Summer 2011

Prevention of Identity Theft: A Review of the Literature

Portland State University. Criminology and Criminal Justice Senior Capstone

Prevention of Identity Theft

Summer 2011

A Review of the Literature

Portland State University

Criminology and Criminal Justice Senior Capstone Class:

Michelle Arno, Shari Burns, Karen Carlson, Chris Ehle, Elizabeth Everett, Shaun Feero, Andy Hasenkamp, Kirstina Imes, Eric Kilcup, Amanda Leavitt, Joseph Lim, Jerrod Marshall, Jessica Marshall, Rick Milteer, Bryan Morris, Elizabeth Perez, Jennifer Petty, Crystal Pleninger, Zainab Priest, Jonathan Ridge, Lindsay Roberson, Anna Rowley, Samantha Serpa, Jeremy Tallmadge, Timothy Veling

Supervised by: Dr. Debra Lindberg

Table of Contents

Introduction..... 3

Definition and Prevalence..... 3-4

Victims…….4-5

Offenders…….5-6

Modus Operandi…….6-7

Prevention……..……..7-8

Conclusion……..……8-9

References……..10-11

Introduction

With advances in technology and increases in impersonal electronic transactions, identity theft IT) is becoming a major problem in today's society. One may ask why IT is growing in America. The answer is simple, as a review of literature reveals: IT is extremely hard to detect, prevent, and prosecute.

There are many ways people can protect themselves, their identities and secure their personal information; many do not concern themselves with this knowledge, however, until they become victims of this crime, themselves. With advances in technology, offenders are often turning to new methods to access information and use it for financial gain or to hide their true identity. This is why it is imperative for people to be aware of these threats and use caution when providing personal information to anyone to protect themselves from becoming victims of IT.

This report seeks to provide a more clear understanding of the definition of IT, its prevalence, characteristics of the victims and offenders, as well as the myriad methods used to commit IT crimes. In addition, strategies for preventing IT will be discussed, including but not limited to transaction awareness and inter-agency collaboration

Definition and Prevalence

The expansion of the internet and the popularity of online purchasing and banking have evolved into a billion dollar industry. In 2007, online sales boomed to $136.4 billion, a 19% increase over 2006 (Reisig, Pratt, and Holtfreter, 2009, p.369). After a review of existing literature on IT, six articles were identified that discussed definitions and prevalence of IT.

As described by the U.S. Department of Justice (2010b), IT is:

> [The] unauthorized use or attempted use of an existing account, such as a credit/debit card, checking, savings, telephone, online, or insurance account, unauthorized use or attempted use of personal information to open a new account, such as a credit/debit card, telephone, checking, savings, loan, or mortgage account, or misuse of personal information for a fraudulent purpose, such as getting medical care, a job, or government benefits; renting an apartment or house; or providing false information to law enforcement when charged with a crime or traffic violation (p.2).

It is estimated there have been over 15 million victims of IT resulting in nearly $745 million in losses to both consumers and businesses (Newman, 2004, p.5). Maintaining a level of integrity has also come into question as more people are utilizing the internet to take online courses and are providing personal information to gain acceptance to organizations or employment. Businesses are also at risk of losing profits. For example, illegal music or movie

downloads have created an avenue for typical consumers and cyber thieves alike (Selwyn, 2008, p.447).

There were over half a million consumer complaints filed with The Federal Trade Commission (FTC) in 2003. Consumers reported that they were victimized during the course of everyday life (e.g., the top categories are internet auctions - 15%, shop at home/catalog sales - 9%, and internet services and computer products - 6%). In 2003, fraud victims reported losses of $437,463,950, with a median loss of $228. Internet related fraud amounted to $200,000,000 in 2003 with a median loss of $195. Recovery of any of these funds is extremely low if any, in many instances. The most common ID theft complaint was credit card fraud, followed by phone or utility fraud; bank fraud; employment related fraud; government, document or benefit fraud; and loan fraud (FTC, 2004, p.3). These data also suggest IT rose from 86,212 in 2000 to 214,905 in 2003: nearly a 250% increase (p.9).

Victims

We read seven scholarly articles which provided information regarding victims of IT. The information from these articles included characteristics of those most likely to become victims and victim reporting information.

The simple act of using the internet creates a potential victim. According to Pratt, Holtfreter, and Reisig, (2010, p.270), an estimated 221.3 million people in the U.S. use the internet. Of those people, 66% make online purchases. Because the internet is used more and more frequently for purchases, there are additional opportunities to steal a person's financial information and identity. A Federal Trade Commission study revealed 12.7% of persons they surveyed had been victims of IT within the past five years (2003, p.4). The more people use the internet (and use it for making purchases) the greater the opportunities for becoming victims of identity theft.

Many victims discover they have become objects of IT only after they have applied for credit and were rejected, were contacted by their banks about possible fraudulent charges, or contacted by collection agencies (Benner, Mierzwinski, & Givens, 2000, p.5). White's research indicates only 25% of victims will report IT to a police agency, while a greater number of people (over 40%) will report the crimes to credit agencies (2008, p.9). According to the FTC, 33% of IT cases were related to credit card fraud and 19.2% of those cases were related to the opening of new accounts. Bank fraud accounted for 17% of all cases, while 8.2% of the thefts came from already existing accounts. Phone or utilities fraud accounted for 21% ITs, with 10.4% of those thefts occurring while having new wireless lines installed (FTC, 2004, p.10).

The 2000 census found the majority of IT victims were white males with an average age of 41 years, though most victims ranged in age from 18 to 49. Older individuals were more likely to be targets of IT than those who were younger (Allison Schuck, and Lersch, 2005, p.25). The

victims were targeted based on income level, occupation, and age and selected by means of random dialing, telephone directories, shared registries of public companies, and articles about wealthy people in the media (Levi, 2008, p.404). While Newman states anyone can become a victim of IT and victim characteristics may not be related to risk of victimization, (2004, p.7), research by the U.S. Department of Justice (2010a, p.4) indicates income may be one of the most important factors when targeting victims, as 11.2% of ITs occurred against victims with an income greater than $75,000 and 7.7% against victims whose incomes were $50,000 to $74,999 per year.

Another variable in becoming a victim of IT has to do with the degree of caution used in guarding one's personal information. According to Newman (2004, p.11), people who are not careful when securing wallets, mail, internet purchases, or entering PIN numbers in public are more likely to become victims of IT. Offenders can easily steal names, addresses and credit card information as a result of this negligence.

In many instances consumers are not only victims of IT but they also suffer continued monetary damage in attempting to resolve the problem with credit agencies, businesses and law enforcement (Benner et al., 2000, p.1).

Offenders

Profiling IT offenders is difficult because in the majority of instances, the individual offenders are never discovered. IT is a growing problem and since it is such a new offense it is still hard to identify and apprehend offenders. As of 2009, there had been only two studies conducted related to IT offenders (Copes & Vieraitis, 2009). Although identity theft is a federal offense, offenders are not deterred from continuing to find various ways of committing the crime.

Allison et al, (2005, p.25) suggest identity thieves are solely motivated by economic gain, but Wang, Yuan, and Archer (2008) say identity thieves attempt to steal and use others' identities for fraudulent financial gain, as well as other purposes. They can be individual criminals, terrorists, or a group of individuals. They are often known to their victims (e.g., family members, friends, or colleagues) and not simply faceless strangers preying on unknown victims. They also state that internal employees are responsible for as much as 70% of personal data stolen from companies (Wang et al., 2008, p.31). While almost half (44%) of IT victims do not know the offenders who stole their identities, more than 17% of IT victims are certain business associates, relatives, or acquaintances were the thieves (Benner et al., 2000, p.3).

Selwyn (2008) collected data from online users to determine the amount of deviant behavior committed online. Of the respondents, 26% admitted to accessing another person's email account without the person knowing, while 6% admitted to using information from other persons' credit cards without their knowledge (p.446). Allison et al (2005) found 53% of offenders were

unemployed, when they committed their crimes; 41 % were employed; 3% were retired; and another 3% were disabled and unemployed (p.25).

Gizzi and Gerkin (2010) examined 163 criminal cases to evaluate the types of crimes most often perpetrated by methamphetamine users, including property offenses, violent crimes, and financial crimes. They found, when compared to offenders who did not use meth, users were not more likely to commit financial crimes, unless the charge of possession of a financial transaction device was involved (p.930).

Modus Operandi

Technological advances have created additional risks for becoming a victim of IT. According to Pratt, Holtfreter, and Reisig, (2010, p.270), there are an estimated 221.3 million people in the U.S. who use the internet. Of those people, 66% make online purchases. Because the internet is being used more and more frequently for purchases, there are additional opportunities to steal a person's financial information and identity. The use of technology also means offenders no longer need direct physical contact with their victims, which may reduce the perceived risk of committing IT. (Berghel, 2000, p.20).

While the art of IT has lead offenders to develop a number of techniques and strategies to obtain another individual's personal information, it is not uncommon for offenders to obtain information through old-fashioned thefts of wallets, purses, or trash containing personal information or by making copies of victims' credit cards or writing down the credit card information when victims make credit card purchases in a restaurant or shopping center. Most IT, however, is committed by electronically obtaining credit card information, followed by making purchases, and forging victims' names (Newman, 2004, p.10; Copes, 2009, p.333).

Wang et al. (2008) state IT usually occurs by one of two methods. The first involves low technology, consisting of "stealing wallets/purses, dumpster diving, bribing employees for customer information, or physically stealing files or computer hard drives" (p.31). The second involves more sophisticated technology: *skimming* (using a computer to obtain information from the magnetic strip of an ATM or credit card), *spoofing* (sending messages to the victim from a site pretending to be a trusted source), or *phishing* (sending email messages mimicking a trusted source and asking for private/personal identity information) (p.31). In addition, social media sites have become hot spots for thieves to copy or "clone" victims' profiles to gain access to personal information, to be used to obtain loans, cash advances, credit applications, open accounts, write bad checks, or max out credit cards, which have the potential to destroy the victims' credit scores and/or bankrupt them (White & Fisher, 2008, p.8; Bilge et al, 2009, p.8).

Another ploy is to use the same "ad-ware" employed by marketing companies to learn the online searching habits of users. Offenders gain physical access to online accounts by hiding programs within e-mail attachments or programs which take screenshots every few seconds. Keystroke loggers record every key typed, including passwords, e-mails, websites and pin numbers to allow access to potential victims' information (Southworth, 2007, p.848). Offenders can also be roommates who often have access to mailboxes where preapproved credit cards are delivered. They print receipts containing card numbers and expiration dates, then use them on the internet where additional identification is not required (Newman, 2004, p.37).

Another, more recent way of committing IT is through the use of social networking sites such as Facebook, StudiVZ, MeinVZ and XING. "Crawlers" are programs which browse through these sites to collect information not blocked from public view, to create user profiles, send friend requests, access real users' profiles and more (Bilge, 2009, p.6).

Some offenders utilize their places employment to commit IT. Individuals who have easy access to personal and financial information, not readily available to other employees, have been known to commit IT and some employees in charge of company funds embezzle large amounts of company money or resources. Other scenarios include management personnel who instruct lower level employees to make transactions for them. In these cases, lower level employees may be unaware of the fraudulent activities or may feel intimidated or obligated to complete the illegal transactions (Levi, 2008, p.394).

Prevention Strategies

To develop strategies to prevent IT, it is important to understand how and why people are being victimized. Reisig et al., (2009) analyzed whether respondents, who were perceived as socially vulnerable, such as lower socioeconomic status (SES) consumers and financially impulsive people, were more at-risk for IT than others. They found people with lower SES used more caution and spent less time on the internet, which contributed to decreased risk for identity theft. By contrast, financially impulsive users had higher rates of victimization, possibly due to their inability to constrain their online behaviors (Reisig et al, 2009, p.380). One might conclude exercising restraint in the number of internet purchases one make could reduce IT.

Other researchers make similar suggestions for reducing the ways an identity thief might access one's personal information. Because stealing from mail boxes is common, White and Fisher recommend implementing reforms, industry-wide in the U.S. mail service to reduce blind mailings of credit card applications and to increase security measures for new credit card accounts, such as unique account identifiers (2009, pp.15-16). Wang et al. (2008) say educating the public is an effective way to prevent identity exposure and subsequent theft. Informed consumers may be more motivated to protect their personal information. They also advise

avoiding providing personal information to strangers over the phone or via email, having a separate bank account with a low credit limit for online transactions, and immediately informing the police and the credit bureaus when victimized by IT (p.34).

The International Civil Aviation Authority is currently investigating how to expand IT prevention internationally, specifically through the use of biometric technology. Biometric technology can reduce IT by identifying the owner through unique human characteristics such as fingerprints, voiceprints, retinal eye scans, and other characteristics of the human body. The obvious use of this type of technology is that it requires the person being identified to be physically present for identification (Lyon, 2007, p.166).

Newman (2004) makes additions suggestions for preventing IT. This includes increasing the responsibilities of businesses and their employees when it comes to protecting client records (p. 32). Businesses can become more responsible by using a shredder or document disposal system, limiting data collection to pertinent information only, and restricting access to only those employees with legitimate reasons to see or use the information (p.33). He also discusses the importance of individuals being vigilant about how their names, social security numbers, and accounts are used. This is in addition to keeping social security numbers out of general circulation and prohibiting their use in order to obtain a driver's license, health insurance ID cards, or other forms of identification (pp.34-35).

As the studies demonstrate, to prevent IT, it is recommended individuals take proactive stances with their personal information and business transactions. Smart identification cards can assist in protecting personal information, but this is only part of the solution. It is suggested individuals need to be aware of how they conduct business and dispose of, or share personal information. The articles suggest prevention can be as simple as taking protective measures when making transactions or as complex as the use of biometric identification.

Conclusion

With increases in online shopping, social media, and the general use of the internet as common day-to-day activities, a new global lifestyle has emerged. Offenders, including identity thieves, have adapted to this new lifestyle by developing innovative methods of committing crimes.

As summarized in this report, offenders are not only interested in financial gains, but also means of hiding their identities in order to evade the law, participate in federally funded social programs, obtain work permits, or participate in terrorists plots. The challenge in preventing such crimes is in the high costs of researching and apprehending offenders at a time when budget cuts are commonplace. The problems are made even more difficult because victims often do not

realize they have been victimized until months, or even years, after the crimes have been committed.

Research suggests the public should be educated about the dangers, causes, and methods used to gain access to personal information. By implementing a public awareness campaign and educating the public, it is conceivable crimes of identity theft could become very difficult for offenders to execute and would, therefore, decline. Other methods for decreasing IT include the discontinuation of social security numbers as a means of identification and the education of businesses better to secure the personal information of their customers. More costly prevention methods include the use of biometrics (body measurement and monitoring) as a means of identifying the individual who is using personal information (Aas, 2006, p.145). In the future, as new technologies emerge and become viable options, it is possible biometrics or other similar technologies could play major roles in the reduction of IT. In the meantime, it is up to every person, business (public or private), and government entity to be vigilant on protecting personal information by decreasing its availability and accessibility.

References

Aas, K. F. (2006). The body does not lie: Identity, risk and trust in technoculture. *Crime, Media, Culture, 2*(2), 143-158.

Allison, S. F.H., Schuck, A.M., & Lersch, K.M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice*, *33*, 19-29.

Benner, J., Mierzwinski, E., & Givens, B. (2000). *Nowhere to turn: Victims speak out on identity theft. A survey of identity theft victims and recommendations for reform.* Sacramento, CA: CALPIRG/Privacy Right Clearinghouse.

Berghel, H. (2000). Identity theft, social security numbers, and the web: Privacy is lost in the proliferation of technology's omnipresent accessibility. *Communications of the ACH, 48*(2) 17-21.

Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009). All your contacts belong to us: Automated identity theft attacks on social networks. International World Wide Web Conference Committee (IW3C2), 1-10.

Copes, H., & Vieraitis, L.M. (2009). Understanding identity theft: Offenders' accounts of their lives and crimes. *Criminal Justice Review*, *34*(3), 329-349.

Federal Trade Commission (2003). *Identity theft survey report.*

Federal Trade Commission (2004). *National and state trends in fraud and identity theft, January through December 2003.*

Gizzi, M.C. & Gerkin, P. (2010). Methamphetamine use and criminal behavior. *International Journal of Offender Therapy and Comparative Criminology, 54*(6), 915-936.

Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. *Criminology and Criminal Justice, 8*(4), 389-419.

Lyon, D. (2007). Surveillance, security, and social sorting: Emerging research priorities. *International Criminal Justice Review, 17*(3), 161-170.

Newman, G. (2004). Identity theft. *Problem-Oriented Guides for Police Problem-Specific Guides Series, 25*, 1-64.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3) 267-296.

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived risk of internet theft victimization: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior, 36*(4), 369-384.

Selwyn, N. (2008). A safe haven for misbehaving?: An investigation of online misbehavior among university students. *Social Science Computer Review*, *26*(4), 446-465.

Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007). Intimate partner violence, technology, and stalking. *Violence against Women*, *13*(8), 842-56.

U.S. Department of Justice, Office of Justice Programs. (2010). *Identity theft reported by households, 2007- statistical tables.* NCJ 230742. Retrieved from: http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=2294.

U.S. Department of Justice, Office of Justice Programs. (2010). *Victims of identity theft, 2008.* NCJ 231680. Retrieved from: http://bjs.gov/index.cfm?ty=pbdetail&iid=2222.

Wang, W., Yuan, Y., & Archer, N. (2008). *A contextual framework for combating identity theft.* IEEE Security & Privacy.

White, M. (2008). Assessing our knowledge of identity theft: The challenges to effective prevention and control efforts. *Criminal Justice Policy Review, 19*(1), 3-24.

Wilson, D. (2007). Australian biometrics and global surveillance. *International Criminal Justice Review, 17*(3), 207-219.