Stealing More than Just Identity

Faisal Alrashed

Abstract— This paper discusses what Identity theft is and what it can cause. Moreover, it addresses the methods of Identity theft and how government can deal with it as well as the protection methods.

INTRODUCTION

Identity theft can be described as the misappropriation of another person's identity that typically involves impersonating someone else and taking up that person's personality. Most cases of identity theft frequently involve the need to access valuable resources or take credit and other advantages that accompany a renowned person's title. Victims of identity theft are the people whose identities have been stolen, and who are caught off guard to suffer unfavorable consequences if they are assumed responsible for the actions of the perpetrator. Identity theft happens when an individual illegally acquires and exploits other people's private information such as names or PIN numbers to carry out swindles or other offenses. While this nature of identity theft is very common, several unexplored aspects of this phenomenon exist in the real world. This category contains many questions on the nature and description of identity theft (Anania, Johannes, and Eeten 29). This new perspective is far much broader and includes events that were initially assumed ordinary and non-criminal. This paper will discuss the meaning and nature of identity theft, and will explore the motives of the offenders behind the identity theft along with miseries of the victims whose identities are stolen, and the preventive measures being taken by the relevant authorities to check this crime.

By far, the most common form of identity theft involves exploiting flaws that exist in the common information technology platforms. Credit card, Email, and Internet identity thefts fall in this category. Fraudsters normally use different techniques that tamper with the technology or alter the information within the cards. Regardless of the approach, such types of theft have a thin threshold that allows them to be categorized as genuine "identity thefts" (Lenardon 43). Stolen credit cards may be used for fraudulent purposes and returned to the owner's possession without them even realizing. Such misdemeanors take place over a span of several hours. In such a situation, it may be difficult to prove that identity theft occurred.

More interesting is the rise in identity theft not as the final crime but as insurance cover for perpetrating new crimes. The theft of personal documents is usually perpetrated with an intention of facilitating other serious crimes. An experienced identity thief strives to acquire several sets of useful individual identity such as date of births and PIN numbers, and use these to create supplementary documents. The deliberate exploitation of this information through different channels such as telephone, online, personal contact with bank tellers, and even applying for new credit cards contribute towards acquiring more information that is personal for instance, bank details, driver's permit and passports (Anania et al., 48). This fresh information may be exploited to falsify new documents such as fake credit cards that may possess account and names of genuine account holders. This web of uncertainty is an important factor that complicates the investigation process of discovering these fraudsters. Fresh bank accounts may be created, new credit cards acquired. A parallel way of conducting business and completing essential transactions to perpetrate further crime under a different guise may be achieved. The main intention of perpetrating a crime is to commit it without being revealed. To commit an offense under the identity of another person for that reason is an appealing proposal. It lowers the risk both in the perpetration of the offense and in being arrested after the felony. Fabricating the necessary enabling documentation to facilitate business dealings lowers risks when committing crimes (Lenardon 28). For example, making transactions with falsified documents lowers the chances of being arrested. In the event that a criminal is arrested, presenting a fake identity forged from an innocent person's identity card can avoid detention, particularly if the detainee already posses a previous criminal record. Perpetrating offences in another individual's name implies that the police force will be investigating for a different person and not the genuine offender (Anania et al., 67).

EXPLOITING OPPORTUNITIES

Perpetrators have developed ingenious ways to exploit the opportunities presented by flaws in technology, human beings, and other organizations. With the advancement in technology, banks are trying to introduce new products based on the Internet to facilitate their customers, but in fact they are risking their customers by putting their personal data in online databases. These databases are vulnerable to the attacks of hackers who are lurking around to pounce upon every opportunity that comes their way to benefit them. In this competition race, the customers can be the ultimate losers whose identities are being stolen without their knowledge, their money is being withdrawn without their knowledge, and their bank accounts are being used to transfer money to some terrorist group. Hackers can also send some virus through email to steal personal data from computer and use it in some illegal activity. They use the method of temptation to get secret information such as passwords and banking information by telling the people that they want to deposit prize money into their bank account. These innocent people are unaware of the fact that their account is going to be used by some mafia group to sponsor terrorism, and when law enforcement agencies will get involved, they will be held responsible due to the fact that

their account has been used in activities like money laundering.

The techniques used by most offenders can be categorized as either approaches that steal identities or approaches that convert the identities into rewards being pursued. Most offenders who steal identities are basic criminals that double up as violent criminals (Anania et al., 89). Such offenders steal purses, wallets, and bags with the potential of having important documents. They also steal envelopes from mailboxes, documents from hospitals and on personal computers. For such perpetrators, collecting the personal documents and using them for short-term benefit such as petty cash, reputation, and acknowledgment (Abagnale 45). Conversely, offenders who take up new identities in illegal ways for advanced benefits are more complicated. They use the acquired identity to create new credit cards and bank accounts. Furthermore, they also steal other benefits such as insurance, loans, and tax returns (Lenardon 68).

WHAT MOTIVATES OFFENDERS OF IDENTITY THEFT

Concealment is one of the key motivators that drive many offenders to commit identity theft crimes. Concealing previous crimes is a significant reason for people to steal or take up fake identities. A prominent example is that of Kathleen, the woman behind numerous city bombings and murders who took up the identity of Sara Olson, a Scandinavian national living in Minnesota. She managed to avoid being arrested for over two decades (Anania et al., 178). During this period, she married, became a doctor, bore three children, took up a job as a community volunteer, volunteered for charity in Africa, and moved to a fashionable neighborhood in Minnesota (Lenardon 56). Terrorism has emerged as a significant channel through which identities are stolen to cover up criminal activities, and to complicate the investigation of their genuine identities after they have perpetrated crimes. All of the terrorists involved in the September 11 attack on the United States were protected by experts in identity theft in different ways. This contributed to a massive security problem when innocent American citizens who were the victims of identity theft were mistakenly arrested (Abagnale 67).

The psychological state of most identity theft offenders is a serious issue that must be investigated in depth since it holds the key toward understanding their drive and consequently, how to stop their behavior. The prevalence of the Internet has allowed for increased anonymity that protects all types of first-time and constant offenders who have not been arrested by the authorities (Anania et al., 208). Coupled with the increasing cases of breakdown in family relationships and communication, many people resort to using the Internet to let off steam and relate with other people. With the lack of proper knowledge on internet security and usage, many people unknowingly offer their personal information on online websites, email service companies, and social media sites. It is relatively easy to perpetrate identity theft crimes since there is a wealth of ready personal information on the Internet, or attached to other emails that can be accessed by fraudulent people. Many ordinary Internet users fail to follow the necessary protocols and security measures that protect their personal information. Similarly, companies are rarely careful with the customer information and allow it to be accessed by random users. Opportunities are rife. Several avenues for creating counterfeit public documents such as alternative IDs are available within the Internet (Lenardon 19). Conversely, the profile of most victims of identity theft plays an insignificant role in the study of identity theft (Anania et al., 29). Most of the victims are approximately 40 years of age and residing in the urban centers. Regretfully, these victims are the people whose sufferings are not taken into the account while discussing this issue. The United States Department of Justice has reported a case of Identity theft in which the criminal withdrew more than $100,000 from the victim's credit card, managed to sanction a federal loan by using the false identity, and bought a number of homes, motorbikes, and handguns. Then he also called the victim to tell him about all these things, and then filed a case of bankruptcy in the victim's name. He did so bravely because there was no such law at that time to prosecute the criminals because identity theft was not a crime in those days.

EFFORTS MADE BY THE GOVERNMENT TO CHECK IDENTITY THEFT

Most government-led efforts to restrict identity theft have been targeted the reinforcement of legislation surrounding the penalties and restriction of access to personal information. Federal and state legislators have tackled the issue by voting for laws that can denote identity theft as a crime, outline sentences for offenders, and intensifying protection to online users and victims of identity theft (Abagnale 93). For example, in 1998, "Identity Theft and Assumption Deterrence Act" was passed by the Congress which declared identity theft as an offence. This law has prohibited the assuming of another person's identity with the intention of performing an unlawful activity. In addition to lawmaking initiatives, several charity groups, and private organizations have started movements to sensitize consumers on how to safeguard their personal information. Sadly, enough, the Internet security companies has also created a window of opportunity for generating the profits by playing with the hype of this identity theft fear. They have started marketing their anti-theft products by exaggerating the facts and fears about the identity theft crimes. They persuade the internet users to use their products to get protection while shopping or making online transactions. Although restricted, the currently available statistics recommend that definite situational crime deterrence approaches may be helpful in lowering the incidence of identity theft. Particularly, intensifying the effort and dangers of obtaining information and transforming information to money or property, eradicating ways in which information is obtained and changed into valuable products, and communicating the potential legal ramifications of stealing other people's identity may assist in lowering identity theft (Biegelman 45). To comprehend the felony of identity theft and therefore maximize the possibility that legislators and law enforcement are helpful in eliminating this crime, more studies needs to be conducted (Anania et al., 39). First, several laws have been implemented to extend assistance to consumers and identity theft victims. Federal prose-

cutors are also working in collaboration with investigative agencies like United States Secret Service, Federal Bureau of Investigation, and the United States Postal Inspection Services to curb these crimes of identity theft and fraud. There are a number of recent cases in which people have been tried by the federal courts, and have been sentenced after the establishment of charges against him. A man got 27 months imprisonment for using private bank account information to transfer money into another bank account illegally. In California, three people were arrested on the charges of opening bank accounts by using stolen identity information and depositing U.S. Treasury checks, and withdrawing the amount. Nonetheless, the efficiency of these regulations has not yet been evaluated. A greater part of this legislation is moderately new, prospective research should assess the level to which the law is an effective approach in lowering cases of identity theft.

THE RESPONSIBILITY OF CORPORATIONS IN PREVENTING IDENTITY THEFT AND FRAUD

Business firms and organizations that handle personal information have a responsibility to ensure safety of data and remain vigilant in the prevention of identity theft. Notably, identity theft or fraud occurs when someone wrongfully, deceptively, or without authorization, obtains another person's personal information and uses it for economic gain or to confer him/herself a certain benefit. This means that access to personal information is a prerequisite to identity theft and the fraud or crime that results from it (Whitman and Matford 5). Businesses, organizations, companies, and virtually every entity that requires clients, customers, members, or stakeholders to provide personal information is tasked with the responsibility of ensuring that data is safe (Whitman and Matford 7). For example, a bank has the responsibility to take care of its clients' personal and financial information, and it may be held liable for allowing unwarranted access to personal information. Similarly, a state agency should be liable for allowing third parties to access its clients' or members' social security or credit card numbers. In the modern era in which information is very valuable and the internet is not safe, customers only have confidence in a firm only if it has a proven record of privacy and confidentiality.

Businesses and organizations have many methods to protect personal information. One of the key ways through which businesses can protect personal information is through basic office information management strategies. Poor stewardship of sensitive personal information at businesses can expose individuals and also the business to identity theft (Biegelman 23). For example, companies should effectively shred documents that may contain personal information before dumping it in dumpsters. Notably, individuals can ferret through waste in bins and recover documents that can be used in identity theft and fraud. In addition, the failure of government agencies and organizations to verify the identity of who they are working with and who is handling their personal information may result to serious cases of identity theft. For example, an organization that fails to verify the identity of its data handlers and other individuals who have access to sensitive personal information may fail victim of data brokerage by the individual, who may have an unchecked criminal past on identity theft. Organizations can also deal with individuals who have stolen others identities without knowing. This means that it is crucial for all organizations, including government agencies and private businesses, to verify the identities of individuals who have access to personal information in the firm (US Department of Justice 4).

Corporations have a responsibility to protect sensitive and confidential information at all costs (Cordell 2). There are many ways that organizations can protect their data, but the best way is to manage information in such a manner that is cognizant of the threat of identity theft and hence preventive of unauthorized data access. First, organizations should make secure personal information through controlling who has access to it. Normally, only a few people in an entire organization have access to personal information. In addition, the use of passwords and identifiers ensures that a firm can trace who accessed what kind of information and for what reason. Secondly, businesses should prevent the unauthorized access of sensitive information through several ways that protect data even in cases of emergency or error. For example, strong encryption of data on computer devices ensures that even in the case of an emergency that may result to breach of the firm's security and perhaps access to computers, data is inaccessible because it is coded. Third, business firms and other organizations should ensure that all stakeholders in the business who have access to personal information have adequate data security controls and are impervious to data brokerage crimes that may offer sensitive personal information to individuals with malicious intent.

Another method that organizations can use to protect personal information is to limit how much data they collect from customers in a transaction and also limit how the length of time they hold the information. For example, if a company is paid through credit card services, it only needs a credit card number, its expiration date, and the security code. In such a circumstance, obtaining the customers social security number is unnecessary. To ensure protective data handling, once all the transactions have been done and the firm has been compensated by the credit card company, then the personal information is not needed anymore (US Department of Justice 13). For security reasons, the business firm can archive the data for only a few days or weeks depending on the nature of the transaction, then the sensitive information such as the credit card number can be deleted for safety reasons, leaving only evidence that the transaction took place, and perhaps the customers contact. Some businesses do not need customer's personal information at all, and they should refrain from collecting it.

In this era of heightened threats of internet insecurity, all firms handling personal information over the internet have a responsibility to protect such data (Nemati 125). When customers and other people transact online, they assume that the firm has taken the adequate measures to protect any personal information exchanged during such transactions (Sileo 174). Companies are expected to invest in reliable information technology systems that constantly protect personal information from unauthorized access (Sileo 181). Databases should be regularly checked for unauthorized access and firewalls

should be used to protect personal information. Organizations are usually liable for unauthorized access to personal information resulting from poor data protection. For example, if a company is hacked or loses personal information because it has a poor data protection system, customers and stakeholders can sue it for inadequate protection of sensitive personal information. The case of Sony Studios is a good example in this case. In 2014, several ex-employees of Sony Pictures Studios filed a lawsuit against the firm claiming that it was negligent to warnings that its system was prone to a hacking attack until it was hacked, resulting to the loss of more than 50,000 pieces of personal information including social security numbers and salary details (Reilly 3). The case of Sony is one of the recent key incidences that show that organizations have a huge role to play in enhancing cyber-security.

INDIVIDUAL IDENTITY THEFT PROTECTION

Prevention of identity theft at the personal level is very important because until personal information is collected, identity fraud cannot be committed. Though organizations and government agencies have invested heavily on data security, individuals should not rely on them to protect them from identity theft. Defense from identity fraud at the personal level is most effective and can provide early remedies before much damage is done in case there is a breach in personal information. Individuals have a significant role to play in preventing identity theft by improving how they handle their personal information. To minimize the risk of identity theft, individuals should beware of the threat that faces them and be stingy in providing personal information. Individuals should use a 'need-to-know' criteria when evaluating who to give information to (US Department of Justice 7). For example, a person from the bank would not call to enquire about an individual's account number when it is in the bank. Similarly, a person from a gas delivery business would not need a social security number. Ensuring that personal information is provided only to people that have a genuine need to know is one of the key ways through which individuals can protect themselves against identity theft.

Individuals should also exercise good information management to prevent unauthorized access to sensitive information and the resultant identity fraud. Documents containing sensitive personal information should not be disposed in bins but destroyed completely. This is because fraudsters can obtain data that can be used in identity crime from garbage dumps. The provision of data to unknown entities should also minimized. If an individual is not sure of the identity of an individual or agency that is requesting for a piece of personal information, he or she should ask for a written request for such information (US Department of Justice 3). In essence, before giving up their personal information, individuals should do their best to establish the identity of the individuals or firms in need of such information. The importance of this is that when fraudsters have incomplete information about an individual, they will try their best to acquire such information in any way possible, including the use of deception to lure the target to send such information.

While prevention is the most important way to avoid identity theft, early detection is important for remedy before a lot of damage is done through identity fraud and other crimes. It is important for individuals to regularly scrutinize their monthly financial statements to ensure that all is well (Goodridge 3). Many people usually just give a glance without reviewing them to ensure that there are no unusual charges or withdrawals. Fraudsters with personal information about a person can open request for credit cards and also order charges to an account under someone else's name. By periodically reviewing credit reports, individuals can identify charges that they did not make and then follow them up to determine whether the unusual charges are due to identity fraud (Goodridge 5). Early detection of unusual financial activity due to identity fraud allows for an early solution to the problem. If an individual notes unusual financial activity in credit reports or suspects identity fraud, he or she should notify the financial institution concerned immediately for follow up. Early detection means that fraud can be nipped in the bud before more damage is done (Stickley 74).

After discovering or suspecting that they may have become victims of identity theft, individuals should not only contact their banks but also immediately inform the agencies involved in investigating such cases (Stickley 74). The Federal Trade Commission (FTC) and the Privacy Rights Clearinghouse (PRC) are some of the agencies that can be contacted immediately for reporting of identity theft cases (US Department of Justice 9). In every jurisdiction, there are several agencies that are concerned with the reception and processing of identity theft and fraud complaints. Though investigations after identity theft can help remedy the situation, the task of correcting financial information and restoring personal status may be a very daunting task in which some of the pieces may be missing and others cannot fit as they did before the crime. The misuse of stolen identity may also continue after discovery (McNally 27). Fraudsters can do a lot of damage to someone's identity as they use his or her connections to commit fraud that may be shaming and very destructive to the victims' reputation and public image. The immediate and short term effects of identity fraud include financial losses, damage in reputation, and loss of access to credit services such as mortgages and loans (McNally 25). Financial safety is a personal responsibility, so individuals have the highest responsibility in protecting themselves and ensuring that their organizations do the same.

REFERENCES

[1] Abagnale, Frank W. Stealing Your Life: The Ultimate Identity Theft Prevention Plan. New York: Broadway Books, 2007. Print.

[2] Anania, Loretta, Johannes M. Bauer, and Eeten M. Van. "The Economics of Cyber-security." Communications & Strategies. 2011. 81 (2011): 13-149. Print.

[3] Biegelman, Martin T. Identity Theft Handbook: Detection, Prevention, and Security. Hoboken, NJ: Wiley & Sons, 2009. Print.

[4] Cordell, Matthew A. "Beware of 'Red Flags': What Must Your Business Do to Protect Customers from Identity Theft?" 3 July 2013. Ward and Smith. Web. 12 April 2015. http://www.wardandsmith.com/articles/what-must-your-business-do-to-protect-customers-from-identity-theft#.VSqxQPD7L4Z.

[5] Goodridge, Elisabeth. "Steps to Prevent Identity Theft, and What to do if It Happens." 1 May 2009. The New York Times. Web. 12 April 2015.

http://www.nytimes.com/2009/05/02/your-money/identity-theft/02idtheftprimer.html?pagewanted=all&_r=0.

[6] Lenardon, John. Identity Theft Toolkit: How to Recover from and Avoid Identity Theft. North Vancouver, BC: Self-Counsel Press, 2006. Print.

[7] McNally, Megan. Identity Theft in Today's World. New York, NY: ABC-CLIO, 2012. Print.

[8] Nemati, Hamid R. Analyzing Security, Trust, and Crime in the Digital World. New York, NY: IGI Global, 2013. Print.

[9] Reilly, Jim. "Ex-Employees Sue Sony for Not Preventing Hackers from Stealing Personal Information in Cyber Attack." 16 December 2014. The DailyMail. Web. 12 April 2015. http://www.dailymail.co.uk/news/article-2876465/Ex-employees-sue-Sony-not-preventing-hackers-stealing-nearly-personal-information.html.

[10] Sileo, John. Privacy Means Profit: Prevent Identity Theft and Secure You and Your Bottom Line. New York, NY: John Wiley and Sons, 2010. Print.

[11] Stickley, Jim. The Truth About Identity Theft. New York, NY: FT Press, 2008. Print.

[12] US Department of Justice. "Identity Theft and Identity Fraud." 2015. US Department of Justice. Web. 12 April 2015. http://www.justice.gov/criminal/fraud/websites/idtheft.html.

[13] Whitman, Michael and Herbert Matford. Principles of Information Security. Stamford, CT: Cengange Learning, 2010. Print.