VICTIMS & OFFENDERS
2021, VOL. 16, NO. 3, 444–463
https://doi.org/10.1080/15564886.2020.1826023

Routledge
Taylor & Francis Group

Preventing Identity Theft: Perspectives on Technological Solutions from Industry Insiders

Nicole Leeper Piquero[a], Alex R. Piquero[a,b], Stephen Gies[c], Brandn Green[c], Amanda Bobnis[c], and Eva Velasquez[d]

[a]Department of Sociology, University of Miami, Miami, Florida, USA; [b]Monash University, Melbourne, Australia; [c]Development Services Group, Inc., Bethesda, Maryland, USA; [d]Identity Theft Resource Center, San Diego, California, USA

ABSTRACT

An estimated 26 million American citizens per year have been victims of an identity-based crime. This study contributes to the scholarship on financial crimes facilitated through identity-based criminal activity by examining the views on technological approaches to the prevention of identity theft among 50 professionals working in the identity-based crime victim services, including those from the public sector and private industry. The professionally diverse sample included private investigators, fraud examiners, victim service providers, and executives of firms offering victim services and protection services. Data were collected during a series of focus groups held at professional conferences. The paper reports on the views held by focus group participants on specific technological solutions to identity theft victimization, including biometric scanning, dark web scanning, subscription - based monitoring programs, and broader thematic observations about the current environment for protecting information, emerging sources of risk, and policy recommendations identified by focus group participants. Perspectives from insiders about the pros and cons of each approach can provide researchers and enforcement agencies with enhanced capacity to avoid empty technological promises that fail to protect victims from subsequent victimizations.

KEYWORDS

Identity Theft; Fraud; White-Collar Crime

Introduction

Identity-based victimization continues to be a growing problem in terms of both the total number of victims and the amount of direct and indirect harm caused to those victims. Like other white-collar crimes, the victims are individuals as well as organizations. The costs of identity-based crimes often are believed to be easily calculated by simply assessing the amount of direct victimization or the amount of money that has been taken (Cohen, 2016). However, as many scholars who estimate the costs of crimes have found, the taxonomy of crime costs includes at least three major categories: 1) costs incurred in anticipation of the crime (i.e., prevention), 2) costs incurred as a consequence of the crime (i.e., victimization), and 3) costs in response to crime (i.e., criminal justice expenditures) (Brand & Price, 2000; Cohen, 2005, 2016). The focus of this paper is on understanding prevention efforts, particularly the technological approaches, to combating identity-based crimes. In order to do so, we asked

CONTACT Brandn Green bgreen@dsgonline.com Development Services Group, Inc., 7315 Wisconsin Ave, Suite 800, Bethesda, MD 20814, USA.

industry insiders their views about existing and emerging threats to victims, both individual and organizational, their assessment of effectiveness and limitations to specific technological prevention solutions, and recommendations for improving systems and policies.

The prevention of identity theft (Gilbert & Archer, 2012; Milne, 2003) does not lie with only one entity but rather requires the responsibility, cooperation, and actions of three major groups: individuals, businesses, and government. Individuals have the information that must be protected and need to take care to guard their personally identifiable information (PII). To help them do so, agencies such as the Federal Trade Commission recommend a plethora of preventive measures, such as shredding sensitive documents and regularly reviewing credit reports and credit card statements, which individuals are encouraged to undertake for their own protection. Businesses are entrusted with consumers' PII, whether they require individuals to give it to them during business transactions or whether individuals freely share such information with them (e.g., on free social networking sites). Government or legislative bodies enact legislative measures that are designed either to deter the crime by creating tough punishments for those guilty of identity theft or to prod businesses into improving security measures for safeguarding the PII that individuals have entrusted to them. Actions taken in isolation by any one of the three entities (individuals, businesses, or government) will increase protection; however, as indicated by industry experts we spoke with, what really must occur is the collective cooperation and proactive engagement of all who bear responsibility for preventing identity-based crimes.

Background evidence

Identity theft and identity fraud, while connected, are not the same (Sullivan, 2009). Identity theft is often the first step in a two-step process by which specific types of personally identifiable information (PII) are stolen and used to commit identity fraud (Vieraitis et al., 2015).

Incidence of identity-based victimization

In 2016 the estimate for incidents of past-year identity-based victimization in the United States was at 26 million (Harrell, 2019). Identity-based crimes, including identity theft and fraud, are growing areas of crime (Center for Victim Research [CVR], 2019). Comparison studies of identity-based crime victims and victims of both violent and nonviolent crimes have concluded that victims of identity-based crimes are less likely to report an incident to law enforcement and are more likely to report it to non-law enforcement agencies than other types of victims (Copes et al., 2010; Harrell & Langton, 2013; Piquero, 2018; Reyns & Randa, 2017; Tcherni et al., 2016). Victims generally do not report the incidents of identity-based crime to law enforcement for one of two reasons: they have settled the issue with their financial institution, or they believe their losses are minor and have little hope that their personally identifiable information (PII) will be recovered (Tcherni et al., 2016). Remediation efforts vary greatly across different types of identity-based crimes. In addition, prior scholarship has noted that some personal data can be readily canceled (e.g., credit card numbers) whereas others (e.g., fingerprints) cannot (Solove & Citron, 2018).

Risk factors for identity-based victimization

Victimization research examining the relationship between activities taken by victims and exposure to the risk of identity theft has concentrated on online transactions (Lai et al.,

2012; Milne et al., 2004; Solove & Citron, 2018), the consequences of being the victim of a data breach (Solove & Citron, 2018), spending time in chat rooms and engaging in social networking (Holt & Bossler, 2014), and use of online security tools (Ricci et al., 2019). The consensus is that those who engage in routine computer communication and commerce supported by electronic transfers (e.g., credit cards) are at a slightly higher risk for identity-based crimes and that this risk is in contrast to the convenience electronic commerce creates for those who participate in modern business transactions (Chen et al., 2017; Payne & Kennett-Hensel, 2017; Reyns & Randa, 2017).

Adoption of technologies to prevent identity theft

As individuals spend more time online (e.g., checking e-mail, reading social media, ordering goods and services, banking), it is no surprise that there has been a concomitant increase in the risk of identity theft victimization, and in the range of services and technologies that people can use to help lower – but not eliminate – the risk of victimization. Unfortunately, not much is known about these services.

A recent study on fraud trends in the technology and payments industries offered recommended practices for individuals seeking to secure their PII, detect fraudulent activity, and obtain damages. Methods included using a digital wallet for instore and online purchases, setting up two-factor authentication for online accounts, adopting security measures for digital devices (e.g., screen locking, encrypting data, avoiding public Wi-Fi), placing security freezes on credit reports, and signing up for suspicious-activity monitoring of financial accounts (Tedder & Buzzard, 2020).

Zou et al. (2020) examined individuals' reasons for following or rejecting 30 expert-recommended security, privacy, and identity theft protection practices. A major concern associated with many of the recommended practices was their usability for the general public. Issues with set-up times, low quality of service, or barriers to implementation (such as lack of password managers, two-factor authentication, tools to limit tracking, e-mail encryption, or key management) affected the likelihood that individuals would continue these practices. Individuals were most likely to use security practices (e.g., evaluating the safety of links and attachments before accessing them, using good antivirus software) followed by privacy practices (e.g., hiding non-essential information in online transactions, using privacy-enhanced extensions for web browsers). The identity theft protection practice most used by individuals was regular checking of account statements. Interestingly, credit freezes and fraud alerts were among the top rejected identity theft protection practices, although they are two of the most commonly recommended practices for victims of data breaches.

Current study

Much has been learned about identity theft since it became a federal crime in 1998. Out of necessity, this body of work has expanded rapidly as more people move to doing daily tasks online, whether by computer, tablet, or, increasingly, cell phone. Identity theft research has helped to provide needed information on the characteristics of victims (Golladay & Holtfreter, 2017; Holtfreter et al., 2005; Rebovich, 2009), risks of exposure to victimization (Lai et al., 2012; Payne & Kennett-Hensel, 2017; Reyns & Randa, 2017), prevention strategies utilized (Lai et al., 2012), and understanding the motives of offenders (Copes &

Vieraitis, 2012) but much less effort has been devoted to understanding the technologies used to guard against victimization and the extent to which these technologies are useful.

This study is the outgrowth of a two-phase, mixed-methods project on the effects and quality of services available for victims of serious identity-based crime[1] in the United States. The project was funded through a grant awarded by the U.S. Department of Justice's National Institute of Justice to Development Services Group, Inc. In phase 1, the investigators integrated existing quantitative data from the U. S. Bureau of Justice Statistics' National Crime Victimization Survey with primary data collected from victims who used services provided by the Identity Theft Resource Center (Green et al., 2020). In phase 2, they collected qualitative data through interviews and focus groups with experts from public and private sector organizations engaged in preventing or remediating identity theft, and they analyzed these data (Green et al., 2020). For the analysis presented here, the key research questions were as follows: 1) How do identity theft industry professionals define the existing threats facing organizations and potential victims? 2) What are the emerging threats associated with serious identity-based crimes? 3) What proactive steps might individuals and organizations take to address the current and emerging threats for identity-based crimes?

Methodology

Participant recruitment

In coordination with the Identity Theft Resource Center (ITRC), the investigators prepared an initial list of 10 professional conferences that directly or indirectly address identity-based crime victimization. For each conference, ITRC's president or lead communications officer contacted the sponsoring organization's director or meeting planner to determine if the researchers could conduct focus groups during a regularly scheduled conference session. Two of the 10 organizations agreed to participate: the Association of Certified Fraud Examiners and the National Center for Victims of Crime. In addition to multiple focus groups at each of these two conferences, the investigators conducted focus groups of professionals who regularly engaged with the ITRC but were not ITRC employees. Advertisements for the focus groups were included with conference registration materials available before the meetings and were displayed at a vendor table staffed by the research team and ITRC personnel during the meetings. Potential participants were given the opportunity to join a focus group or complete a one-on-one interview. This recruitment process produced a total of 50 participants, including 45 people who were separated into 7 focus groups and 5 individuals who chose one-on-one interviews. To increase the comfort of focus group participants, no demographic or personal information was collected during these focus groups. All events occurred within the United States and all participants who shared details about their professional roles shared that they work primarily in the context of the United States.

Data collection

A focus group interview guide was developed by the research team, reviewed by ITRC personnel, and piloted with three individuals prior to use at the first focus group. The same

interview guide was used for all focus groups. The focus group interview guide was semi-structured and the focus group facilitator prompted respondents to elaborate or provide more detailed information about their answers. Each focus group member was asked to sign a consent form before participating in the focus group.

The research team audio-recorded and transcribed all focus groups sessions and interviews. The research team members also took notes during each meeting and produced an initial set of field notes within 1 day after the completion of each focus group. Each focus group meeting or one-on-one interview was scheduled for 1 hour. All research protocols were reviewed and approved by the DSG Institutional Review Board, the ITRC, and the National Institute of Justice grant project officer.

Data analysis

An inductive, or open, coding scheme was developed by the principal investigator and reviewed by the research team (Creswell, 2017). The inductive coding scheme was informed by the existing literature on technological solutions for preventing or remediating identity-based victimization. The principal investigator and a research assistant coded all transcripts using NVivo to manage the coding process and to enable inter-rater reliability. To begin the analysis process, both coders coded two transcripts and discussed differences and similarities in their coding. This discussion led to some convergence of codes and a few adjustments to the coding scheme. After agreement was reached on the final coding scheme, each of the two coding team members coded all the transcripts. Using the coding comparison query in NVivo enabled the team to further examine intercoder reliability. When there was less than 80% agreement between the coders about the quotations associated with a particular code, the coders re-reviewed all quotations under that code, achieved consensus on the appropriate codes for each quotation, and recoded quotations as needed. All quotations presented in the Results section were lightly edited for clarity and de-identified to protect the study participants' anonymity.

Results

The coding of the data lead to the identification of three overarching themes each corresponding with a specific research topics: (1) context for countering identity theft and fraud, (2) new frontiers of risk for identity-based crimes, and (3) recommendations for improving systems and polices to help prevent identity-based crimes.

Research question 1: How do identity theft industry professionals define the existing threats facing organizations and potential victims?

Industry insiders who participated in the study shared several common perspectives on the current threats faced by organizations and, indirectly, by individual consumers whose information may be stolen and used to commit fraud. The environment is one of constant change, where organizations are playing cat-and-mouse with sophisticated criminal actors who, like the organizations they target, are staying abreast of the most up-to-date technological solutions for preventing and detecting identity theft and related fraud. One focus group member described the context as follows:

> Every time we put a protection in place, the bad guys figure out a way to leverage that and use that to their advantage. So, it's a constant game of whack-a-mole. And so, we're looking at analytics, we're looking at biometrics, we're looking at blockchain, we're looking at what advanced technologies we can use and leverage to help continue to stay in front of that game.

Focus group members emphasized that their goal is no longer to simply prevent the theft of PII, because it already has been stolen. There was a consensus among participants that criminal organizations are acutely aware of the value of information and that the financiers of identity theft operations range from international gang networks to nation–states. One focus group participant who provides businesses with information technology (IT) solutions highlighted some of the challenges associated with trying to stop criminal actors who are attempting to commit identity theft:

> The fundamental issue, particularly for large companies, is the massive investment that these criminal organizations are making to get into our systems. Part of the problem is these people aren't even located here in the U.S. They're located overseas. They're funded by nation–states and are looking to disrupt our country economically. So, to your point, I don't know how our Chief Information Officer sleeps.

The fact that individual organizations' IT departments may be engaging in cybersecurity against nation–states suggests a massive disparity in scale between the two sides regarding personnel and financial resources dedicated to fighting this battle. Advances in the technologies criminal actors use creates another vector of exposure for entities that hold PII. A focus group member who concentrates on services for financial institutions made this observation: *"From the financial industry's perspective there is no single bullet to stopping all this. That's why I mentioned the need for trying to keep pace with where the innovations are coming from the criminal side."*

Throughout the focus groups, participants reflected on the tradeoffs associated with particular technological solutions that are relatively widespread. Table 1 lists intervention mentioned by at least one focus group member and summarizes the groups' perspectives on the general advantages and limitations of each intervention. This table only captures statements made during the focus groups; it does not represent a complete analysis of the tradeoffs associated with each intervention. It does, however, provide insights about how industry professionals view each intervention within the context of identity theft protection services.

When making decisions about implementing an intervention, organizations seek to balance their own fiduciary interests with the public good. Industries sometimes agree to share the cost of a technological solution. The introduction of chip cards, which focus group participants considered an effective intervention, required an agreement between the banking industry and the retail industry to shift the liability for fraudulent activity to the points of sale, away from the banks that issue the credit cards, as articulated by a focus group participant with first-hand knowledge of that process:

> If you're liable for the losses, you're going to do something about it … So the banks rolled out the EMV [Europay, Mastercard, and Visa]technology, the chip cards that you now have in your wallet to help reduce counterfeit fraud and it's very successful at doing that. But it came at enormous costs, right? … and so in order to convince the banks to spend all this money to implement this new security technology the agreement was to shift some of the liability for fraud … Now, if a … physical chip card is used at the retailer, and it's fraudulent, the retailer has the fraud liability, the bank is off the hook. So, we've shifted the liability from the financial institution to the retail organization, sort of in exchange for the banks investing in this security technology.

Table 1. Summary of limitations and perceived effectiveness of specific technological interventions for preventing identity theft.

Intervention	Limitations	Perceived Effectiveness
Identity theft prevention software	• Is heavily marketed but claims of usefulness are exaggerated • Detects identity theft based on credit bureau monitoring but less than half of identity theft incidents include financial events that would result in reports to credit bureaus	• Ineffective
End-user agreements	• Are difficult for users to understand because the prose is highly technical rather than user friendly • Do not engage users as partners in protecting their PII • Fail to effectively anticipate future risks	• Ineffective
Knowledge-based authentication	• Has very limited utility because information used for authentication also has been stolen and can be used to commit identity theft	• Ineffective
Artificial intelligence- and machine learning-based authentication	• Is currently limited in its capacity to detect and prevent identity theft • Is costly and therefore inaccessible to smaller organizations • Is based on algorithms that may be derived from fraudulent or corrupted PII, given the pervasiveness of identity fraud	• Partially effective
Chip cards	• Are costly to manufacture	• Effective
Two-factor authentication	• Is easily manipulated by criminal actors • Does not protect against other vectors of risk, including insider threats	• Partially effective
Monitoring software	• Can be misused by the organization that installed the program	• Not rated
Biometric identifiers (e.g., fingerprints)	• Cannot be replaced with new identifiers if stolen	• Partially effective

In addition to identifying the limitations of particular interventions, focus group participants highlighted two other challenges: insider threats and outdated software. One focus group member commented on the prevalence of identity theft committed by insiders:

> Only 35 percent of all data breaches are related to IT and hacking. IT and hacking are the 'sizzle' that make the news headlines, but it's the insider threat, whether [the victim is] consumer[s] and seniors, insider threat. Or whether [the victim is] business, it's the insider threat.

Participants emphasized the need for a set of integrated risk management systems incorporating processes that help firms identify insider threats among employees who may be recruited to participate in identity theft activity. Insider threats are not new to the world of fraud protection, but they have increased in sophistication and number, as the theft and sale of PII has continued to grow in potential value.

Focus group members who worked with organizations ranging in size and technological sophistication also express concerned about the potential for IT systems to be hacked. One variable that heavily influences criminal actors' ability to access PII is the age, and therefore the security, of the IT systems and software programs businesses used to manage their budgets, human resources, and daily operations. A focus group member working in cybersecurity alluded to the vulnerability associated with outdated technology:

> …from an IT perspective, from a cybersecurity perspective, we're still relying on 30-year-old technologies to protect us. As opposed to technologies that can prevent and detect the kinds of attacks that we've seen for 30 years.

The point was made that industries vary in the resources and capacity they have available for addressing these outdated systems. A focus group member indicated that larger banks

are improving their technology for combatting identity theft, but smaller banks, which tend to be less sophisticated in this regard, are being targeted by criminal actors:

> . . .the bigger banks are getting better at putting in controls. The smaller institutions or one-branch community banks . . . there's a big vulnerability there. And I think part of the criminal elements are shifting focus now and trying to hit the smaller ones.

Other participants noted that all organizations remain at risk because of the ubiquity of the collection of personal information among business. One participant observed that data breaches persist even in industries with the most financial and IT resources:

> When I look at banking, healthcare, the three credit bureaus, and social media, they all collect more personal information than any other business sector, and they all have more financial and IT resources than any other business sector. Banking and healthcare and the three credit bureaus and social media continue to get breached.

Additionally, one focus group member stated that the window of opportunity has closed for preventing identity theft:

> All these conversations of identities being stolen are irrelevant. the data is already stolen. It's over, it's done with, you can't do anything about it . . . it can't be mitigated anymore. The issue is, you have to change the processes . . . companies need to be careful, government entities need to be careful, IRS has had a breach, SEC has had breaches, everyone has had breaches . . . it's just the processes need to change.

When examining the context for combatting identity theft and fraud, our focus group participants described a constantly changing and rather bleak environment, noting that firms of any size or capacity are at risk, that most individuals already have had their PII stolen and distributed, and that firms have a default orientation toward deterrence and minimizing impact for eventual attempts at identity theft.

> **Research question 2: What are the emerging threats associated with serious identity-based crimes?**

Focus group participants were quick to highlight some of the new frontiers of identity-based crime, many of which are unknown to the average consumer but are on the radar of experts in the fraud prevention industry. These frontiers include small and midsize businesses, synthetic identities, and a criminal middle-class.

Small and midsize businesses

A subset of focus group participants worked for a regional grain processor based in the midwestern United States. They shared a story about how as their business grew, they became the target of a wide variety of schemes to access and steal PII. The schemes ranged from phishing through e-mail and the telephone to multiple efforts to hack their database and IT infrastructure. One of these participants drew a correlation between the firm's size and the increased attempts at identity theft:

> I think, too, because we're not invisible now. Because we've grown so large . . . if you Google grain processing and our name comes up right away. So . . . our name is out there a lot more, we have a lot more exposure. So, then people can get our information a lot easier.[2]

After experiencing these threats, the company shifted policies and began to return to a previously used paper-based system for record keeping, verifying sales, and accomplishing transfers of funds. From this company's perspective, switching to a paper-based approach proved to be an effective solution. For businesses and consumers across most sectors, however, returning to paper-based recordkeeping is not an option because the convenience of seamless and quick transactions is so compelling.

As computer-based commercial transactions and social interactions have increased, so have opportunities for identity theft, and as identity theft has increased, federal and state policies have attempted to address the risks of, and liability for, stolen PII. One respondent noted that the risks small and midsize businesses represent may not be effectively addressed by major data protection legislation:

> I think the state and federal laws are important. But they really only apply to people, companies, big money … the FTC [Federal Trade Commission] Red Flags Rule, has been in effect in this country for 8 years. And the majority of SMBs [small and midsize businesses] in the U.S. who have anything to do with FTC Red Flags Rule don't have a clue about it … I think GDPR [the General Data Protection Regulation] is going to be the same way – unless you're a big company, the majority of the small to medium-sized businesses don't care. Unfortunately, the majority of the small to medium-sized businesses are a conduit.

Both smaller and larger businesses have been making progress in decreasing the points of risk and potential exposure, but the continued updating of software and systems needed to manage IT infrastructure creates additional and new opportunities for vulnerabilities. Focus group participants highlighted the Gordian knot of exposure that can arise not only with the use of antiquated systems but also with the adoption of new technology. One industry insider described the ongoing challenge of staying one step ahead of criminal actors as follows:

> We had network firewalls and we shrunk those down to application firewalls, it's the same technology shrunk down. We have squeezed all that we can out of that model, and we now have to look for different models of protecting software because software is even more ambiguous … 111 billion new lines of code added every year. There aren't not enough fingers on keyboards to write correct code to deal with that volume.

A desire to increase the ease of interactions that result in financial transactions and purchases of goods and services drives smaller businesses to augment their computer capability and update their software. However, mixing legacy technology with contemporary technologies while trying to ensure continued ease of interactions creates opportunities for identity theft, and these opportunities are multiplying because more companies are collecting and reselling PII.

Questions arose among focus group participants about the long-term implications of data storage. The observation was made that no limitations have been set on the length of time firms can keep information. One participant noted that companies establish their own policies:

> What limits how long companies can keep data? Companies are putting in rules for record retention. So you might have to keep it for 5 or 10 years, but then you get rid of it when you don't have a legal need for it.

A separate paper (Green et al., 2020) examined in depth the interactive nature of identity theft, in which the behaviors of the organization holding an individual's PII, and the behaviors of the individual whose PII the organization is holding, affect both parties and influence the extent to which each becomes a victim of identity theft. Understanding the dynamic relationship between the organization and the individual is a key part of understanding emerging risks and how the risks vary by organizational size and IT capacity. This knowledge, in turn, is vital to the development of more targeted, and therefore more effective, interventions. One focus group member highlighted the fact that identity theft nearly always involves organizations:

> There's also an organization behind all of that data, for the most part. And those organizations also go through a process of learning. It's a painful learning experience and I can tell you from personal experience of having been there. But … at the end of the day, all of these crimes that we're talking about begin with someone extracting the data resources from an organization, by and large.

Synthetic identities

Focus group participants considered synthetic identities the most worrisome emerging threat to individuals who may be victimized by a serious identity-based crime. Unfortunately, not many people understand what this emerging crime is and how dangerous it can be. Synthetic identity theft requires that a criminal slowly and methodically create an artificial, or synthetic, person they can use to access capital. The process involves pairing a valid social security number with completely fictious personal information derived from one or more individuals such as name, address, date of birth, or any other information necessary to apply for any line of credit.

As one focus group participant ominously noted:

> If James is our bad guy. He will try to get his hands on a valid Social Security numbers and the key prize, the holy grail he's looking for, are SSNs of minors and kids.

Another important thing to note about creating a synthetic identity is that it takes time, patience, and an understanding of how lines of credit are established. The initial stages of forming a synthetic identity entail using the existing systems to check on an individual's credit history. The made-up name paired with the valid stolen social security number is not likely to immediately be granted any line of credit since there is no credit history. However, even though a credit application may at first be denied the attempt to create the synthetic identity has still been successful as it has put into motion the creation of a file at the credit bureau.

> And he will provide his made-up name, John Doe, paired with the valid SSN of a child and apply for a credit card. James' bank is going to go out, they've got an application, they're going to attempt to underwrite it, they will probably call out to a credit bureau to attempt to get a credit history. Well, that credit bureau will try to find a file associated with John Doe's valid SSN and other PI, and of course there's no file. So, they will return that response to James' bank, and James' bank more than likely is not going to take a risk and extend credit to John Doe and will just deny the application and go about their day. Now, what happens, is that inquiry from James' bank triggers the creation of a file at the credit bureaus, with John Doe and the kid's SSN and one denied credit by James' bank.

The focus group participant elaborated on the additional steps in the process:

> James is likely to go to an accomplice of his and do a practice that is legal, called piggy-backing, where they will then associate that synthetic file with their friend's valid credit card. And then make payments. Immediately that pairing of the two [i.e., the synthetic file and the valid credit card] transfers the presumably good credit of his accomplice onto the synthetic file itself. They'll spend some time making payments, buying things, paying it off on time, and over time you start to develop a tradeline on that synthetic file that starts to look OK. At some point James will then go to a new bank and apply for a credit card. Now, this second bank will put that through underwriting, and get a credit file back. It's not great, but it might be enough where [the second bank]doesn't know, it might be a new entry into the workforce, a college student, you never know, but maybe it's enough where you want to extend them a very modest credit line to allow them to get into the banking system. Now, the synthetic identity has credit. You do that multiple times, suddenly you've got a pretty nice chunk of change, and then you're going to bust out, where you max everything out and you disappear.

The preying upon minors' social security numbers likely ensures that the discovery of the identity theft crime is several years if not a decade or more off as it is unlikely that credit checks will be initiated until the victim is in their mid- to late-teens. Participants repeatedly emphasized their concern about the rise of synthetic identity theft and coupled lack of clear and effective prevention practices.

Criminal middle-class

The fact that synthetic identity theft is an emerging threat suggest a new class of criminal actors may be coming into being who have the financial capacity, knowledge, and patience to execute a multi-stage process that unfolds gradually over time.

This concern was echoed by several respondents, who spoke about the ways in which opportunities for identity theft and fraud may appeal to a "middle-class criminal." One participant referred to the "professionalization" of identity fraud:

> It's going to continue to increase as we have more people becoming connected, more people coming online, people realizing how lucrative this is. Right? Because this is the business model now. Fraud has been professionalized . . . We will create a middle-class criminal culture, where education separates those who are street level from those who are not. I'm not positive we need a middle criminal class, but I think we're going to get one.

As many respondents noted, identity theft-based crimes include highly sophisticated operations that may be receiving financial support from nation–states. Coupled with this increased sophistication and support structure is the existence, according to respondents, of a simple and direct way to sell digital goods: the dark web. Echoing other focus group members, one of our participants emphasized the dark web's role in facilitating identity-based crime:

> And there is nearly unlimited consensus for the [criminal] groups, whether organized or unorganized, state actors or not state actors, there is basically a one-way economy that is super productive, and the dark web is going on to make this happen.

To summarize the new frontiers of risk, our industry experts agreed that the emergence of an increasingly sophisticated set of criminal actors and ever-changing techniques will create new challenges for law enforcement and for organizations seeking to protect the

information held by companies. Of particular concern was the unique disadvantage of small and mid-size companies in keeping up with the barrage of new and constant risks, the growing use of synthetic identities as the reaches of which may not be known for quite some time, and the emergence of a new class of professional fraudsters.

Research question 3: What proactive steps might individuals and organizations take to address the current and emerging threats for identity-based crimes?

During each focus group, participants were asked to identify how to address the myriad challenges they had outlined during the discussion. Respondents made a variety of recommendations aimed at different stakeholder groups, including companies, policy makers, victim services professionals and organizations, and law enforcement. In this paper we document the recommendations aimed at companies and policy makers. Recommendations for victim services and law enforcement have been presented elsewhere (Gies et al., 2020; Green et al., 2020).

Recommendations for companies

> But in the world today, with so much doubt of being exposed, the paradigms need to change and that's what we're focusing on as a business. Because at this point . . . it's already done. All the data's stolen.

Companies need to continue upgrading and adapting the approaches they take to protect PII. Their strategies should include, according to focus group participants, extended vigilance to ensure effective mitigation of insider threats, a balance of easy transactions and safety, use of evolving technologies (specifically artificial intelligence and machine learning), and broader efforts to complete regular audits for potential fraud. The challenge participants noted lies in how best to motivate companies to expend the financial resources necessary to update systems and maintain surveillance and monitoring. The point was made that companies can be motivated by modifications or new laws within the regulatory structure established through new state and federal laws. One participant, who was echoed by many others, also highlighted the value of public–private partnerships where financial service industries take the lead:

> I think you're going to see models like that in a number of industries where we kind of come to the table and say, the financial institution may be the best kind of central entity to handle this type of transaction, or it's a healthcare organization or a retail organization or whatever it is, but we have to have some agreement and some process for sharing in this responsibility, this liability and the cost.

These partnerships are fundamentally about cost-sharing and distribution of risk. Multiple participants identified the need for better consumer-oriented protections and more consistency in norms and ethics related to data sharing, data storage, opt-out options for data agreements, expansion of open-sourced software, and adaptations of technological solutions to different types of vulnerable groups (e.g., seniors, teenagers). As the quote at the beginning of this section underscores, paradigm shifts may be needed to ensure the continued viability of electronic transmission and storage of PII in an environment where all the information already has been stolen. In the view of the study participants, within the current paradigm firms are struggling to keep up and already may have lost.

Recommendations for policy makers

The issue of identity theft will expand in importance as will the burden it places on the individuals and organizations that have been defrauded. One respondent highlighted the need for improved responses from the federal government:

> So, I believe the answer is a response from the government. I think companies need to focus on being resilient and compromise-ready. I think they need to focus on response and recovery.

The reason for this need is, as noted earlier, that prevention is no longer an appropriate conceptual framework for identity theft. Participants indicated that complicated questions must be addressed regarding policies associated with individuals' consent for firms to use their PII, for two reasons: first, few current user agreements are intelligible; and, second, it is possible that uses will be made of PII in the future that could not be anticipated at the time a user agreement was developed and signed.

Focus group members pointed out that the rise of synthetic identity theft is a complex phenomenon requiring the attention of experts in the domains of law, ethics, and policy. One industry professional observed that synthetic identity theft raises sweeping security questions:

> And I think people are beginning to understand how easy it is to compile an ID or to steal one or to exploit one. And so, I am seeing it start to move into some of the more kind of legal and risk and broader security questions people are asking.

Underscoring the importance of this issue, respondents described how children whose Social Security numbers have been attached to synthetic identities may not discover that they are victims of identity fraud until they become adults, potentially allowing for a decade or more of fraudulent activity to occur before the fraud comes to light.

A few respondents saw hope amidst the rapidly growing threat of identity theft that stems from the ways in which profits from the sale of PII can be linked to other types of crime. One of our focus group members pointed out that these links may result in better resource allocation to address identity theft:

> I am kind of backhandedly optimistic, because some of the people that I've talked to, particularly in international law enforcement, and at the NYPD [New York Police Department], are [aware of]the number of situations in which these kinds of [identity-based] crimes are being used to fund and facilitate broader crime rings. Right? So, street gangs are the ones who are using the stolen credit cards, and then they're using the stolen IDs to then go and fund gang activity. And so, this is actually – the line between kind of ID theft, cybercrime, ID theft, real-world crime – all of these things are coming together and that's merging. So, I think there's a possibility that there will be better resource allocation, because people will begin to recognize that these are not distinct instances or distinct types of crimes.

This observation also suggests that the funding of law enforcement divisions with the capacity to investigate identity theft-related crimes may be a growing area of need in all law enforcement departments.

Overall, experts who participated in these focus groups suggest the best way to improve systems and policies is to change the paradigm. Those groups responsible for PII, (i.e., individuals, businesses, and government) should stop independently seeking ways to prevent identity-based crimes because as most of our experts agreed PII is already out. Criminals already have access to the valuable information they need and are constantly

finding new ways to use/abuse it. Thus, this is no longer a prevention or even a rescue operation but rather is a recovery operation. The path forward necessitates the groups work collaboratively together to remedy the harms already perpetrated on the victims.

Discussion

This study sought to address three questions: 1) How do identity theft industry professionals define the existing threats facing organizations and potential victims? 2) What are the emerging threats associated with serious identity-based crimes? and 3) What proactive steps might individuals and organizations take to address the current context and emerging threats for identity-based crimes? To investigate these questions, we collected and analyzed data from focus groups, and one-one-one interviews with 50 professionals in the field of identity-based crime victim services. The sample included private investigators, fraud examiners, victim service providers, and executives of firms offering victim services and protection services.

Our results led to three overall conclusions. First, in the context of a rapidly evolving criminal enterprise with deep pockets, firms of all sizes are striving to make technological adaptations that decrease risk from identity theft and ensure trust in their services. Second, study participants highlighted three new frontiers of risk that warrant continued attention: Small and midsize businesses, synthetic identity theft, and an emerging "criminal middle class." Third, focus group members highlighted strategies and adjustments to policies and procedures that could protect both firms and individuals. Most notably, there is a pressing need for many companies to update antiquated technology that may be 30 years old or older, and that often is mixed with new technology. More attention also must be paid to insider fraud (i.e., fraud committed by employees targeting the same organizations that are victims of fraud). Further, individuals and organizations should not presume that identity theft prevention software, end user agreements, or knowledge-based authentication will automatically safeguard one from identity theft victimization. Focus group members deemed these methods ineffective. Biometric identifiers, two-factor authentication, and artificial intelligence-based authentication were considered partially effective. Only chip cards were perceived as effective. At the end of the day, being careful is the essential mitigation strategy that should be practiced regardless of the technological interventions adopted.

These study results underscore the need for a paradigm shift to effectively and efficiently address, and prevent, identity-based crimes. This broad finding has major implications for how law enforcement, businesses and other organizations, and individual consumers conceptualize, manage, and use personally identifiable information (PII).

First, it is incumbent upon law enforcement and other criminal justice system actors to change underlying assumptions regarding identity-based crimes. Identity-based crimes traditionally have been low on the law enforcement priority list, for several reasons. There is a lack of knowledge regarding identity theft and fraud in general as well as a lack of understanding of how widespread the problem is. Further, many law enforcement agencies are not equipped or trained to address the problem because the tactical and strategic responses significantly differ from the enforcement of traditional crime the police were designed to address. Perhaps most important, despite the fact that identity-based crime can be a harrowing and devastating experience for victims (Golladay & Holtfreter,

2017; Reyns et al., 2019; Solove & Citron, 2018), there is an underlying belief that identity-based crimes are not serious because victims often recover the monetary losses through their financial institutions.

One of the consequences of this lack of knowledge and training is that law enforcement and other criminal justice actors have, in some respects, taken a backseat to the financial sector and its institutions when it comes to addressing identity-based crimes. The frontline defenders in this case are less likely to be criminal justice professionals and more likely to be software engineers in the cybersecurity industry and other financial sector entities. This tendency is even true regarding the scholarship on identity-based crimes. The number of manuscripts authored by financial experts exceeds those by criminologists, although we are encouraged by the fact that this trend is shifting, with more recent attention being paid to the issue by criminologists.

Without the invested involvement of the criminal justice system, the emphasis seems to be less on policing and prosecuting identity-based criminals and more on mitigating liability and monetary losses. This shift in the actors (away from law enforcement, toward the cybersecurity industry and financial sector entities) and the focus (away from policing and prosecuting, toward mitigating liability and monetary losses) may have a significant influence on offenders' decision to commit identity-based crimes. Deterrence theory and criminal justice policy hold that, under certain conditions, punishment can improve compliance and deter future criminal activity (Piquero et al., 2011). While the theory of deterrence relies on three individual components of punishment – severity, certainty, and celerity – Nagin (2013) points out that the evidence supporting the deterrent effect of punishment certainty is far more consistent than for punishment severity. Moreover, the evidence supporting the effect of certainty pertains almost exclusively to the probability of apprehension. This finding has important policy implications for identity-based crimes because the probability that perpetrators of identity-based crimes will be apprehended is exceedingly low, owing to the fact that the chief protagonists in the battle to protect PII are software engineers with no legal authority or interest in pursuing criminal sanctions and to the fact that many victims of identity theft do not realize they have been victimized until many months, or even years, later – if at all.

Identity-based crimes are not simply financial crimes that can be adequately addressed by financial institutions. Rather, they are a growing, complex, and often devastating problem for the victims, and they increasingly are being linked to traditional, organized, and transnational crimes. Moreover, identity-based crimes should be policed and prosecuted in an effort to deter future crimes. As noted in an earlier quote, one of our focus group participants expressed this view when asked what steps must be taken to address the current context and emerging threats for identity-based crimes:

> These kinds of [identity-based] crimes are being used to fund and facilitate broader crime rings … real-world crime – all of these things are coming together and that's merging. S,o I think there's a possibility that there will be better resource allocation, because people will begin to recognize that these are not distinct instances or distinct types of crimes.

A second, related point is that the criminal justice system's response to identity-based crimes is disjointed and lacking in coordination (Wyre et al., 2020), which can be attributed to the fact that some of the criminal entities involved in these crimes are multi-jurisdictional and others, as one of our experts observed, are located abroad. The degree to which identity-based crimes are being committed by offenders situated in foreign countries is unclear, but

the experts in our focus groups believe that foreign nationals are responsible for at least some of the identity-based crimes committed against United States citizens. Multi-jurisdictional identity-based crimes cannot be pursued through traditional law enforcement means and techniques. As such, we must rethink our approaches to combatting international identity-based crimes and consider what or which agencies are in the best position to handle such cases? One such approach would be to draw on existing efforts designed to address other types of multi-jurisdictional crime such as the fusion centers created to combat terrorism

Another notable observation made by more than one focus group participant is that efforts to prevent identity theft at this point actually may be futile because the PII already has been. While this perspective merits consideration, it may amount to throwing in the towel a bit too soon. If all the PII already has been stolen, one would think that data breaches would be on the decline. Yet, the available data, although probably incomplete, do not bear that out. According to the Identity Theft Resource Center annual data breach report, the number of U.S. data breaches tracked in 2019 (1,473) increased 17% from the total number of breaches reported in 2018 (1,257) (Identity Theft Resource Center, 2020).

Further, new individuals are added to the pool of potential victims every day in hospitals around the world. According to the Centers for Disease Control and Prevention (CDC), nearly 4 million births occur every year in the United States alone. While protecting these identities is likely fraught with difficulties, it seems prudent to try to protect, as much as possible, the PII of those who have not been exposed. Protecting this information starting at a person's birth can go a long way toward preventing the creation of synthetic identities.

Conclusion

Focusing on preventing identity theft without mitigating the harm caused by identity fraud would be naive. Any strategy for dealing with identity-based crimes must integrate prevention and mitigation. This integration will require that consumers, businesses, and governmental agencies change their approach to the conceptualization and use of PII, as some of our focus group participants noted.

The first step in effecting this change is to increase consumer education regarding how the online exchange of PII may increase the risk of identity-based crimes (Gilbert & Archer, 2012; Milne, 2003; Milne et al., 2009). In today's digital environment, consumers demand the freedom to do almost everything on their own terms – to open new financial accounts, to hail a car through ride-share services, to share vacation photos instantly on social media sites, to send highly confidential information by e-mail. Business entities in turn provide these services, sometimes without charging a fee, in exchange for the consumer consenting to an End User License Agreement (EULA). Because EULAs typically are lengthy, highly technical, and full of legal jargon, most people do not pay close attention to them. In terms of identity-based crimes, the problem with these agreements is that they often (but not always) expose a person's PII by giving the business entity the right to remotely, collect, process, use, share, and store information about the consumer, including PII. As people become increasingly connected across networks, they exponentially expand the footprints of their identities, and thus provide more ways for their identity to be exposed and put at risk.

To prevent, or at least safeguard, this exponential sharing of identity footprints, consumers and governmental entities, like law enforcement, must re-conceptualize PII as currency. In reality, the value of one's identity far exceeds the cost of the paper that it is printed on or the file space in which it is stored. A thief who steals the information can sell it to other criminals or use it himself or herself to fraudulently obtain hundreds or even thousands of dollars in products and/or services. A business entity can sell the information to another business for use in a direct marketing campaign. The important policy implication is that consumers and policymakers must begin to value PII as much as the businesses who legally collect it for legitimate businesses purposes and offenders who illegally steal it.

On the mitigation side of the equation, when identity-based crime occurs, systems and processes must be in place to give victims the comprehensive help they need. Although identity theft and fraud are crimes in every state, victims still often face a tremendous financial, physical, emotional, and social burden in repairing the harm committed against them. How can victims rectify these consequences? Currently, as noted above, financial institutions will typically reimburse fraudulent credit cards charges and certain other financial costs. Like the victims of other types of crime, victims of identity theft and fraud also may have access to counseling services to deal with the crime's emotional consequences. However, victims of identity-based crimes sometimes suffer from long-term, residual effects that are unique to fraud victimization. For example, if a perpetrator uses the victim's name or health insurance policy numbers to see doctors, obtain prescription drugs, or file insurance claims, the victim's health record is adulterated, which may negatively affect the victim's treatment, health insurance, payment record, and credit report. In addition, the victim may receive the wrong medical care based on the false medical history.

Currently, these adulterated records, be they medical, legal, or financial, are not easily corrected and cause constant problems for the victim. Governmental entities must realize that more and more people will require remediation for this growing problem. One potential solution would be to create a mechanism similar to a petition for expungement, the removal of records from public inspection. In Maryland, for example, records may be expunged from 1) Motor Vehicle Administration files, 2) police files, and 3) court and police files. Each process removes very specific files and must be accomplished through the proper agency. Precedent exists for such judicial action. Some safe harbor laws, for example, permit juvenile victims to vacate delinquency adjudications and criminal convictions for offenses arising from commercial sexual exploitation or sex trafficking (Gies et al., 2020). The aim is to mitigate the multifaceted, lasting impact of adjudications and conviction. A similar mechanism could be established to help victims of identity-based crimes address problems posed by adulterated financial and medical records.

We do not want to leave readers with a "doom-and-gloom" conclusion about identity theft victimization and prevention. While our experts were less than impressed with several commonly used prevention techniques (e.g., prevention software, end-user agreements, knowledge-based authentications), they did identify some promising avenues to be pursued such as the use of biometrics, two-factor authentication, and chip cards. These strategies need to be coupled with careful vigilance in order to safeguard PII. Our experts noted several times this is a constant game of "whack-a-mole" thus individuals and organizations must be aware, agile, and adapting to the latest updates and innovations to protect their identities. Much like we have become accustomed to updating our smartphones and

changing our passwords, we must also get in the habit of regularly checking our credit reports and updating technology to try to stay at least one step ahead of identity thieves.

Notes

1. Serious identity-based crime is defined as any incident of identity theft and fraud other than those involving only the misuse of an existing credit card.
2. The type of business was modified slightly to protect the organization's anonymity.

Acknowledgments

We would like to express our appreciation to the staff of the ITRC, specifically Mona Terry and Charity Lacey, for assisting us with recruitment of interviewees. This study would also not have been possible without the willingness of interviewees to share their stories with us. Finally, the editorial and managerial staff at Development Services Group, Inc. provided support and review of the manuscript.

Disclosure statement

The authors of this study have no conflicts of interest that may shape or limit the study.

Funding

This project was supported by [grant number 2016–VF–GX–K006], awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice.

References

Brand, S., & Price, R. (2000). *The economic and social costs of crime*. Home Office.

Center for Victim Research. (2019). *Research brief: Identity theft and fraud*. Office of Victim Services, U.S. Department of Justice. https://ncvc.dspacedirect.org/bitstream/item/1228/CVR%20Research%20Syntheses_Identity%20Theft%20and%20Fraud_Brief.pdf

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291–302. https://doi.org/10.1016/j.chb.2017.01.003

Cohen, M. A. (2005). *The costs of crime and justice*. Routledge.

Cohen, M. A. (2016). The costs of white-collar crime. In S. R. Van Slyke, M. L. Benson, & F. T. Cullen (Eds.), *The Oxford handbook of white-collar crime* (pp. 78–98). Oxford University Press.

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. https://doi.org/10.1016/j.jcrimjus.2010.07.007

Copes, H., & Vieraitis, L. M. (2012). *Identity thieves: Motives and methods*. Northeastern University Press.

Creswell, J. W. (2017). *Qualitative inquiry and research design: Choosing among five approaches*. Sage Publications.

Gies, S., Healy, E., Green, B., & Bobnis, A. (2020). From villain to victim: The impact of safe harbor laws on minors involved in commercial sexual exploitation. *Criminology & Public Policy*, *19*(2), 73–95. https://doi.org/10.1111/1745-9133.12497

Gies, S. V., Piquero, N. L., Piquero, A. R., Green, B., & Bobnis, A. (2020). Wild, wild theft: Identity crimes in the digital frontier. *Criminal Justice Policy Review*, 1–26. https://doi.org/10.1177%2F0887403420949650

Gilbert, J., & Archer, N. (2012). Consumer identity theft prevention and identity fraud detection behaviors. *Journal of Financial Crime*, *19*(1), 20–36. https://doi.org/10.1111/j.1745-6606.2009.01148.x

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. https://doi.org/10.1080/15564886.2016.1177766

Green, B., Gies, S., Bobnis, A., Piquero, N., Piquero, A., Velasquez, E. (2020). Exploring identity-based crime victimizations: Assessing threats and victim services among a sample of professionals. *Deviant Behavior*, 1–20. https://doi.org/10.1080/01639625.2020.1720938

Harrell, E. (2019). *Victims of identity theft, 2016, Bulletin*. United States Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://www.bjs.gov/content/pub/pdf/vit16.pdf

Harrell, E., & Langton, L. (2013). *Victims of identity theft, 2012, bulletin*. United States Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://www.bjs.gov/content/pub/pdf/vit12.pd

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

Holtfreter, K., Van Slyke, S., & Bloomberg, T. G. (2005). Sociolegal changes in consumer fraud: From victim-offender interactions to global networks. *Crime, Law, and Social Change*, *44*(3), 251–275. https://doi.org/10.1007/s10611-006-9006-8

Identity Theft Resource Center. (2020). *2019 end-of-year data breach report*. https://www.idtheftcenter.org/2019-databreaches/?utm_source=pressrelease&utm_medium=web&utm_campaign=Jan20_2019DataBreachReport

Lai, F., Li, D., & Hsieh, C. T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, *52*(2), 353–363. https://doi.org/10.1016/j.dss.2011.09.002

Milne, G. R. (2003). How well do consumers protect themselves from identity theft? *Journal of Consumer Affairs*, *37*(2), 388–402. https://doi.org/10.1111/j.1745-6606.2003.tb00459.x

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward and understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, *43*(2), 449–473. https://doi.org/10.1111/j.1745-6606.2009.01148.x

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs*, *38*(2), 217–232. https://doi.org/10.1111/j.1745-6606.2004.tb00865

Nagin, D. S. (2013). Deterrence in the twenty-first century. *Crime and Justice*, *42*(1), 199–263. https://doi.org/10.1086/670398

Payne, D., & Kennett-Hensel, P. A. (2017). Combatting identity theft: A proposed ethical policy statement and best practices. *Business and Society Review*, *122*(3), 393–420. https://doi.org/10.1111/basr.2017.122.issue-3

Piquero, A. R., Paternoster, R., Pogarsky, G., & Loughran, T. (2011). Elaborating the individual difference component in deterrence theory. *Annual Review of Law and Social Science*, *7*(1), 335–360. https://doi.org/10.1146/annurev-lawsocsci-102510-105404

Piquero, N. L. (2018). White-collar crime is crime: Victims hurt just the same. *Criminology & Public Policy*, *17*(3), 595–600. https://doi.org/10.1111/capp.2018.17.issue-3

Rebovich, D. (2009). Examining identity theft: Empirical explorations of the offense and the offender. *Victims & Offenders*, *4*(4), 357–364. https://doi.org/10.1080/15564880903260603

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. https://doi.org/10.1007/s12103-018-9447-5

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. https://doi.org/10.1177/0011128715620428

Ricci, J., Breitinger, F., & Baggili, I. (2019). Survey results on adults and cybersecurity education. *Education and Information Technologies*, *24*(1), 231–249. https://doi.org/10.1007/s10639-018-9765-8

Solove, D. J., & Citron, D. K. (2018). Risk and anxiety: A theory of data-breach harms. *Texas Law Review*, *96*(4), 737–786. https://texaslawreview.org/wp-content/uploads/2018/03/Solove.pdf

Sullivan, C. L. (2009). Is identity theft really theft? *International Review of Law, Computers & Technology*, *23*(1–2), 77–87. https://doi.org/10.1080/13600860902742596

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly*, *33*(5), 890–911. https://doi.org/10.1080/07418825.2014.994658

Tedder, K., & Buzzard, J. (2020). *Javelin 2020 identity fraud study: Genesis of the identity fraud crisis*. Javelin, Inc. https://www.javelinstrategy.com/coverage-area/2020-identity-fraud-study-genesis-identity-fraud-crisis

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. https://doi.org/10.1016/j.avb.2014.12.008

Wyre, M., Lacey, D., & Allan, K. (2020). The identity theft response system. *Trends and Issues in Crime and Criminal Justice*, *592*, 1–18. https://www.aic.gov.au/sites/default/files/2020-05/ti592_the_identity_theft_response_system.pdf

Zou, Y., Roundy, K., Tamersoy, A., Shintre, S., Roturier, J., & Schaub, F. (2020). *Examining the adoption and abandonment of security, privacy, and identity theft protection practices*. CHI, Honolulu. https://yixinzou.github.io/publications/chi2020-zou.pdf