Document Title:	Recover Me if You Can: Assessing Services to Victims of Identity Theft
Author(s):	Stephen V. Gies, Ph.D., Nicole Piquero, Ph.D.
Document Number:	256014
Date Received:	January 2021
Award Number:	2016–VF–GX–K006

Recover Me if You Can: Assessing Services to Victims of Identity Theft

DRAFT FINAL SUMMARY OVERVIEW

September 2019

Grant No. 2016–VF–GX–K006
Project Period: January 1, 2017, to September 30, 2019

Principal Investigators:

Stephen V. Gies, Ph.D.
Development Services Group, Inc.
7315 Wisconsin Avenue, 800 East
Bethesda, MD 20814
301.951.6600
sgies@dsgonline.com

Nicole Piquero, Ph.D.
University of Texas at Dallas
Program in Criminology
800 W. Campbell Road, AD42
Richardson, TX 75080
972.883.6268
npiquero@utdallas.edu

Submitted to

Jessica Highland
Grant Manager
National Institute of Justice
810 Seventh Street NW
Washington, DC 20531

This project was supported by Award No. 2016–VF–GX–K006, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect those of the Department of Justice.

Overview

The best way to deal with identity theft and the subsequent fraud is to take precautions to prevent it from occurring (e.g., Milne, 2003; Milne, Rohm, and Bahl, 2004; Piquero, Cohen, and Piquero, 2011). Nevertheless, like other crimes, there should be remedies to repair the harm caused by identity-based crimes. In the case of identity-based crimes, however, these processes have not been fully established. Moreover, there has been relatively little investigation into the strategies to repair the harm caused by identity-based crimes (Reyns and Randa, 2017; Payne and Kennett–Hensel, 2017).

Project Design

This multiphase project was designed to understand the effect and quality of services provided to victims of serious identity crime in the United States, to improve our understanding about victim experiences, and to identify the best ways of supporting victims who experience the ramifications of identity-based crime.

Phase 1

Phase 1 integrated existing data from the Identity Theft Supplement (ITS) administered as part of the Bureau of Justice Statistics' *National Crime Victimization Survey* (*NCVS*), with exclusive survey data collected in collaboration with the Identity Theft Resource Center (ITRC), to assess the impact of victim services on a variety of outcomes. The objective of this phase was to assess the impact of identity crime services.

Methodology

Data. The data for phase 1 were derived from two sources: 1) a survey of persons who requested assistance from the ITRC regarding a serious identity crime incident and 2) the Identity Theft Supplement (ITS) administered as part of the *NCVS.* The ITRC survey was designed to mirror several important items from the ITS to assess the outcome of serious identity crime incidents across the two samples 1 year after the initial contact with ITRC.

Sample. After removing all nonserious identity crime incidents (i.e., respondents who indicated only the misuse of an existing account) from the ITS, the sample was reduced to 6,320 respondents, with 287 subjects from the ITRC group and 6,033 subjects from the ITS group.

Next, because we are unable to randomly assign victimization, a propensity score matching (PSM) procedure was employed to make the two groups as comparable as possible by using the data available in both data sources. The covariates used in the matching procedure included key demographic variables that are likely to differ across the two samples: age, gender, race (white), married, income, and post–high school graduation.

Then we segmented the ITS sample into two groups. A no-treatment group consisted of those ITS respondents who did not report the identity crime incident and received no services. A treatment-as-usual group comprised those ITS respondents who reported the incident to any one of a variety of entities and thus received a diverse array of services. Each of these groups was compared with the subjects who contacted the ITRC.

Outcomes. The three groups were compared across five outcomes: 1) general problems, 2) financial problems, 3) physical health problems, 4) mental health problems, and 5) social problems. All items are summarized from a series of single items.

Analysis. The matching procedure yielded 5,162 untreated (ITS) and 106 treated (ITRC) cases. There were no significant differences (at p<.05) postmatching. A series of one-way ANOVAs was conducted to contrast the five outcomes across the three groups.

Findings

In five of these cases, the ITRC group reports more problems/experiences than either of the two ITS groups. Specifically, the ITRC respondents report more general problems, more financial problems, more employment/educational problems, more family/friend problems, and more physical health problems (see Table 1). In contrast, however, the ITRC subjects report fewer mental health problems.

Table 1. Three-Group Comparison of Problems/Experiences Attributable to Identity Theft Victimization Based on Reporting

Type of Problem	ITS No Contact	ITS Contact	ITRC
General Problems	.019 (.139)	.012 (.111)	.958 (.201)[a]
Financial Problems	.048 (.213)	.055 (.228)	.431 (.499)[a]
Employment/Educational Problems	.018 (.133)	.017 (.129)	.206 (.407)[a]
Family/Friend Problems	.064 (.245)	.035 (.183)	.386 (.490)[a]
Mental Health Problems	.890 (.312)	.825 (.379)	.763 (.427)[a]
Physical Health Problems	.265 (.442)	.225 (.417)	.527 (.502)[a]

[a]$p<.05$

Limitations. These findings should not be taken as an indication that the specialized customizable services provided by the ITRC to help victims of serious identity-based crimes are ineffective, as there were several limitations. First, subjects who contacted the ITRC and subsequently responded to our survey (M=3.21, SD=2.06) suffered significantly more (t [91.24] = –6.83, p = 0.00) losses than those in the ITS sample (M=1.72, SD=1.40). Thus, while we restricted the sample to victims of serious identity-based crimes, there appears to be a wide degree of variation in seriousness—even within those identity-based crimes identified as serious and for which we could not control. Further, it is likely that this degree of crime seriousness is exactly what prompted these individuals to contact the ITRC in lieu of or subsequent to other entities, resulting in a selection effect in which the negative findings are an artifact of the seriousness of the crime.

Moreover, it is reasonable to assume that more-serious cases take more time than less-serious cases to fully resolve. For example, nearly 40 percent of the ITRC respondents indicated that their case had not been cleared/resolved 1 year after the incident. Thus, it is possible that 1 year is simply an insufficient follow-up period to fully assess the impact of the ITRC services.

Another consideration is that there is, unfortunately, little to no available evidence regarding the victim's implementation of the ITRC prescribed action plan. Thus, it is possible that the findings reflect not a fundamentally flawed theory or practice by the ITRC but instead derive from missteps in execution (i.e., the clients did not follow through with the plan). In fact, qualitative data suggest that this is may be accurate.

Implications

This study contributes to a small but growing body of literature that suggests like victims of violent crime, identity-based crime victims suffer a considerable amount of emotional and physical stress (Golladay and Holtfretter, 2017). Moreover, the findings of this research provide policymakers, practitioners, domestic law enforcement agencies and the general public with several important implications for better addressing the investigation, prosecution, and remediation of identity-based crimes.

First, in the review of the literature we found a general lack of clarity in delineating the differences as well as documenting the connectivity between identity theft and the subsequent fraud perpetrated with that stolen information. As noted earlier, the thieving of PII is an antecedent to the crime of fraud, but these terms are often used interchangeably. Such lax language causes definitional problems that in turn likely leads to a misrepresentation regarding the nature of the criminal acts, victim experiences, and the need for law enforcement–based investigations, and victim remediation practices.

For example, compared to fraud, the thieving of PII by itself has no intrinsic monetary value. This basic difference influences how the victim may perceive the crime which in turn sets off a ripple effect throughout the criminal justice process. In most cases, the stolen PII is simply a piece of paper or a file stored in an electronic format. As such, the victim may perceive the harm suffered from identity theft as insignificant, and the crime therefore as minor. As a result of the lack of perceived value and the degree of ambiguity surrounding the crime, identity theft is often met with apathy by both the victim and law enforcement officials. However, the reality of the matter is that the value of one’s identity far exceeds the cost of the paper it's printed on or the file space in which it is stored. The important point here is that at the moment when it is discovered that the PII is used fraudulently to obtain something of worth, it suddenly takes on a tangible value. Moreover, once the value is established, it stands to reason that the crime will be perceived as more egregious in nature, and those impacted are more likely to seek help in resolving it (Baumer and Lauritsen, 2010; Skogan, 1976). This is consistent with studies on victims that have consistently found that when a crime is perceived to be more serious in nature, the victim is more likely to report it to the police (Reyns and Randa, 2017; Reyns and Englebrecht, 2013; Gottfredson and Hindelang, 1979).

The important policy implication derived from a clearer understanding of the differences between these crimes is that a paradigm shift is required in which policymakers, practitioners, domestic law enforcement agencies and citizens themselves begin to value PII as much as those who steal the information do and thus put more emphasis on the original theft of the PII as opposed to only the subsequent fraud. Such an emphasis could enable victim service providers like the ITRC to more proactively support victims of identity theft before their information is used for identity fraud and, ideally, limit the impacts of the theft on financial losses or the misuse of medical or government benefits (Ricks and Irvin–Erickson, 2019).

A second important finding from this research is that individuals who suffer from serious identity fraud face more formidable problems than individuals who are victims to less serious crimes and consequently require more intensive services. This finding has important policy implications in how service providers can provide the quality of care to identity crime victims. One potential avenue that providers may wish to investigate is the use of case triaging. Although the concept of triage applies to all resource allocation issues, it is most commonly discussed in the field of medicine (Koenig and Schultz, 2010). In essence, triage systems are used in medical-care systems to determine who gets care first when there are more people who need care than there are available resources to care for them. Such a system ensures the patients who need lifesaving treatment or other immediate attention are seen before those who may be presenting for a less serious condition.

A similar system could be established with identity-based crimes. As we noted earlier, identity-based crimes are rising almost yearly. This rise, coupled with the fact that there appears to be quite a large gap in the degree of seriousness both across the broader spectrum of identity-based crimes and even within the narrower scope of those crimes identified as serious, suggests that triaging cases into high-, medium-, and low-need-based case management structures may be a more efficient use of resources and ultimately provide higher quality of care to a wider array of victims.

Finally, while this study was more focused on the remediation needs of victims, the findings also have some important implications for law enforcement investigations of identity-based crimes as it relates to victim satisfaction. Specifically, the cross-jurisdictional nature coupled with the highly technological aspects of identity-based crimes makes it difficult for local law enforcement to effectively address the complex nature of these crimes. For these reasons, investigating cyber-crime has traditionally fallen under the purview of the FBI, with little involvement from local police (Police Executive Research Forum, 2017). As a result, we believe there is a fundamental need to restructure the reporting of, investigation, and response to identity-based crimes in order to produce a more focused, yet collaborative approach that can yield more capability and capacity than local law enforcement to effectively deal with these crimes. For example, one potential way to do this is by expanding the use of the Utah Model of Operation Wellspring, an FBI initiative through which state and local law enforcement officers are embedded in and trained by the FBI (Police Executive Research Forum, 2017). The bottom line is that the criminal justice system must reevaluate the processes by which they are dealing with identity-based crimes in order to match the way identity thieves operate in the digital world.

PHASE 2

Phase 2 utilized qualitative data collected from experts in the field, to expand our understanding about identity crime victimization and the interaction between individuals and organizations. Specifically, in this phase we conducted focus groups with professionals working in identity crime victim services, including private investigators, fraud examiners, victim service professionals, and executives of firms providing victim and protection services. There were two primary questions that structured the focus groups:

1. How do experts in the field of identity theft define the victims of identity theft?
2. How can the services for victims of identity theft be improved or expanded?

Methodology

Participant Recruitment. In coordination with the ITRC, we made an initial list of 10 professional meetings that had a direct or indirect focus on identity-based crimes. Of the 10 organizations that were contacted, 2 agreed to participate: the Association of Certified Fraud Examiners and the National Center for Victims of Crime. In addition, we conducted focus groups with professionals who regularly engaged with the ITRC but who are not ITRC staff.

Sample. The recruitment process produced a total of 50 participants, across seven focus groups, with 45 people being involved in focus groups and 5 electing one-on-one interviews.

Data Collection. A focus group interview guide was used to prompt the 1-hour discussion. All focus groups were audio-recorded, with the research team also taking notes and producing an initial set of field notes. The audio recordings were transcribed.

Analysis. The research team used a deductive coding scheme. All transcripts were coded by the principal investigator and a research assistant, using NVivo to manage the coding process and to enable interrater reliability verification and examination.

Findings

Defining the Victim. Focus group participants were asked by the facilitator at the start of each session, "Who is the victim when there is identity theft?" This question elicited a consensus view that there is not a single victim within incidents of identity crimes. Participants identified several victims, including the businesses that have been breached, the businesses that have been defrauded, the company staff who have been defrauded, shareholders, family members associated with the breached record file, fellow customers of firms, and the individuals whose personally identifiable information (PII) had been taken. The results of this phase suggest an expansion of the dual model of identity crime victimization to a new tri-partite model that includes not only the 1) individual whose information was stolen and 2) the organization that will ultimately be defrauded, but also 3) the organization or entity that is the subject of an intentional data breach leading to the exposure or the theft of protected information.

Another key focal point of the discussion on victims highlighted those who are most vulnerable and the least able to respond once their information has been taken. This manifested as concern about foster children, 13- to 18-year-olds, seniors, victims of domestic violence, and undocumented immigrants.

Improving Services for Victims. Participants were specifically asked about which types of services could be improved or expanded to better support victims as they sought to address the ramifications of their victimization. These conversations were eclectic and varied across the focus groups. Participants did, however, consistently emphasize the general lack of services for victims, including educational programming that may aid in the prevention of identity crimes.

The Next Big Thing. Participants were asked to identify where they see the future of identity-based crimes going and what services these future victims may need. The dominant area of concern, expressed across all focus groups was the rise of synthetic ID[1]s, as seen in this quote:

> Even though synthetic IDs are starting to manifest, we haven't seen them reach peak yet. Right? This is going to be a big, big problem in 8 to 10 years.

Implications

Services for individuals who and organizations that have been victims of identity theft and associated identity fraud will continue to be needed, with a likely increase in the expertise required to fully support victims as the sophistication of the criminal actors increases. As a result, we believe that victim services for identity-based crimes should be tailored to the type of identity crime incident, provided by an entity with the expertise and sophistication required to address the issue, and able to be sustained over time. Moreover, as with many consumer-based crimes, there is a significant need for regular, continued education and efforts to raise awareness for evolving threats and prevention methods.

[1] A synthetic identity is one in which a criminal combines real and fake information to create a brand-new identity. For example, real name and birthdate lifted from an online account may be combined with an address made up on the spot, a Social Security number (SSN) stolen via a data breach and an email address that has not been used in years. This information is then used to open fraudulent accounts and make fraudulent purchases. https://www.idtheftcenter.org/synthetic-identity-theft-the-frankenstein-of-identity-crime/

Finally, there is a very real sense that everyone has already been victimized, and that the challenge of providing services within an environment of population wide victimization simply lacks precedent or clear conceptualization. Our tri-partite model of victimization adds to our understanding of identity theft by providing a more precise and complete explanation of how victimization occurs, which we hope, through application and further development, can help improve victim services both for organizations and individuals.

PHASE 3

Phase 3 of the project was designed to understand the service delivery of the ITRC victim call center through interviews with victims who had used ITRC services. It concentrated on three key research questions:

1. How do victims of serious identity-based crime describe their victimization experience?
2. Do victims of serious identity-based crime who receive victim support services from a nonprofit view those services as helpful or useful?
3. What areas of need remain for victims of serious identity-based crimes who have used some victim services?

Methodology

Participant Recruitment. Subjects were recruited from a list of 70 potential interviewees provided by the ITRC to the research team. The sample included clients who were willing to be contacted for follow-up research. For each potential interviewee, we used three waves of telephone-based recruitment, leaving a detailed message each time. Of these 70 potential interviewees, 8 contained out-of-date information, 22 did not respond, 15 declined to participate, and 8 agreed to participate but failed to appear for the scheduled interview.

Sample. Of the 17 completed interviews, 7 were female and 10 were male. Out of respect for their prior victimization, we did not ask any additional demographic questions. They had experienced a broad range of identity-based crimes, had different types of resolution statuses, and had each used multiple types of victim services.

Data Collection. Each interview was completed on the telephone and was audio-recorded. The 45–60 minutes interviews followed a semi structured interview guide, and all interviews were completed by one interviewer with extensive experience in qualitative research. Following each interview, a member of the research team transcribed a de-identified audio file.

Analysis. The completed transcripts were uploaded to NVivo to enable the coding process. Both open and closed codes were used. Closed codes were based on existing literature on victim services and focused on the sequential experiences of victims. These codes included discovery of the incident, initial response to the incident, seeking services for remediation, satisfaction with services, resolution status, and long-term impacts. During the coding process, open codes were created to provide thematic grouping and analysis within each of these broader, closed codes. To ensure intercoder reliability, two members of the research team coded all transcripts. The team members reviewed all quotes where 80 percent agreement among the coders was not achieved, came to consensus on the appropriate code, and recoded.

Findings

Discovery of the Incident. Victims discovered the identity-based crime in a variety of ways. Data breach victims were notified by the point of potential breach (i.e., banks, credit cards, stores, etc.). In non–data breach cases, victims were alerted when their application for government benefits (Social Security, income tax forms) was denied, they were stopped by law enforcement in a case of mistaken identity, or they found fraudulent activity via self-monitoring.

Initial Response to the Incident. Most victims initially felt fearful, angry, violated, and anxious. The emotional tumult held throughout the experience as well, as one interviewee felt the entire process was "kind of {an} emotional rollercoaster."

Seeking Services for Remediation. Many respondents immediately tried to search for remediation methods over the Internet. For victims of financial fraud, the initial response was to contact their financial institution. Few respondents turned to law enforcement. Otherwise, participants sought out services that aligned with the type of identity crime they experienced.

Satisfaction With Services. Respondents shared varying levels of satisfaction with services, depending on the type of identity-based crime they experienced and whether it was

This resource was prepared by the author(s) using Federal funds provided by the U.S. Department of Justice. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

resolved. Victims reported the most helpful services were the ITRC, law enforcement, and legal services. However, many victims indicated that nothing was particularly helpful.

Resolution of the Incident. In most cases of financial fraud, victims indicated the incident was fully resolved by the financial institutions. Nevertheless, several victims felt their cases were not fully resolved, because of hurdles with law enforcement. In addition, many victims still echoed the fear that their information is still "out there."

Long-Term Impacts. Generally, most victims reported checking their financial accounts more often to watch for any indication of fraud. Additionally, many victims reported lowered trust in financial and government institutions. For example, one interviewee acknowledged,

> I guess it's made me into a little bit of a skeptic as far as, you know, entering any information, not just with taxes but just my information online.

Implications

One unique element to this project was the inclusion of victims who experienced identity theft and a variety of subsequent fraud crimes (e.g., governmental, criminal, financial). To our knowledge, no existing study has interviewed victims of each type of fraud in a single study.

From these comparisons, we learned of both similarities and differences between financial and other types of identity-based fraud victims. All victims we interviewed had similar experiences with having to manage the negative emotional impact of their victimization, sought initial information about remediation advice through Internet searches, engaged law enforcement after being instructed to do so by an intermediate organization, and reported making small adjustments to their personal behaviors to prevent subsequent fraud. However, victims of identity-based crimes that were not primarily financial had a much more negative experience with seeking support or assistance from the defrauded organization, reported lower levels of issue resolution, and were more likely to know their perpetrator.

Finally, it seems likely these observed differences between financial and nonfinancial identity fraud victims should inform the type of support and level of assistance that these different victim groups need. As such, these results provide additional support that a tiered system of support is vital for identity-based crime victims, and that a tiered system can ensure both efficient use of resources and effective support for victims as they work to remediate the adverse impacts of their identity-based victimization.

Addendum

The ITRC produces a monthly data breach newsletter for 3,607 subscribers. Though data breaches were not the direct subject of this study, their relationship to identity theft incidents became clear during our first round of focus groups. Thus, we felt the opportunity to poll industry professionals on how they view and address data exposure events, and the subsequent identity theft incidents would add a new and timely dimension to the study.

Findings

We received surveys from 75 unique respondents. Of these 75 respondents, 45 did not consent to take part in the survey. Thus, the final sample included 30 respondents. Due to the small sample, we simply review the descriptive statistics from the sample.

Respondents worked across a host of industries—including financial (38.5 percent), business (15.4 percent), education (15.4 percent), and government (7.7 percent)—and represented predominantly (37.9 percent) large organizations (500+ employees). Regarding their satisfaction with the amount of resources their organization invests in cyber security, well over half of the sample (61.6 percent) reported being satisfied or very satisfied. Regarding specific cyberattack experiences, most respondents indicated that their organization had never experienced an attack (68 percent) or exposure event (80 percent).

Every respondent (100 percent) indicated it was both the organization and the individual's responsibility to protect PII, but well more than half (61.9 percent) felt their organization did a good job protecting PII. In an interesting contrast, 68.2 percent of the respondents reported their industry in general did not do enough to protect PII.

Implications

There appears to be some ambiguity concerning the nature of an organization's responsibility in protecting individual-level PII. This issue bears further investigation.

REFERENCES

Baumer, E., and Lauritsen, J. (2010). Reporting Crime to the Police, 1973-2005: A Multivariate Analysis of Long-Term Trends in the National Crime Survey (NCS) and National Crime Victimization Survey (NCVS). *Criminology*, 48, 131-185. https://doi.org/10.1111/j.1745-9125.2010.00182.x

Golladay, K. and Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims and Offenders: An International Journal of Evidence-based Research, Policy, and Practice*, 12(5), 741-760.

Gottfredson, M.R. and Hindelang, M.J. (1979). A Study of the Behavior of Law. *American Sociological Review*, 44(1): 3-18.

Koenig, K.L. and Schultz, K.H. (2010). *Koenig and Schultz's Disaster Medicine: Comprehensive Principles and Practices*. Cambridge University Press.

Milne, G.R. 2003. How well do consumers protect themselves from identity theft? *Journal of Consumer Affairs* 37(2):388–402.

Milne, G.R., Rohm, A.J., and Bahl, S. 2004. Consumers' protection of online privacy and identity. *Journal of Consumer Affairs* 38(2):217–32.

Payne, D., and Kennett–Hensel, P.A. 2017. Combatting identity theft: A proposed ethical policy statement and best practices. *Business and Society Review* 122(3):393–420.

Piquero, N.L., Cohen, M., and Piquero, A.R. 2011. How much is the public willing to pay to be protected from identity theft? *Justice Quarterly* 28(3):437–59.

Police Executive Research Forum. (2017). *The Utah Model: A Path Forward for Investigating and Building Resilience to Cyber Crime.* Washington, D.C.: US Dept of Justice, Office of Justice Programs, Bureau of Justice Assistance.

Reyns, B.W. and Englebrecht, C.M. (2013). The Fear Factor Exploring Predictors of Fear Among Stalking Victims Throughout the Stalking Encounter. *Crime and Delinquency*, 59(5): 788-808.

Reyns, B.W., and Randa, R. 2017. Victim reporting behaviors following identity theft victimization: Results from the *National Crime Victimization Survey*. *Crime & Delinquency* 63(7):814–38.

Ricks, A., and Irvin–Erickson, Y. (2019). *Identity theft and fraud (Research Brief).* Washington: Center for Victim Research. Retrieved from https://ncvc.dspacedirect.org/bitstream/item/1228/CVR%20Research%20Syntheses_Identity%20Theft%20and%20Fraud_Brief.pdf

Skogan, W.G. (1976). Citizen Reporting of Crime: Some National Panel Data. *Criminology*, 13(4):535-549.