Testimony for the
House Committee on Ways and Means
Subcommittee on Social Security
Field Hearing on
Social Security Numbers and Child Identity Theft

Lynne M. Vieraitis, Ph.D.
Associate Professor of Criminology
University of Texas at Dallas

Qualifications

I have a PhD in criminology from Florida State University and am an associate professor of criminology at the University of Texas at Dallas. My research focuses on identity theft, specifically on those who choose to commit it, and has been supported by the National Institute of Justice.[1] I have published frequently in peer-reviewed journals, presented research findings for government agencies, including the Federal Trade Commission and the National Institute of Justice, as well as for various professional conferences and news media outlets. My co-author (Heith Copes) and I have a book, *Identity Thieves: Motives and Methods*, forthcoming from Northeastern University Press in spring 2012.

Summary

According to the most recent estimates from the National Crime Victimization Survey (NCVS), approximately 12 million persons or 5 percent of all persons age 16 or older were victims of at least one type of identity theft during 2006-2007.[2] These estimates are slightly higher than other estimates including those from the Federal Trade Commission (FTC), which estimates 8 million victims over the age of 18 years.[3] Unfortunately, as with most frauds, it is difficult to ascertain the true picture of the pervasiveness and costs of identity theft with the available data. One reason for the differences in estimates is that not all agencies define identity theft in the same way. For example, the NCVS considers credit card fraud in its estimates of identity theft, but other agencies do not. Since there is no universally accepted definition of identity theft we find differences not only on the estimates of the prevalence and costs of identity theft but also on the portraits of both victims and offenders. Another reason for the differences in estimates is that identity theft is likely an underreported type of crime. Moreover, underreporting by victims may be associated with the type of theft that occurs. Victims whose information is stolen and used by someone they know are less likely to report than those victimized by strangers. Some victims, as in the case of child identity theft, may not know they

---

[1] National Institute of Justice, Office of Justice Programs, U.S. Department of Justice (Grant No. 2005-IJ-CX-0012).
[2] Bureau of Justice Statistics. 2010. *Identity Theft Reported by Households, 2007—Statistical Tables.* Washington, DC: U.S. Government Printing Office
[3] Federal Trade Commission. 2009. *Consumer Sentinel Network Data Book for January to December 2008.*

have been victimized. Other differences may be attributed to the population from which the agency or company is sampling with some agencies relying on reports from victims, other agencies relying on local law enforcement data, and others on data from their own customers.

The problem with estimating prevalence of identity theft is exacerbated when the victims are children. Child victim identity theft can go unnoticed for many years; if not decades. It is often not until the victim begins to apply for credit that the theft or fraud is discovered. Additionally, if the child's information is being used by a parent, step-parent, sibling, or other family member, the likelihood that it is reported is much lower than if the child's information is being used by a stranger. Thus, the extent of child identity theft and whether it is growing is difficult to assess with existing data. The FTC has recently reported an increase in the number of child identity theft cases reported to their agency, but caution must be used when interpreting these results. It is possible that people are simply more likely to report identity theft than in previous years, are more aware of it, or shifts in the population age 18 years and older and the numbers applying for credit, including student loans may have changed. According to existing research, child identity theft makes up approximately 3 to 8 percent of all identity theft cases.[4]

What we do know is that there are millions of victims every year, there are billions of dollars lost (estimates range from $16 billion to $50 billion per year), and we know that US citizens are very concerned about identity theft and fraud.[5] Information is available from both public and private agencies that collect data on identity theft and suggest that identity theft is becoming more common and more costly. Yet, while much has been written about victims, prevention techniques, and state and federal legislation, little research has devoted attention to studying those who engage in identity theft.[6] Our research begins to fill this gap. By examining the perspectives of offenders, our goal was to produce a more comprehensive picture of identity theft, one that would offer suggestions for how identity theft might be better controlled.

The research I conducted with my colleague, Dr. Copes from the University of Alabama at Birmingham, is based on in-depth, face-to-face interviews with fifty-nine identity thieves.[7] The interviews were conducted with men and women serving time in federal prisons across the United States for violating the federal statute for identity theft (18 U.S.C. § 1028).

---

[4] Kresse, William, Kathleen Watland, and John Lucki. 2007. *Identity Theft: Findings and Public Policy Recommendations.* Final report to the Institute for Fraud Prevention http://www.sxu.edu/Academic/Graham/Documents/identitytheft_study.pdf).;Pontell, Henry N., Gregory C. Brown, and Anastasia Tosouni. 2008. Stolen Identities: A Victim Survey. In Crime Prevention Studies: Identity Theft and Opportunity, edited by Graeme Newman and Megan McNally. New York: Criminal Justice Press.

[5] Unisys. 2009. *Unisys Security Index Reveals High Concern among Americans about Government and Business Protection of Private Data.* Retrieved on January 20, 2010 (http://www.unisys.com).

[6] Most of what we know about identity thieves comes from closed case reports, either from the U.S. Secret Service or local police departments (e.g., Kresse et al; Allison, et al.). Allison, Stuart, Amie Schuck, and Kim M. Lersch. 2005. "Exploring the Crime of Identity Theft: Prevalence, Clearance Rates, and Victim/Offender Characteristics." *Journal of Criminal Justice* 33:19–29.

[7] We interviewed 65 individuals but six offenders claimed to be innocent of all charges by either denying they had taken part in or had knowledge of the identity theft (if they had co-defendants). Our findings are based on interviews with 59 identity thieves.

The motivation for our research was based on our belief that it is important to gain the offender's perspective when trying to improve our understanding of crime and to design policies aimed at curtailing it. Although gathering accurate information from victims, law enforcement officers and prosecutors is essential to understanding identity theft, we recognize that information from the identity thieves themselves also provides an important piece to the puzzle. With that goal in mind, we questioned identity thieves about their lives and crimes. We wanted to know: who engages in identity theft? Why do they choose identity theft instead of other types of crime? How do they organize themselves to commit their crimes? How do they acquire a victim's personal identifying information? What do they do with the information? What risks they associate with their crimes? What steps they take to avoid detection and capture? How their crimes eventually come to an end? By asking identity thieves to answer these questions in their own words, we hoped to better understand their motives for choosing identity theft, the methods they use to commit it, and the meaning all of this has for developing informed theory and policy.[8]

What We Learned

Who? Although I am often asked to describe the "typical" identity thief, it is difficult to paint a portrait of a "typical" one. Those we spoke with came from all walks of life and had diverse criminal histories. Their backgrounds ranged from the upper to lower class, the unemployed to the employed, from day laborers to professionals, middle-school dropouts to college graduates, and from those with lengthy criminal histories to "first timers." They ranged in age from 23 to 60 with a mean age of 38.

We found that some thieves worked alone, while others were involved in teams of up to 30 members. Some were fueled by their addictions to illegal drugs, while others simply wanted to live above their means. The diversity in their backgrounds and current lifestyles influenced the ways in which they chose to carry out their crimes. Our interviews revealed that identity thieves relied on three primary organization schemes to carry out their crimes: loners, street-level identity theft (SLIT) rings,[9] and occupational teams.

How? Twenty-four percent of the offenders in our sample were typed as loners. They typically used the personal information of others to open credit card accounts or secure bank loans. Many of these offenders claimed that they tried to make payments on the accounts to prevent victims from discovering the fraud, but eventually repayment became impossible. In some cases, they used information available to them for their place of work and in some cases they used the information of family members, including their own children, or friends. In one case, a woman employed at a mortgage company used client information to obtain personal bank

---

[8] Copes, Heith and Lynne M. Vieraitis. *Identity Thieves: Motives and Methods.* Boston: Northeastern University Press. (In Press).

[9] Pavlicek, Bruno. 2005. "Identity Theft and slit Rings: An Unrecognized yet Growing Cancer." *Crime and Justice International* 21:29–33.

loans. In another, the offender used the personal information of deceased family members to open bank accounts, get credit cards, and apply for a HUD loan. One thief used the personal information of her children and mother to take out bank loans. Other thieves used more sophisticated and elaborate schemes to dupe strangers into revealing their information. For example, one set up fake employment sites with applicants willingly supplying all their personal information, another used obituaries to access information and file fraudulent Medicare claims.

The majority of the identity thieves we interviewed operated in teams characterized by an elaborate division of labor in which members perform different roles depending on their knowledge and skills. There was considerable diversity among this group and necessitated the division of teams into two types: street level identity theft rings and occupational teams. SLIT rings and occupational teams share many similarities but they differ noticeably in the methods they use to steal and convert information.

SLIT rings relied on numerous methods to acquire and convert information. Some rings relied on an individual employed by a company that possessed legitimate access to names and personally identifying information of company or agency clients to get information. Others targeted residential and commercial mailboxes to steal checkbooks, bank statements, or medical bills. For most SLIT rings in our sample, the person supplying the information was a street-level criminal—typically engaged in drug sales, robbery, burglary, or other street crimes—who sold the information to the ringleader. This information included drivers' licenses and social security cards. Some rings obtained information from willing acquaintances, friends and family members in exchange for a fee. The "victim" would then wait a while before reporting the "theft." In one case involving a well-known gang, the ringleader paid someone to purchase birth certificates from drug addicted mothers. The birth certificates of US children were used to gain passports so the children of gang members and their associates could enter the country "legally."

After obtaining a victim's information, offenders applied for credit cards in the victims' names, opened new bank accounts and deposited counterfeit checks, withdrew money from existing bank accounts, applied for loans, or opened utility or telephone accounts. Because such transactions all require some form of official identification, the false identity document source played an important role. To produce these documents, teams recruited employees of state or federal agencies with access to social security cards or birth certificates, which could then be used to order identification cards. While thieves could use fraudulent information to obtain identification cards through conventional channels, it also was possible to manufacture false cards using rogue employees of state departments of motor vehicles, or through street hustlers who had managed to obtain the necessary equipment. (Some offenders specialize in the production of false identification cards for use by underage students to purchase alcohol and by illegal immigrants to apply for jobs.) For slit rings, the most common strategy for converting information into cash was by applying for credit cards, both from major card issuers and individual retailers. Offenders could use a stolen identity to order new credit cards, or to issue a duplicate card on an existing account. With these cards in hand, they could buy merchandise for their own personal use, for resale to friends and acquaintances, or to return for cash.

Another common strategy for converting information into cash or goods involved producing counterfeit checks. Offenders typically used such checks to open new bank accounts, or deposited them in the victim's existing account before withdrawing cash. Counterfeit checks also could be cashed at grocery stores, or used to purchase merchandise and pay bills.

Members of occupational teams used their legitimate place of employment to steal information and convert it to goods or cash, acting almost exclusively with fellow employees to commit their crimes. In mortgage fraud schemes, the majority of players were employed at the same company or at companies that worked together to process home loans. In cases involving workers at a state department of motor vehicles, an outside source provided information to employees, who then issued state identification cards or driver's licenses that were subsequently used to carry out identity thefts. The thefts committed by occupational teams typically involved theft on a larger scale, characterized by numerous victims and high dollar losses than those committed by SLIT rings or loners.

Why? In addition to the question, "how do they do it?" I am often asked "why they do it?" The simple answer is quick and easy money. Data from victims and law enforcement suggests that identity thieves are motivated by a desire for money, to avoid authorities, or to avoid using their own information to set up utility or cell phone accounts. These are all true, but merely skim the surface of offenders' motivations. It does not, for example, tell us why they choose identity theft instead of legitimate work or even other types of crimes. What we found was that offenders engage in identity theft because they see it as financially and emotionally rewarding, believe it to be relatively low in risk, and find it is easy to justify or excuse their actions. In short, they perceive the rewards to be "high" and the risks "low."

Consistent with research on persistent offenders, the identity thieves we spoke with were confident in their abilities to profit from their crimes and to avoid detection. Most didn't focus on the risks of crime, but all actively engaged in strategies to reduce the likelihood of detection. They spoke about the many ways in which they minimize the risk of detection by victims, financial institutions, and law enforcement. Briefly, they reduced the number and amount of transactions conducted with each identity, selected the right times, places and people to get and use information, and took steps to "blend in."

Policy Recommendations

The crime of identity theft includes the acquisition of information as well as the use of that information for ill gotten gains including avoiding bill collectors, law enforcement, opening bank accounts, taking out home, car and personal loans, etc. Thus, there are several points along the crime continuum that can be addressed through policy. The challenge for policymakers and law enforcement is identifying policies and strategies that can target these weak points while at the same time allowing businesses and customers to conduct transactions.

Several suggestions for prevention are provided that draw upon several well-known situational crime-prevention techniques, including increasing the effort the offender must use to acquire and convert information, increasing the risks of getting caught, and removing excuses that offenders may use to justify their crime. Each of these strategies is more effective when they can be catered to highly specific forms of identity theft (e.g., child identity theft vs. adult identity theft and identity theft committed by loners vs. those committed by SLIT rings).

- *Increase the Effort and Risk of Obtaining Information*
    - Educate consumers on ways to protect their identity. State and federal policymakers have made tremendous strides in passing legislation that attempts to reduce the opportunities for would-be identity thieves to steal information. We need to continue to promote awareness of identity theft especially to citizens who don't necessarily have easy access to information.
    - Educate consumers on what to do when their identity is stolen and when it is used.
    - Encourage individuals to report their victimization to law enforcement, federal agencies, and businesses. Require businesses to report theft of data in a timely manner.
    - Reduce unsafe business practices. It is essential that businesses and agencies whose employees are responsible for the handling of such information be trained properly on the best practices for protecting information and management should establish a set protocol for checking to ensure that employees are following these practices. Institutions that house data on children, including hospitals and schools, should be vigilant. Special populations, such as children in the foster care system should be issued an identification number when placed in a home. The social security number should only be used by the state agency to verify eligibility and issue benefits.
    - To the extent law enforcement and other agencies can reduce the number of individuals involved in other street crimes including, drug use, sales, and manufacturing, burglary, robbery, prostitution, etc. there will be fewer sources of information from which identity thieves can buy information.

- *Increase the effort and risk of converting information*
    - Educate and encourage victims to report their victimization immediately to all appropriate agencies. If someone is victimize by burglary, take steps with credit agencies just in case the offender has your information.
    - Reduce unsafe business practices and develop strategies to ensure employees are following the rules. Offenders say the scariest and riskiest part of identity theft is going to the bank or store to commit fraud. They know which stores check identification and under what conditions. It is important that all stores, banks, and other financial institutions follow policies carefully and consistently.
    - Systems should be in place to verify and alert credit granting agencies, for example, that a social security number is issued to a person under the age of 18 years.

- *Increase the risks of getting caught*
    - Encourage local law enforcement to devote time and energy to investigating identity theft.
    - Encourage investigators to consider that identity theft may be part of other street crimes such as residential burglaries, theft from motor vehicles, shoplifting, etc.
    - Develop strategies based on behavioral cues that businesses can incorporate into training employees. In most cases, the identity thieves regardless of how they acquired information were easily able to convert the information into cash or goods.
    - Consider expanding the definition of child abuse and neglect to include financial abuse and fraud.

What Remains to be Learned

We need better and consistent measures of identity theft and fraud, specifically those frauds that target children. We need more systematic data collection from agencies responsible for personal information, agencies that use personal information in legitimate business practices, from law enforcement agencies at local, state, and federal levels, from victims, and from those who know most about how and why identity theft occurs—the identity thieves themselves. From offenders, we need to know how they adapt to changes in technology and business practices, how they have responded to changes in legislation designed to prevent them from accessing information and converting that information into cash or goods and whether they target children and if so, why they do so. Child identity theft is harder to detect, harder for victims to report if they are victimized by someone they know, and harder to address particularly with our lack of data. It may occur over a longer period of time than other forms of identity theft making it not only more difficult to discover but more difficult for the victim to restore their "good name." It is important when developing policy that we clearly identify and understand the problem we are dealing with. Child identity theft that is facilitated by family members poses a different challenge for policymakers and law enforcement than does theft by organized criminal groups.