussion of how findings have contributed to knowledge and might be applied to policy, practice, or theory development Findings presented in a way that offers new insights or alternative ways of thinking Limitations of evidence discussed and what remains unknown or unclear
Findings	3. How well does the study address its original aims and purpose?	Clear statement of aims and objectives, including reasons for any changes Findings clearly linked to purposes of the study Summary/conclusions related to aims Discussion of limitations of study in meeting aims
Findings	4. How well is the scope for making wider inferences explained?	Discussion of what can be generalized to the wider population from which the sample was drawn or cases selected Detailed description of the contexts in which the data were collected to allow assessment of applicability to other settings Discussion of how propositions/findings may relate to wider theory and consideration of rival explanations Evidence supplied to support claims for wider inference Discussion of limitations on drawing wider inferences
Design	5. How defensible is the research design?	Discussion of how the overall research strategy was designed to meet the aims of the study Discussion of rationale for study design Convincing argument for specific features/components Use of different features and data sources evidence in findings presented Discussion of limitations of design and their implications for evidence produced
Sample	6. How well defended is the sample design or target selection of cases/documents?	Description of study locations, and how and why chosen Description of population of interest and how sample selection relates to it Rationale for selection of target sample, settings or documents Discussion of how sample/selections allowed necessary comparisons to be made

Features/processes of the study	Appraisal questions	Quality indicators (i.e., possible features of the study for consideration)
Sample	7. How well is the eventual sample composition/case inclusion described?	Detailed description of achieved sample/cases covered Efforts taken to maximize inclusion of all groups Discussion of any missing coverage in achieved samples/cases and implications for study evidence Documentation of reasons for non-participation among sample approached or cases selected Discussion of access and methods of approach, and how these might have affected coverage
Data collection	8. How well were the data collected?	Discussion of who collected the data; procedures and documents used; checks on origin, status, and authorship of documents Audio- or video-recording of interviews, focus groups, discussions, etc. (if not, were justifiable reasons given?) Description of conventions for taking field notes Description of how fieldwork methods may have influenced data collected Demonstration, through portrayal and use of data. that depth, detail, and richness were achieved in collection
Analysis	9. How well has the analysis been conveyed?	Description of form of original data (e.g., transcripts, observations, notes, documents, etc.) Clear rationale for choice of data management method, tools, or software package Evidence of how descriptive analytic categories, classes, labels, etc. were generated and used Discussion, with examples, of how any constructed analytic concepts, typologies, etc. were devised and used
Analysis	10. How well are the contexts of data sources retained and portrayed?	Description of background, history and socioeconomic/organizational characteristics of study sites/settings Participants’ perspectives/observations are placed in personal context (e.g., use of case studies, vignettes, etc. are annotated with details of contributors) Explanation of origins of written documents Use of data management methods that preserve context (i.e., facilitate within case analysis)
Analysis	11. How well has diversity of perspectives and content been explored?	Discussion of contribution of sample design/case selection to generating diversity Description of diversity/multiple perspectives/alternative positions in the evidence displayed Evidence of attention to negative cases, outliers or exceptions (deviant cases) Typologies/models of variation derived and discussed Examination of reasons for opposing or differing positions Identification of patterns of association/linkages with divergent positions/groups

Features/processes of the study	Appraisal questions	Quality indicators (i.e., possible features of the study for consideration)
Analysis	12. How well has detail, depth and complexity (i.e., richness) of the data been conveyed?	Use and exploration of contributors' terms, concepts and meanings Portrayal of subtlety/intricacy within data Discussion of explicit and implicit explanations Detection of underlying factors/influences Identification of patterns of association/conceptual linkages within data Presentation of illuminating textual extracts/observations
Reporting	13. How clear are the links between data, interpretation and conclusions?	Clear conceptual links between analytic commentary and presentation of original data (i.e. commentary relates to data cited) Discussion of how/why a particular interpretation is assigned to specific aspects of data, with illustrative extracts to support this Discussion of how explanations, theories, and conclusions were derived; how they relate to interpretations and content of original data; and whether alternative explanations were explored Display of negative cases and how they lie outside main propositions/theory; or how propositions/theory revised to include them
Reporting	14. How clear and coherent is the reporting?	Demonstrates link to aims/questions of study Provides a narrative or clearly constructed thematic account Has structure and signposting that usefully guide reader Provides accessible information for target audiences Key messages are highlighted or summarized
Reflexivity and neutrality	15. How clear are the assumptions, theoretical perspectives and values that have shaped the research and its reporting?	Discussion/evidence of main assumptions, hypotheses and theories on which study was based and how these affected each stage of the study Discussion/evidence of ideological perspectives, values, and philosophy of the researchers and how these affected methods and substance of the study Evidence of openness to new/alternative ways of viewing subject, theories, or assumptions Discussion of how error or bias may have arisen at each stage of the research, and how this threat was addressed, if at all Reflections on impact of researcher(s) on research process
Ethics	16. What evidence is there of attention to ethical issues?	Evidence of thoughtfulness/sensitivity to research contexts and participants Documentation of how research was presented in study settings and to participants Documentation of consent procedures and information provided to participants Discussion of how anonymity of participants/sources was protected, if appropriate or feasible Discussion of any measures to offer information, advice, support, etc. after the study where participation exposed need for these Discussion of potential harm or difficulty caused by participation and how avoided

Features/processes of the study	Appraisal questions	Quality indicators (i.e., possible features of the study for consideration)
Auditability	17. How adequately has the research process been documented?	Discussion of strengths and weaknesses of data sources and methods Documentation of changes made to design and reasons; implications for study coverage Documents and reasons for changes in sample coverage, data collection, analysis, etc. and implications Reproduction of main study documents (e.g., interview guides, data management frameworks, letters of invitation)

Appendix 4

Quality/risk of bias evaluations and ratings for included studies

Evaluation of quantitative studies

This review adopted criteria from Hoy et al.'s (2012) risk of bias evaluation tool (see Appendix 2) to evaluate the risk of bias within quantitative studies. Hoy et al.'s (2012) risk of study bias assessment, similar to the GRADE approach, does not include a numerical rating but rather evaluates the overall risk of bias based on assessment of risk of bias of individual risk items (Hoy et al., 2012). Each quantitative study in this study was assigned into one of the following three categories based on an overall evaluation of risk of study bias based on this tool: low risk of bias, moderate risk of bias, or high risk of bias (see below for individual study ratings and Appendix 5 for bias/quality notes).

Evaluation of qualitative studies

Seventeen appraisal questions from Mays and Pope (2020) were used to evaluate the quality of qualitative studies based on the reporting of findings, study design, data collection, analysis, reporting, reflexivity and neutrality, ethics, and auditability of the studies (see Appendix 3). In this review, each qualitative study was allocated into one of the following three categories based on an overall evaluation of the study quality based on these 17 indicators: low quality, medium quality, or high quality (see below for individual study ratings and Appendix 5 for bias/quality notes).

Evaluation of mixed-method studies

For the only mixed-method study included in this review (see ITRC, 2003), the risk of bias and the study quality were evaluated separately for qualitative and quantitative elements of the study utilizing the frameworks by Hoy et al. (2012) and Mays and Pope (2020) (see below for individual study rating and Appendix 5 for bias/quality notes).

Study	Rating	Study	Rating
1. Anderson (2006)*	Low risk of bias	27. ITRC (2010)*	High risk of bias
2. Betz (2012)**	Medium quality	28. ITRC (2014)*	High risk of bias
3. Binette (2004)*	High risk of bias	29. ITRC (2015)*	High risk of bias
4. Burnes et al. (2020)*	Low risk of bias	30. ITRC (2017)*	High risk of bias
5. Burton (2008)*	High risk of bias	31. ITRC (2018a)*	High risk of bias
6. Copes et al. (2010)*	Moderate risk of bias	32. ITRC (2018b)*	High risk of bias
7. Cornelius (2016)*	High risk of bias	33. ITRC (2021)*	High risk of bias
8. DeLiema et al. (2021)*	Moderate risk of bias	34. Kpaduwa (2010)*	High risk of bias
9. Dinger and Sauer (2006) *	High risk of bias	35. Langton and Planty (2010)*	Moderate risk of bias
10. Gies et al. (2021)*	Moderate risk of bias	36. Li et al. (2019)*	High risk of bias
11. Golladay (2017)*	Low risk of bias	37. Marcum et al. (2016)*	High risk of bias
12. Golladay and Holtfreter (2017)*	Low risk of bias	38. Navarro and Higgins (2017)*	High risk of bias
13. Gray (2010)*	High risk of bias	39. Ponemon Institute (2011)*	High risk of bias
14. Green et al. (2020)**	Medium quality	40. Ponemon Institute (2012)*	High risk of bias
15. Green et al. (2021)*	Moderate risk of bias	41. Ponemon Institute (2013)*	High risk of bias
16. Harrell (2017)*	Low risk of bias	42. Ponemon Institute (2015)*	High risk of bias
17. Harrell (2019)*	Low risk of bias	43. Pryor (2009)**	Medium quality
18. Harrell (2021)*	Low risk of bias	44. Randa and Reyns (2020)*	Low risk of bias
19. Harrell and Langton (2013)*	Low risk of bias	45. Reynolds (2020)*	Low risk of bias
20. Holt and Turner (2012)*	High risk of bias	46. Reyns and Randa (2017)*	Low risk of bias
21. Holtfreter et al. (2015)*	Moderate risk of bias	47. Reyns et al. (2019)*	High risk of bias
22. ITRC (2003)***	High risk of bias/low quality	48. Sauer (2005)*	High risk of bias

Study	Rating	Study	Rating
23. ITRC (2005)*	High risk of bias	49. Sauer (2010)*	High risk of bias
24. ITRC (2007)*	High risk of bias	50. Silberman (2004)*	High risk of bias
25. ITRC (2008)*	High risk of bias	51. Synovate (2003)*	Low risk of bias
26. ITRC (2009)*	High risk of bias	52. Synovate (2007)*	Low risk of bias

*Studies that analyze data quantitatively were classified into one of the following three bias ratings: low risk of bias, moderate risk of bias, or high risk of bias

**Studies that analyze data qualitatively were classified into one of the following three quality ratings: low quality, medium quality, or high quality

***For the only mixed-method study included in this review, results from qualitative and quantitative analysis were evaluated separately

Appendix 5

Bias and quality assessment summary notes for included studies

Study	Notes on bias and quality
AARP publications: Binette (2004); Burton (2008); Dinger and Sauer (2006); Sauer (2005, 2010); Silberman (2004)	*Sample stratification based on few or no variables. *Response weighting on few or no variables. *Measurement of victimization experiences in the past 5 years (as opposed to a shorter time period) introduces risk of bias due to recall issues. *Questions aimed at capturing respondents' identity theft victimization experiences ask (1) if the respondent or somebody known by the respondent experienced identity theft victimization in the past 5 years and (2) what kind of identity theft was experienced by the respondent and somebody they knew. Although for the first question, it is possible to discern between the personal victimization experiences of the respondents and people known by the respondents, it is not possible to discern between (a) the type of identity theft experienced by respondents and people known by respondents and (b) the geographical scope of victimization. *the surveys ask about victimization experiences of people known by the respondents without limiting the residence of these acquaintances to respondents' state of residence
BJS 2010 report: Langton and Planty (2010)	The shortest prevalence period (two years) introduces recall bias
BJS 2012, 2014, 2016, 2018, 2021 reports: *Harrell* (2017, 2019, 2021); Harrell and Langton (2013)	National surveys. The response rate was less than 75%, however, the nonresponse bias analysis suggested that there was little or no bias of substantive importance due to nonresponse in the ITS estimates
FTC reports: Synovate (2003, 2007*)*	National surveys. Sample weights including a design weight to provide unbiased estimates
Anderson (2006)	There were no missing values in 3217 observations, but there was a missing value for one variable in 650 observations. There were missing values for three or more variables in only 111 cases. To avoid losing observations because of these missing data, conditional mean imputation was employed to provide estimates for missing values of independent variables. Weighted regressions are used
Betz (2012)	The study had many strengths with regards to reporting of findings, description of the study design, sample, linking of study findings to the original conceptual framework, ethical considerations, and limitations of the study. The author used several strategies such as member checks, peer review, and reflexivity to increase the rigor of the study. However, this study was rated as moderate quality due to the author not explaining the scope for making wider inferences well-enough; the eventual sample composition; the author not providing much information with regards to the efforts taken to maximize inclusion of all groups; and the author not being able to achieve triangulation. Only 1 out of the 6 participants in the study engaged in one-on-one interviews with the author and provided additional documentation about their victimization. The rest of the interviews were conducted over phone and the author did not seek additional documentation from these 5 participants
Burnes et al. (2020)	Data from national survey; pooled data (despite not being longitudinal); missing data were managed with a fully conditional specification multiple imputation method using five pooled data sets

Study	Notes on bias and quality
Copes et al. (2010)	This study used data derived from the second wave of the National Public Survey on White Collar Crime. The response rate was less than 75%; the authors did not describe the steps taken to address for any dissimilarities between the sample and the target population; there are important forms of identity theft not captured by the NW3C survey (e.g., utilities fraud, income tax fraud, or mortgage fraud); because the survey was administered at the household level, it is not always possible to ensure that that responses about victimization and reporting correspond to the responding individual's experience or whether it reflects the experiences of multiple individuals in the same household; the cross-sectional survey data does not allow for a determination of the exact causal ordering of risky behaviors and fraud victimization
Cornelius (2016)	The researcher used Survey Monkey's demographic selection tool to source potential and eligible participants for the study. There was no description of how the study sample resembles the target population; the author used listwise deletion for participants with missing responses and there was no description of how much data was deleted as a result of this process and the measures taken to reduce nonresponse bias; no study instrument was provided for the identity theft questions
DeLiema et al. (2021)	The data is from two pooled iterations of the NCVS-ITS. Data were weighted to reflect a nationally representative sample in regard to age, gender and race/ethnicity and to compensate for survey nonresponse and aspects of the staged sampling design. The main shortcoming of the study was the study focuses on experiences of older individuals; however, certain groups are excluded from the NCVS-ITS: individuals in institutional settings, individuals living in transient settings and individuals with severe cognitive impairment all of whom might be at higher risk of identity fraud victimization among the targeted age group
Gies et al. (2021)	The data for this study are derived from two sources: (a) a survey of persons who requested assistance from the ITRC regarding a serious identity crime incident and (b) the ITS administered as part of the Bureau of Justice Statistics' NCVS. The first source of data is the ITRC Survey. The study used propensity score matching technique with key demographic variables identified by research and analysis revealed no significant differences between groups with regards to key matching variables. However, the ITRC survey response was very low and there was no discussion on strategies employed by the researchers to reduce bias associated with this low response. Furthermore, although the study design allowed for comparison of experiences of identity theft victims who contacted the ITRC, another organization, or did not contact any organization; because of the type of questions asked to capture these experiences, it is not possible to temporally discern if the outcomes are a result of help-seeking behavior of the victims. Method of data collection is not the same for the ITRC survey and the ITS survey
Golladay (2017)	The analysis was based on the NCVS-ITS. With the exception of potential omission of some variables in relation to the seriousness of the offense, no other significant issues were detected with regards to study design, construction of the analysis model, or reporting of results
Golladay and Holtfreter (2017)	The analysis was based on the 2012 NCVS-ITS and no significant issues were detected with regards to study design, construction of the analysis model, or reporting of results
Gray (2010)	Data were retrieved from 70 respondents living in Rio Grande Valley, Texas via a 70-question survey over the Internet and data were analyzed using multiple regression to determine the variables most influential on the reporting of internet identity theft incidents. The study had a small non-representative convenience sample (snowball sampling) and a low response rate

Study	Notes on bias and quality
Green et al. (2020)	The scope for making wider explanations was not explained well; the information on data collection and data analysis and the impact of these on concluded results was fairly limited; there was not enough discussion on the limitations of the sample and the methodology; there was not enough information to reproduce the findings from the study (such as information about the changes made to the study instruments, data collection and data analysis plans); there was no discussion on how error or bias may have arisen at each stage of the research and how this was addressed
Green et al. (2021)	The scope for making wider explanations not explained well; the information on data collection and data analysis and the impact of these on concluded results was fairly limited; there was no discussion on how error or bias may have arisen at each stage of the research and how this was addressed
Holt and Turner (2012)	University sample. Information not provided regarding nonresponse rate, any issues regarding bias, or the strategies used to address such bias
Holtfreter et al. (2015)	Sample excluded mobile phone only households; the response rate to the survey was low (less than 50%); underrepresentation of certain demographic groups in the sample in comparison to each state's demographic profiles (i.e., individuals who identify as male, Hispanic, and individual who report a higher education level)
ITRC studies: ITRC (2003, 2005, 2007, 2008, 2009, 2010, 2014, 2015, 2017, 2018a, 2018b, 2021)	The population of these studies are individuals who contacted the ITRC which might be already a narrow group of victims who had more serious identity theft experiences. Very high non-response rate; no clear explanation of bias introduced by non-response and sampling frame and strategies used to address these biases
Kpaduwa (2010)	Convenience university sample; stratified sampling but does not provide details about the process; does not provide information about what has been done to address nonresponse bias
Li (2019)	Small sample size; no discussion on the bias introduced by the Qualtrics sample; no weighting to adjust for potential difference of the sample from the target population

Study	Notes on bias and quality
Marcum et al. (2016)	Low response rate; no explanation of strategies taken to reduce nonresponse bias; data on students' victimization information is collected from counsellors
Navarro and Higgins (2017)	Study is based on the 2012 iteration of the NCVS. The authors indicate that there is a large amount of missing data in the variables they included in their models and they excluded the cases with missing data. However, authors do not indicate how much of a loss this was and how they decided to exclude cases
Ponemon Institute reports: *Ponemon* (2011, 2012, 2013, 2015)	Although the Ponemon studies aim for a nationally representative sample and the reports mention the performing of non-response bias tests, there is not enough information provided in any of the four studies included in this review to evaluate if the sample was representative of the US adult population and if non-response introduced any bias. Furthermore, survey participants provided victimization information for themselves and household members. Accordingly, prevalence estimates are not solely based on data collected directly from victims
Pryor (2009)	The sample composition and case inclusion and the context of data were not explained in detail; diversity of perspectives were not explored in detail; the depth of the data was not conveyed in detail; the assumptions and values that have shaped the research and its reporting were not clear
Randa and Reyns (2020)	The analysis was based on the NCVS-ITS and no significant issues were detected with regards to study design, construction of the analysis model; or reporting of results
Reynolds (2020)	The analysis was based on the NCVS-ITS and no significant issues were detected with regards to study design, construction of the analysis model; or reporting of results
Reyns and Randa (2017)	The analysis was based on the NCVS-ITS and no significant issues were detected with regards to study design, construction of the analysis model; or reporting of results

Study	Notes on bias and quality
Reyns et al. (2019)	University sample (with participants from 2 universities); the response rate to the survey was low; authors did not provide information regarding how the sample differed from the target population, the steps taken by the authors to address potential biases introduced by level of non-response to the survey, and the differences between the sample and the target population

Acknowledgements
I would like to thank the anonymous peer reviewers, Dr. Schumann, and Dr. Wortley for their thoughtful feedback on this manuscript. I would like to thank Alexandra Ricks for her contribution to the early stages of this project. I would like to thank Dr. David B. Wilson for sharing resources on assessments of quality of qualitative research. I would like to also thank Dr. Christopher Koper for his review of and thoughtful feedback on an earlier version of this article.

Author Contribution
The author conducted the review presented in this article and approved the final manuscript.

Declarations

Competing interests
The author declares that she has no competing interests.

Received: 11 August 2023 Accepted: 27 January 2024
Published online: 10 February 2024

References

*Anderson, K. B. (2006). Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing, 25*(2), 160–171.
*Betz, A.E. (2012). The experiences of adult/child identity theft victims. (Unpublished doctoral dissertation). Iowa State University, Ames.
Binette, J. (2004). AARP Oklahoma Legislative issues survey: identity theft. https://assets.aarp.org/rgcenter/post-import/ok_id_theft.pdf. Accessed 5 Dec 2021.
*Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports, 17*, 101058.
*Burton, C. (2008). *Consumer fraud: A 2008 survey of AARP Colorado members' experiences and opinions*. AARP Foundation.
Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36–54.
Buzzard, J., & Kitten, T. (2021). Identity fraud study: Shifting angles". https://www.javelinstrategy.com/research/2021-identity-fraud-study-shifting-angles. Accessed 5 Dec 2021.
*Copes, H., Kerley, K. R., Huff, R., & Kane, J. (2010). Differentiating identity theft: An exploratory study of victims using a national victimization survey. *Journal of Criminal Justice, 38*(5), 1045–1052.
Copes, H., & Vieraitis, L. M. (2009). Bounded rationality of identity thieves: Using offender-based research to inform policy. *Criminology & Public Policy, 8*(2), 237–262.
Copes, H., & Vieraitis, L. M. (2012). *Identity thieves: Motives and methods*. UPNE.
Cornish, D., & Clarke, R. V. (1986). *The reasoning criminal: Rational choice perspectives on offending*. Springer-Verlag.
*Cornelius, D. R. (2016). Online identity theft victimization: An assessment of victims and non-victims level of cyber security knowledge (Doctoral dissertation, Colorado Technical University).
*DeLiema, M., Burnes, D., & Langton, L. (2021). The financial and psychological impact of identity theft among older adults. *Innovation in Aging*. https://doi.org/10.1093/geroni/igab043
*Dinger, E., & Sauer, J. (2006). Protecting your name: A survey of Montanans on identity theft. https://www.aarp.org/money/scams-fraud/info-2006/mt_id.html. Accessed 5 Dec 2021.
Dixon, P. & Barrett, T. (2013). *Medical identity theft.* Office for Victims of Crime's National Identity Theft Network. https://www.youtube.com/watch?v=sOa6AWzHSEs. Accessed 5 Dec 2021.
Federal Trade Commission (FTC). (2004). FTC issues final rules on FACTA identity theft definitions, active duty alert duration, and appropriate proof of identity. https://www.ftc.gov/news-events/press-releases/2004/10/ftc-issues-final-rules-facta-identity-theft-definitions-active. Accessed 5 Dec 2021.
Federal Trade Commission (FTC). (2011). Stolen futures: A forum on child identity theft. https://www.ftc.gov/news-events/events-calendar/2011/07/stolen-futuresforum-child-identity-theft. Accessed 5 Dec 2021.
Federal Trade Commission (FTC). (2017). *Identity theft: planning for the future, parts 1, 2, and 3*. https://www.ftc.gov/news-events/audio-video/video/identity-theft-planning-future-part-1. Accessed 5 Dec 2021.
Federal Trade Commission (FTC). (2018). *Consumer sentinel network data book 2017*. Washington, DC: Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf. Accessed 5 Dec 2021.
Federal Trade Commission (FTC). (2022). Data breach response: A guide for business. https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business. Accessed 20 Dec 2022.
*Gies, S. V., Piquero, N. L., Piquero, A. R., Green, B., & Bobnis, A. (2021). Wild, wild theft: Identity crimes in the digital frontier. *Criminal Justice Policy Review, 32*(6), 592–617.
*Golladay, K. A. (2017). Reporting behaviors of identity theft victims: An empirical test of Black's theory of law. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-01-2016-0010
*Golladay, K., & 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.* https://www.gao.gov/assets/690/683842.pdf. Accessed 5 Dec 2021.
*Gray, K. (2010). Internet identity theft: An insight into victimology and law enforcement response. (Unpublished doctoral dissertation). Capella University.
*Green, B., Gies, S., Bobnis, A., Leeper Piquero, N., Piquero, A. R., & Velasquez, E. (2021). Exploring identity-based crime victimizations: Assessing threats and victim services among a sample of professionals. *Deviant Behavior, 42*(9), 1086–1099.
*Green, B., Gies, S., Bobnis, A., Piquero, N. L., Piquero, A. R., & Velasquez, E. (2020). The role of victim services for individuals who have experienced serious identity-based crime. *Victims & Offenders, 15*(6), 720–743.
*Harrell, E. (2017). Victims of Identity Theft, 2014. Washington, DC: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://www.bjs.gov/content/pub/pdf/vit14.pdf. Accessed 5 Dec 2021.
*Harrell, E. (2019). Victims of Identity Theft, 2016. Washington, DC: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://www.bjs.gov/content/pub/pdf/vit16.pdf. Accessed 5 Dec 2021.
*Harrell, E. (2021). Victims of identity theft, 2018. Washington, DC: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://www.bjs.gov/content/pub/pdf/vit16.pdf. Accessed 5 Dec 2021.
*Harrell, E., & Langton, L. (2013). Victims of identity theft, 2012. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://bjs.ojp.gov/content/pub/pdf/vit12.pdf. Accessed 5 Dec 2021.
*Holt, T. J., & Turner, M. G. (2012). Examining risks and protective factors of on-line identity theft. *Deviant Behavior, 33*(4), 308–323.
*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.
Hoy, D., Brooks, P., Woolf, A., Blyth, F., March, L., Bain, C., Baker, P., Smith, E., & Buchbinder, R. (2012). Assessing risk of bias in prevalence studies: modification of an existing tool and evidence of interrater agreement. *Journal of Clinical Epidemiology, 65*(9), 934–939.

Irvin-Erickson, Y., & Ricks, A. (2019). Identity theft and fraud victimization: What we know about identity theft and fraud victims from research-and practice-based evidence. https://www.ojp.gov/ncjrs/virtual-library/abstracts/identity-theft-and-fraud-victimization-what-we-know-about-0. Accessed 5 Dec 2021.

*ITRC. (2021). *Identity theft: the aftermath study*. Identity Theft Resource Center.

*ITRC. (2003). Identity theft: the aftermath 2003. https://www.idtheftcenter.org/images/page-docs/IdentityTheftTheAftermath2003.pdF. Accessed 5 Dec 2021.

*ITRC. (2005). Identity theft: the aftermath 2004. https://www.idtheftcenter.org/images/surveys_studies/Aftermath2004.pdf. Accessed 5 Dec 2021.

*ITRC. (2007). Identity theft: the aftermath 2006. https://www.idtheftcenter.org/images/surveys_studies/Aftermath2006.pdf. Accessed 5 Dec 2021.

*ITRC. (2008). Identity theft: the aftermath 2007. https://www.idtheftcenter.org/images/surveys_studies/Aftermath2007.pdf. Accessed 5 Dec 2021.

*ITRC. (2009). Identity theft: the aftermath 2008. https://www.idtheftcenter.org/images/surveys_studies/Aftermath2008.pdf. Accessed 5 Dec 2021.

*ITRC. (2010). Identity theft: the aftermath 2009. https://www.idtheftcenter.org/images/surveys_studies/Aftermath2009.pdf. Accessed 5 Dec 2021.

*ITRC. (2014). Identity theft: the aftermath 2013. https://www.idtheftcenter.org/images/surveys_studies/Aftermath2013.pdf. Accessed 5 Dec 2021.

*ITRC. (2015). Identity theft: the aftermath 2014 https://www.idtheftcenter.org/images/surveys_studies/Aftermath2014FINAL.pdf. Accessed 5 Dec 2021.

*ITRC. (2017). Identity theft: the aftermath 2016. https://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf. Accessed 5 Dec 2021.

*ITRC. (2018a). Identity theft: the aftermath 2017. https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf. Accessed 5 Dec 2021.

*ITRC. (2018b). *The aftermath: the non-economic impacts of identity theft*. Identity Theft Resource Center.

ITRC. (2019). *First-ever AI fraud case steals money by impersonating CEO*. Identity Theft Resource Center.

*Kpaduwa, F. I. (2010). Evaluation of residential consumers knowledge of wireless network security and its correlation with identity theft (Unpublished doctoral dissertation). University of Phoenix.

*Langton, L., & Planty, M. (2010). Victims of identity theft, 2008. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://bjs.ojp.gov/content/pub/pdf/vit08.pdf. Accessed 5 Dec 2021.

*Li, Y., Yazdanmehr, A., Wang, J., & Rao, H. R. (2019). Responding to identity theft: A victimization perspective. *Decision Support Systems, 121*, 13–24.

*Marcum, C. D., Higgins, G. E., & Mackinnon, A. (2016). Identity theft reports of adolescents. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-07-2015-0038

Mays, N., & Pope, C. (2020). Quality in qualitative research. In C. Pope & N. Mays (Eds.), *Qualitative research in health care* (pp. 211–233). Wiley.

McNally, M. M., Newman, G. R., & Graham, C. (2008). *Perspectives on identity theft* (Vol. 23). Criminal Justice Press.

National Conference of State Legislatures, (2022). Security breach notification laws. https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Accessed 20 Dec 2022.

*Navarro, J. C., & Higgins, G. E. (2017). Familial identity theft. *American Journal of Criminal Justice, 42*(1), 218–230.

Newman, G. R., & McNally, M. M. (2005). Identity theft literature review. https://www.ojp.gov/ncjrs/virtual-library/abstracts/identity-theft-literature-review. Accessed 5 Dec 2021.

Newman, G. R., & McNally, M. M. (2007). Identity theft: a research review. https://www.ojp.gov/ncjrs/virtual-library/abstracts/identity-theft-research-review. Accessed 5 Dec 2021.

Office for Victims of Crime (OVC). (2010). *Expanding services to reach victims of identity theft and financial fraud*. https://www.ovc.gov/pubs/ID_theft/pfv.html. Accessed 5 Dec 2021.

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. http://www.ncdsv.org/images/OVCTTAC_IdentityTheftResourcePaper_2012.pdf. Accessed 5 Dec 2021.

*Ponemon Institute. (2011). Second annual survey on medical identity theft. https://www.experian.com/innovation/thought-leadership/medical-identity-theft-second-annual-survey.jsp. Accessed 5 Dec 2021.

*Ponemon Institute. (2012). Third annual survey on medical identity theft. https://www.ponemon.org/research/ponemon-library/security/?tag=38. Accessed 5 Dec 2021.

*Ponemon Institute. (2013). 2013 survey on medical identity theft. https://www.ponemon.org/local/%20upload/file/2013%20Medical%20Identity%20Theft%20%20Report%20FINAL%2011.pdf. Accessed 5 Dec 2021.

*Ponemon Institute. (2015). Fifth annual study on medical identity theft. https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65#:~:text=The%20five%2Dyear%20growth%20rate,victim%20or%20non%2Dvictim%20status.&text=This%20year%20we%20collected%2051,victims%20after%20sampling%205%2C000%20trials. Accessed 5 Dec 2021.

*Pryor, W. J. (2009). *When your identity gets hijacked: The victim's experience of identity theft (un published doctoral dissertation)*. California Institute of Integral Studies.

*Randa, R., & Reyns, B. W. (2020). The physical and emotional toll of identity theft victimization: A situational and demographic analysis of the National Crime Victimization Survey. *Deviant Behavior, 41*(10), 1290–1304.

*Reynolds, D. (2020). The differential effects of identity theft victimization: How demographics predict suffering out-of-pocket losses. *Security Journal*. https://doi.org/10.1057/s41284-020-00258-y

*Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2019). Opportunity and self-control: Do they predict multiple forms of online victimization? *American Journal of Criminal Justice, 44*(1), 63–82.

*Reyns, B. W., & Randa, R. (2017). Victim reporting behaviors following identity theft victimization: Results from the National Crime Victimization Survey. *Crime & Delinquency, 63*(7), 814–838.

*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. https://www.aarp.org/money/scams-fraud/info-2005/stealing_your_good_name_a_survey_of_washington_sta.html. Accessed 5 Dec 2021.

*Sauer, J.H. (2010). Consumer fraud issues: survey of AARP members 50+ in West Virginia. AARP Knowledge Management, AARP Research. https://www.aarp.org/money/scams-fraud/info-03-2010/wva_fraud_10.html. Accessed 5 Dec 2021.

*Silberman, S.L. (2004). AARP minnesota identity theft survey: a study of residents 18+. AARP Knowledge Management, AARP Research. https://www.aarp.org/money/scams-fraud/info-2004/aresearch-import-927.html. Accessed 5 Dec 2021.

*Synovate. (2003). Federal Trade Commission—identity theft survey report. https://www.ftc.gov/sites/default/files/documents/reports/federal-tradecommission-identity-theft-program/synovatereport.pdf. Accessed 5 Dec 2021.

*Synovate. (2007). Federal Trade Commission—2006 identity theft survey report. https://www.ftc.gov/sites/default/files/documents/reports/federal-tradecommission-2006-identity-theft-survey-report-preparedcommission-synovate/synovatereport.pdf. Accessed 5 Dec 2021.

Tedder, K. & Buzzard, J. (2020). 2020 Identity fraud study: genesis of the identity fraud crisis. https://www.javelinstrategy.com/research/2020-identity-fraud-study-genesis-identity-fraud-crisis. Accessed 5 Dec 2021.

Turanovic, J. J., & Pratt, T. C. (2019). *Thinking about victimization: Context and consequences*. Routledge.

Vieraitis, L. M., Copes, H., Powell, Z. A., & Pike, A. (2015). A little information goes a long way: Expertise and identity theft. *Aggression and Violent Behavior, 20*, 10–18.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.