The Bill Blackwood
Law Enforcement Management Institute of Texas

Identity Theft: A Growing Problem

A Leadership White Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

By
Paul Neumann

Denison Police Department
Denison, Texas
February 2018

ABSTRACT

Identity theft, defined as the illegal use of someone else's personal information (such as a Social Security number) especially in order to obtain money or credit, has quickly become the most prevalent financial crime in the United States (Merriam-Webster, n.d.). Despite its substantial growth, basic questions about identity theft such as its prevalence, nature, and consequences; characteristics of offenders and victims; and extent of victims' losses remain unanswered. Law enforcement should devote more resources to the detection and prevention of identity theft. Often, a victim of identity theft must spend countless hours proving their own innocence and may suffer from extreme physical and emotional stress due to drained bank accounts, lost wages during their own investigating, plus an inability to borrow. Identity theft is an after the fact crime due to victims not realizing they are victims for months or as long as years from when the personal information was used.

Educating the public in being diligent of protecting their personal information while using public wi-fi and recognizing phishing emails requesting personal information is a critical start in lowering the number of victims. There is an estimated 156 million emails sent every day with 80,000 victims falling for a scam and giving their personal information ("Phishing-How Many Take The Bait," 2015). Agencies must commit to fully investigating incidents with their capabilities to identify and prosecute suspects of identity theft. A victim who has an agency willing to provide direction on recovering their identity could easily make the uphill battle of the victim a few steps shorter. Public service announcements warning Americans of giving personal information could decrease the incidents law enforcement would be asked to investigate.

TABLE OF CONTENTS

INTRODUCTION

As the evolution of technology in every aspect of life progresses where a car will drive itself and a bill can be paid by merely waving a cell phone over a reader, so does the evolution of the identity thief. Identity theft is the wrongful use of another person's identifying information, such as credit card, social security, or driver's license numbers, to commit financial or other crimes. Personal information can be found in a persons' back pocket, cell phone, trash can, home computer, and data base of any business or bank where a product/service was rendered. During the year 2014, 7% of persons 16 years of age or older were victims of identity theft at a cost of $15 billion, while 15% of individuals will experience identity theft during their lifetime, as found in Bureau of Justice Statistics (Harrell, 2015).

The scale of identity theft goes from a single victim who lost an ATM card where the offender withdrew funds to a hacker compromising a business or governmental agency selling the information of thousands of victims. Identity Theft Resource Center published data through March 22, 2016 that states 177 breaches have occurred exposing 4,607,752 records containing personal information. A local law enforcement agency will experience victim complaints of a common occurrence called 'phishing' (pronounced fishing). This occurs when an internet con artist, using bogus emails and websites designed to look like those of legitimate companies, banks, or government agencies, trick unwitting customers into divulging sensitive financial information. Just as effective is a perpetrator calling a business or a residence stating they represent a utilities company and advising the victim that their utilities will be disconnected unless a payment is made over the phone. A child's identity can be stolen when criminals create

what is known as a "synthetic identity," a process by which suspect will take child's Social Security number (SSN) and associate it with a different date of birth. Using an actual SSN, the most crucial piece of every American's identity, confuses the credit issuers and they think it is a new person.

Identifying offenders is at times a daunting task. Studies by Gordon, Choo, Rebovich and Gordon (2007) and Copes and Vieraitis (2009) confirmed that most offenders do not know their victims and those who do know their victims, the relationship could be one of business/client/employment (as cited in Rebovich, 2009). These relationships could involve any entity that receives an individual's personal data as a condition of a purchase or service. Trust in the employees that handle data of this nature has to be given without merit on the assumption that checks and balances are in place. Those that deal in mass amounts of personal data will operate in a forum called the Darknet, which is an area of the internet that most do not know about and fewer know how to access. The average arrest rate for identity thieves is less than 5% with a conviction rate even lower ("What you should know", n.d.). The circumstances are often too complicated to research and assemble.

Repairing credit after the problem arises is a daunting task requiring hundreds of hours, over sometimes years, of painstaking phone calls and emails requiring most to take time off work resulting in lost wages to fix credit issues. A victim of identity theft will file a police report in the jurisdiction where they live where an attempt to follow an electronic trail will begin. An aggressive approach to addressing the identity theft issue where multijurisdictional agencies can collaborate to identify suspects and successfully prosecute will save billions of dollars for citizens and business annually. Local law

enforcement should devote more resources to the detection and prevention of identity theft.

POSITION

Agencies should use a multijurisdictional approach to identity theft because it is a growing problem. An annual identity fraud study found that 13.1 million consumers fell victim to identity theft fraud in 2015 but the total fraud amount lost fell to $15 billion (Al Pascual, 2016). Lifelock CEO Todd Davis was so confident in his company's ability to stop identity theft that he displayed is Social Security Number (SSN) in an advertising campaign. Davis learned of being a victim of identity theft when contacted by a collection agency reference an outstanding $500 loan obtained by a man in Texas. Davis also learned of an fraudulent AT&T wireless account created by an individual in Georgia. Jerry Phillips stole the identity of John Harrison and racked up $265,000 in debt that included two Ford vehicles, a Kawasaki, and a Harley. Carlos Gomez (UPS driver) was arrested by federal agents in the middle of the night being accused of money laundering headed up by a Wachovia bank employee (Chen, 2014). In a country where a person is innocent until proven guilty, all too often a victim of identity theft must spend countless hours proving their own innocence when a law enforcement entity cannot or will not help. The victim and family suffer extreme physical and emotional stress due to drained bank accounts, lost wages during their own investigating, plus an inability to borrow. Identity theft is an after the fact crime due to victims not realizing they are victims for months or as long as years from when the personal information was used. Guardchild.com indicated 40% of victims felt denial, disbelief, anger, and felt

defiled (“Identity Theft Statistics,” 2013). Victims felt an inability to trust people and felt unprotected by the police.

It was not until Congress passed the Identity Theft and Assumption Deterrence Act of 1998 that identity theft was officially listed as a federal crime. The act strengthened the criminal laws governing identity theft. Specifically, it amended 18 U.S.C. § 1028 ("Fraud and related activity in connection with identification documents") to make it a federal crime to knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law. The penalty ranges to a maximum of 15 years and substantial fines. In Texas, identity theft is articulated in the Business and Commerce Code Sec. 521.051 as the unauthorized use or possession of personal identifying information. A person may not obtain, possess, transfer, or use personal identifying information of another person without the other person's consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name.

The local law enforcement agency needs to be more willing to follow an identity theft incident to include other jurisdictions and to include the federal government. A victim who has an agency willing to provide direction on recovering their identity as well as being available to contact creditors to verify the investigation could easily make the uphill battle of the victim a few steps shorter. Departments should create a policy that articulates steps necessary to assist an identity theft victim when the circumstances are within that departments’ ability to investigate.

The Federal Trade Commission (FTC) created the red flags rule for business and organizations. This policy requires a written identity theft prevention policy designed specifically for that entity to detect the red flags of identity theft in their day-to-day operations. The plan must include unusual account activity, consumer report fraud alerts, suspicious account applications, and responses to each of these. The FTC created a how-to guide that curtails to specific services an entity provides to its customers and what red flags to look for. This written policy must be managed by a board of directors or senior management staff. New ways to obtain this information are being created faster that ways to prevent it. On December 18, 2010, President Obama signed into law S. 3987, a bill that removes certain businesses including veterinary, doctor, and lawyer practices that do not receive full payment at the time of service from the FTC's "Red Flags Rule." The bill defines the term "creditor" more narrowly than the FTC had, with the intent of exempting small businesses and other service providers who do not receive payment in full from their clients at the time they provide their services. Unfortunately, small business financial security often lacks in comparison to the larger companies with a budget able to handle this task.

Trust is a word held close when it comes to giving personal information to an entity for service. 2016 data breach statistics published by the Identity Theft Resource Center (Identity Theft Resource Center, 2013) in the categories of banking/credit/financial, business, educational, government/military, and medical/healthcare, 980 data breaches occurred with 35,233,317 records compromised with Government (37.1%) and Healthcare (43.8%) being the largest sources of compromised records (ITRC, 2016).

Carelessness is too often common when it comes to individuals protecting physical property but even more so when the topic of personal data is presented. There was a time when paying a bill with a personal check and putting the envelope in the mail box was the norm. In 2006, the Federal Trade Commission reported that 2% of all identity theft cases were the result of information taken from the U.S. mail. The Ponemon Institute Report (2004) stated that the postal service continues to be the most trusted government agency to present day. Postal inspectors have jurisdiction to investigate and enforce more than 200 federal statutes. Title 18, U.S. Code, Section 1708, allows postal inspectors to arrest anyone suspected of stealing mail or filing a false change of address order.

Throwing credit card bills and bank statement into the trash when no longer needed was not given a second thought only to have someone go through the trash to retrieve that information, a.k.a. dumpster diving. Mihm (2003) wrote about Stephen Massey, a successful maintenance manager who was married with two daughters. Massey experimented with methamphetamine (meth) and began to forge checks to feed his drug use. Massey was invited to go dumpster diving at a local dump for ‘junk’ when he located a shed where recycling was stored. Massey located a barrel full of discarded tax forms from a local accounting firm. As Massey’s enterprise grew, he would have younger meth users called ‘tweekers’ who would receive meth, cellphones, and other items for peoples social security numbers and birth dates retrieved from various means including dumpster diving. Massey’s accomplice, Kari Melton, estimated the total funds stolen exceeded a million dollars by the time they were caught.

Identitytheft.info suggested that trash day for a dumpster diver should be considered ‘cash day’ (“Identity Theft and Scam Prevention” n.d.). What identity thieves look for are checking/savings account statements, cancelled checks, wage and earning statements, medical bills, investment documents, among many others. Expressrecycling.com suggested “shred it and forget it” and that ripping up documents is not sufficient. Medical care is part of life and giving basic personal information to the receptionist is a requirement. The Medical Identity Theft Alliance (MIFA) produced Fifth Annual Study on Medical Identity Theft (2015) that stated that there was a 22% increase in medical identity theft during 2014. The Poneman Institute estimated there were 500,000 victims in 2014 alone. These results did not include the Anthem data breach that compromised 80 million Americans. Add into the equation improperly discarded medical records and unscrupulous clerks and receptionists who use or provide personal information for profit. A data breach containing thousands of records would be overwhelming for local law enforcement agency, thus a federal entity would take lead on such an investigation. The individual in the medical office who forwards personal information can be investigated along a trail that could identify a hierarchy of individuals for prosecution.

With today’s technology, most restaurant’s, bookstores, basically any place of leisure is equipped with wireless internet (a Wi-Fi hot spot). Someone accessing financial accounts and personal data on their computer or device is allowing anyone else connected to the same hot spot the opportunity to access personal data on those devices. Identity Theft Resource Center (2013) explained that wifi hotspots are susceptible to hacks identified as sniffers, sidejacking, evil twin/honeypot attack, arp

spoofing, rogue network, man in the middle attacks. Each has a varying level of effectiveness, but all will compromise personal information, email, and apps. Failing to take common sense precautions causes compromised personal information when using public Wi-Fi locations.

Another reason why agencies should be aggressive is that citizens are being taken advantage of by phishing (fishing) scams. A suspect will call an individual or a business claiming to be a utilities representative and state that unless an outstanding balance is paid over the phone the utility will be disconnected. Too often out of fear, either credit card information or bank information is given out to later find the money is lost forever. Another version of phishing is when mass emails are sent out referencing an update of personal information with a link that sends the recipient to a web site astonishingly close to an actual business website. A victim will again unwittingly provide personal information only to find months or even years later that the web page was fictitious. It is estimated that 156 million emails are sent every day, 16 million make it through filters, 8 million are opened, 800,000 links are clicked, 80,000 fall for a scam giving their personal information ("Phishing-How Many Take The Bait," 2015).

COUNTER POSITION

Opposition believes local law enforcement agencies should not devote the time or resources to identify identity theft suspects who would receive minimal or no punishment for their crime. Grimes (2012) found that between 2003-2006, the FBI was able to arrest between 1200 to1600 identity thieves and about one third of those cases resulted in convictions with short jail time. These crimes affected 8.3 million victims, which represents nearly 4% of the US adult population, which means one conviction for

every 20,750 victims. These statistics are only at the federal level. As a whole, it is estimated that 5% of identity thieves are identified and prosecuted. Local law enforcement has taken a position of identity theft would require internet technology (IT) skills and equipment that would be necessary to digitally track the trail of a suspect without the budget dollars to dedicate to this growing problem. Law enforcement will provide the victim with an incident number and direct them to identity theft self help web sites and get back to the priority cases.

With any specialty investigation, training is the key to responding to new or innovative crimes. Training sources are plentiful through the federal government for law enforcement entities. The National Criminal Justice Reference Service provides a CD-ROM, Identity Crime: An Interactive Resource Guide, from the U.S. Secret Service that provides a user-friendly, convenient tool to local and state law enforcement that will enhance their understanding of identity crime. This encourages entities to become more involved in combating this crime and provide them with a comprehensive guide of both investigative and victim resources. Investigating identity theft is a time-consuming endeavor that requires the cooperation of financial entities, creation of subpoenas, and search warrants required due to privacy acts.

Additionally, some agencies may believe that they do not need to work identity theft crimes due to victims of identity theft recouping monetary loses through their financial institution who in turn incur all loses and side effects of identity theft. With a low probability of identifying the suspect much less get a conviction, local law enforcement has chosen not dedicate the time and personnel to a futile endeavor. The victim is given an incident number to take to their financial institution and thus

recovering the lost money or the removal of fraudulent charges leaving financial institutions to take the losses.

Though not a violent crime, the devastation to a victim financially can be months or years long process to remove fraudulent accounts and repair ones' credit not to mention the psychological effects. The time spent repairing credit takes the victim away from the job causing even more financial hardship. Questions arise as to why law enforcement should take time and effort to follow a digital suspect. It is law enforcement's responsibility to the community they serve to do more than just take a report but to take the investigation as far as possible eliciting the input of other local agencies and utilizing the resources available from the Federal Government for resources and free training. Jones (2015) suggested that a fusion center created for multi-jurisdictional agencies could collaborate and share offence-specific information. Fusion centers "also have the benefit of allowing investigators to link their offences to other on-going offences which in turn increases the odds of a successful prosecution" (Jones, 2015. p. 6).

RECOMMENDATION

Today's technology is progressing at a pace faster than any time in history. Companies are trying to maintain security of client's personal information at the same time identity thieves are attempting to breach those same firewalls. Bureau of Justice Statistics suggested in the year 2014, 7% of persons 16 years of age or older were victims of identity theft at a cost of $15 billion while 15% of individuals will experience identity theft during their lifetime (*Victims of Identity Theft,* 2014). The devastation of identity theft on a victim just emphasizes the need for law enforcement to devote more

resources to the detection and prevention of identity theft. The local law enforcement agency needs to be more willing to follow an identity theft incident to include other jurisdictions and to include the federal government. A victim who has an agency willing to provide direction on recovering their identity as well as being available to contact creditors to verify the investigation could easily make the uphill battle of the victim a few steps shorter. Departments should adopt policy that articulates steps necessary to assist an identity theft victim when the circumstances are within that departments' ability to investigate.

The consequences of identity theft in most cases is monetary but in extreme cases the effects are much greater. A victim can experience lost wages taking time off work to fix discrepancies, mental anguish of not being able to get a loan, along with receiving collection calls from credit companies. Educating the public on how to protect their personal information is an easy way to help deter identity theft. The problem is the public getting lazy with their information and tossing it in the garbage versus shredding it. The phishing frenzy of today preys on the naive who are too willing to believe the scare tactics of a voice on the phone threatening to shut off a utility unless credit card or bank information is given over the phone to satisfy an alleged outstanding bill.

A frustration common among law enforcement agencies is the lack of punishment dealt out to offenders in any criminal case. Grimes (2012) estimated that one third of identity theft suspects are convicted and those convictions result in short jail times. With those statistics, agencies are not motivated to devote the resources to thoroughly investigate identity theft crimes. Law enforcement owes the community the due diligence to investigate any crime as defined by state and federal statutes. The

resources available through the federal government for training and equipment is there for those agencies serous about fighting identity theft. There will be instances where an identity theft victim will be involved in an incident so large that a local agency will not be able to thoroughly investigate the crime. An open line to the area federal authority will aid in helping victims due to additional resources and same or similar cases ongoing.

The easy way out for an agency is to give the victim a call number in order to recoup lost monies or removing fraudulent charges from credit cards and closing the case with all leads exhausted letting the financial institutions deal with the loses. That is just the beginning for a victim whose identity was used in such a way that the amount of time to resolve the issue is devastating to the individual and the family. The amount of lost wages taking time off work to solve the issues along with the mental anguish of no credit can be a strain on a person and their family. The burden of recouping one's identity is on the victim to make the numerous phone calls and dealing with attorneys to clear up discrepancies now attached to the victim. A thorough investigation done by the agency along with some well-placed phone calls could go a long way in helping a person who believes there is no one to help them. A fusion center, as suggested by Jones (2015), would serve as a resource for investigators to take a case potentially to prosecution.

Statistics show over and over that identity theft is a growing problem that individuals and corporations alike are battling on a daily basis. Federal entities have proven that the number of victims are increasing and the devastation to the victim not only effects the individual but the family unit. Lifelock Ceo Steve Davis was confident that no one could use his social security number to gain credit and was proven wrong

twice. Carlos Gomez was a UPS driver arrested in the middle of the night for money laundering only to learn a Wachovia bank employee used his identity (Chen, 2014).

Federal statutes are in place for the prosecution of identity thieves. Local law enforcement must make the internal decision to devote more time and pursue the monies and training available from the federal government to successfully track and identity suspects of the nonviolent but a devastating crime. The task of convincing a city government to devote monies for additional personnel to tackle identity theft will be a challenge. Educating the public on what simple steps can help to protect them from identity theft as well as departments dedicating more resources to this growing problem will progress be made tackling this devastating crime.

REFERENCES

Al Pascual, K. M. (2016, February 2). *2016 Identity Fraud: Fraud Hits an Inflection Point*. Retrieved from https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point

Fifth Annual Study on Medical Theft. (2015, February). Retrieved from Forbes.com: www.forbes.com/sites/danmunro/2015/02/23/new-study-says-over-2-million-americans-are-victims-of-identity-theft/

Grimes, R. (2012). *Why Internet Crimes Go Unpunished.* Retrieved from Infoworld.com: http://www.infoworld.com/article/2618598/cyber-crime/why-internet-crime-goes-unpunished

Identity Theft Resource Center. (2013, June 24). Retrieved from idtheftcenter.org: http://www.idtheftcenter.org/Cybersecurity/how-wifi-hotspot-hacks-occur.html

Identity Theft Resource Center. (2016). Retrieved from Identitytheft.org: https://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2016.pdf

Identity Theft Statistics (n.d.) Retrieved from Guardchild: https://www.guardchild.com/identity-theft-statistics/

Jones, A. (2015). *The Call For A Collaborative Approach To Identify Fraud Through The View Of New Offence -Specific Fusion Centers.* Huntsville, Tx: Bill Blackwood Law Enforcement Management Institute of Texas.

Merriam-Webster. *Identity Theft (n.d.)*. Retrieved July 17, 2017 from https://www.merriam-webster.com/dictionary/identity%20theft

Mihn, R. (2003, 12 21). *Dumpstr-Diving For Your Identity.* Retrieved from nytimes.com: http://www.nytimes.com/2003/12/21/magazine/21IDENTITY.html?pagewanted=al

Chen, L. (2014). *3 Stolen identity stories.* Retrieved from www.consumersadvocate.org/id-theft-protection/stolen-identity

Phishing-How Many Take The Bait. (n.d.). Retrieved from Getcybersafe: http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx

Rebovich, D. J. (2009, Volume 4). Examining Identity Theft: Emperical Explorations of the Offense and Offender. *Victims and Offenders*, 357-364.

Red Flag Clarification Act, S. 3987 . (2010).

Red Flag Rules. (2008). Retrieved from Federal Trade Commision: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/red-flags-rule

Victims of Identity Theft, 2014 (NCJ 248991). (2014). Retrieved from Bureau of Justice Statistics: www.bjs.gov/content/pub/pdf/vit14.pdf

What you should know about identity theft. (n.d.). Retrieved from Financialinfo.org: http://www.financialinfo.org/shocking-statistics-about-identity-theft.html