BOOK CHAPTER | Private Fears in Online Spaces

Mitigating Identity Thefts in Online Spaces

Babatunde O. Lawal
Student Affairs Department
International Psychometrics Centre, Ibadan, Nigeria
Email: lawal5@yahoo.com
Phone No: 08038614477

Abstract

Identity Theft is a crime in which an impostor obtains key pieces of personal Identifying Information (PII) such as Social Security Numbers and driver's license numbers and uses them for their own personal gain. Many decades ago, before the information age, when there was no internet, little or no cases of identity theft were reported. Recently, the internet has created an environment for individuals to input personal details which makes offenders to steal these personal Identifying Information (PII). This study draws on scientific studies that are available and a variety of other sources to assess what we know about identity theft and what could be done to further the research base of identity theft. The study also suggested ways to protect one's identity based on types of identity theft discussed.

Keywords: Identity theft, Identity fraud, personal Identifying Information, Internet

Introduction

Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. The term *identity theft* was coined in 1964 and since that time, the definition of identity theft has been statutorily defined throughout both the U.K. and the United States as the theft of personally identifiable information [1].

Initially, there was no accepted definition of identity theft Until the United States (US) Federal Identity Theft and Assumption Deterrence Act of 1998 was made. This Act defined identity theft very broadly and made it much easier for prosecutors to conduct their cases in courts. However, it was of little help to researchers, because a closer examination of the problem revealed that identity theft was composed of a number of disparate kinds of crimes committed in widely varying venues and circumstances [1]. Over the past decade, many States and countries have now passed identity theft legislation, and the generic crime of identity theft has become a major issue of concern. Many identified and severe cases of identity theft that were made public in the print and electronic media have made identity theft a known crime that is now widely recognized by the public [1].

Citation: Babatunde, O. Lawal (2022). Mitigating Identity Thefts in Online
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series

The Internet has played a major role in disseminating information about identity theft, both in terms of risks and information on how individuals may avoid victimization. It has also been identified as a major contributor to identity theft because of the environment of anonymity and the opportunities it provides offenders or would-be offenders to obtain basic components of other persons' identities [1].

The greatest hindrance of conducting scientific research on identity theft and findings interpretation have been difficult in defining it. This is because a considerable number of different crimes may often include the use or abuse of another person's identity or identity related factors. Such crimes may include check fraud, plastic card fraud (credit cards, check cards, debit cards, phone cards etc.), immigration fraud, forgery, terrorism using false or stolen identities, theft of various kinds.

Personal Identifying Information (PII)

Personal Identifiable Information (PII) is defined as any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: [2]

(i) that directly identifies an individual (e.g., name, address, social security number, BVN or other identifying number or code, telephone number, email address, etc.) or

(ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media. Note: Your name + key information = PII [3]

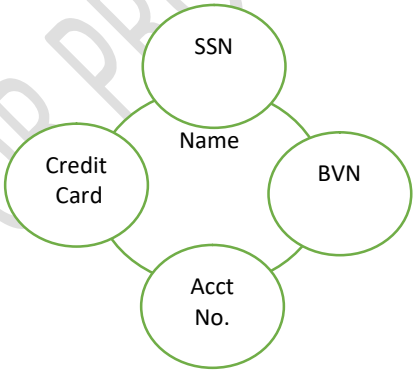

Fig 1: Personal Identifying Information (PII) [3]

Types Of Identity Theft

Identity theft is majorly categorized into five different types:

i. **Criminal identity theft:** Criminal identity theft occurs when someone cited or arrested for a crime presents himself as another person, by using that person's name and identifying information. This result into a crime in the name of a victim, who may not know of the crime until it is too late.[4]

As identity theft is a crime, the term "criminal identity theft" can be confusing[5], but it refers particularly to the crime of intentionally misleading law enforcement to believe that the person being cited or arrested is someone else. The California Attorney General's office says criminal identity theft doesn't happen a lot, but when it does, the ramifications can be serious.[4]

ii. **Financial identity theft:** In financial identity theft, someone uses another person's identity or information to obtain favours and benefits such as credit, goods, services, or other benefits. This is the most common form of identity theft. [5]

iii. **Identity cloning:** In this situation, the identity thief impersonates someone else to conceal their own true identity. Examples are illegal immigrants hiding their illegal status, people hiding from creditors or other individuals and those who simply want to become "anonymous" for personal reasons. Another example is *posers*, a label given to people who use someone else's photos and information on social networking sites. Posers mostly create believable stories involving friends of the real person they are imitating. Unlike identity theft used to obtain credit which usually comes to light when the debts mount, concealment may continue indefinitely without being detected, particularly if the identity thief can obtain false credentials to pass various authentication tests in everyday life.

iv. **Medical identity theft (using another's identity to obtain medical care or drugs):** In this type of ID theft, someone will pose as another person to obtain free medical care. This can cause confusion to some medical practitioners and the victims. An example is If the victim is a known Asthma patient and the Identity thief got free medical care or bought drugs for ulcer treatment. [6]

v. **Child identity theft :** In child identity theft, someone uses a child's identity for various forms of personal gain. This is common, as children typically do not have information associated with them that could pose obstacles for the perpetrator. The fraudster may use the child's name and Social Security number to obtain a residence, find employment, obtain loans, or avoid arrest on outstanding warrants. Often, the victim is a family member, the child of a friend, or someone else close to the perpetrator. Some people even steal the personal information of deceased loves ones.

Other Types of Identity Theft

vi. Social Security Theft

If identity thieves obtain your Social Security number, they can use it to apply for credit cards and loans and then not pay outstanding balances. Fraudsters can also use your number to receive medical, disability, and other benefits.[5]

vii. Synthetic Identity Theft

This is a type of fraud in which a criminal fellow combines real (usually stolen) and fake information to create a new identity, which is used to open fraudulent accounts and make fraudulent purchases. Synthetic identity theft allows the criminal to steal money from any credit card companies or lenders who extend credit based on the fake identity.

viii. Tax Identity Theft

One of the major identity theft categories is tax identity theft. The most common method is to use a person's authentic name, address, and Social Security Number to file a tax return with false information, and have the resulting refund direct-deposited into a bank account controlled by the thief. The thief in this case can also try to get a job and then their employer will report the income of the real taxpayer, this then results in the taxpayer getting in trouble with the IRS.[5]

Extent and Patterns of Identity Theft

The Federal Trade Commission (FTC) provides the best available estimates of the extent and distribution of identity theft from its victimization surveys and database of consumer complaints. A recent estimate, produced by a study modeled after the FTC's original 2003 methodology, suggests that 9.3 million adults were victims of some form of identity theft in 2004.[10] This may represent a leveling-off from the FTC's previous finding of 9.91 million in 2003.[10]. Although the incidence of identity theft differs by State, region, and, to some extent, age, the available data suggest that all persons, regardless of social or economic background, are potentially vulnerable,

especially to those types of identity theft that occur when an offender steals a complete database of credit card information.[6]

Stages of Identity Theft

Three stages of identity theft have been identified. A particular crime of identity theft may include one or all of these stages.

1. **Stage 1**: Acquisition of the identity through theft, computer hacking, fraud, trickery, force, re-directing or intercepting mail, or even by legal means (e.g., purchase information on the Internet). [7]
2. **Stage 2**: Use of the identity for financial gain (the most common motivation) or to avoid arrest or otherwise hide one's identity from law enforcement or other authorities (such as bill collectors). Crimes in this stage may include account takeover, opening of new accounts, extensive use of debit or credit card, sale of the identity information on the street or black market, acquisition ("breeding") of additional identity related documents such as driver's license, passport, visas, health cards etc.), filing tax returns for large refunds, insurance fraud, stealing rental cars, and many more. [8]
3. **Stage 3:** Discovery. While many misuses of credit cards are discovered quickly, the "classic" identity theft involves a long period of time to discovery, typically from 6 months to as long as several years. Evidence suggests that the time it takes to discovery is related to the amount of loss incurred by the victim. At this point the criminal justice system may or may not be involved and it is here that considerable research is needed. [8]

Warning Signs and Potential Victims of Identity Theft

Warning Signs

Usually, victim may not know that he/she have experienced identity theft immediately. One could be affected by identity theft if any of the below situation are experienced: [9]

- Bills for items that were not bought or ordered
- Debt collection calls for accounts that were not opened
- Denials for loan applications
- Receipt of anonymous phone calls or text messages requesting for vital financial information such as date of birth, account number and or Bank Verification Number (BVN).

Potential Victims of Identity Theft

Anyone can experience identity theft. Children and Seniors are both vulnerable to identity theft. [9] Identity theft is a dual crime, that is, it usually affects two victims: the individual whose identity was stolen and the business whose service was stolen [Foley]. In reality, however, individuals have not always been treated as "victims," since it was assumed that they would not take ultimate responsibility for any resulting financial loss. Indeed, it seems that no one is safe from this "equal opportunity crime" (Joint hearing before the Subcommittee on Oversight and Investigations 2002).[10]

Victim Demographics [11]

- According to Identity Theft Clearinghouse data, which represent only those victims who reported their age, individuals aged 30-39 and 18-29 consistently reported more incidents of identity theft. In addition to finding that those in the 30-39 age group reported the highest incidence of identity theft, one independent survey[10] noted several additional sociodemographic trends:
- minorities reported experiencing a higher incidence of identity theft than whites;
- the incidence of identity theft increased with income;
- more males reported that someone had obtained their credit card information or forged a credit card in their name, compared to females;

- young people, aged 18-24, more often reported that someone stole or otherwise improperly obtained a paper or computer record with their personal information and used it to forge their identity;
- blacks overwhelmingly reported that a friend, relative or co-worker had stolen their identity (P&AB 2003) and
- victims with post-graduate degrees reported being victimized more frequently than college graduates or victims with a high school degree or less [10].

Children as victims of identity theft

Child identity theft may go undetected for many years. Victims may not know until they are adults, and when they applying for their own loans. There is only one source of data regarding victims under the age of 18 - the Consumer Sentinel Network. However, the data are not publicly available in disaggregated form, so the distribution of victimization across this vast age group is unknown. [11] Child identity theft may only represent a small percentage of cases (albeit based on reported incidents), but there is some anecdotal evidence to suggest that the crime may go undetected until the victim reaches an age when (s)he begins to drive, attends college, applies for various types of loans or credit accounts, or otherwise reaches adulthood.

The deceased as victims of identity theft

The number of deceased victims in the U.S. has not been estimated, although the deceased have long been recognized as "favorite targets of identity thieves" [12]. One U.K. fraud prevention service, CIFAS, has dubbed identity theft of the deceased "Britain's largest growing identity theft related crime,".

Seniors often share their personal information with doctors and caregivers and the number of people and offices that access seniors' information put them at risk.

Institutional victims

Certain groups of victims may be more vulnerable than others because of the organizations to which they belong. Students and members of the armed services may be particularly at risk. Considering the extensive use of Social Security Numbers among institutions of higher learning and students' increased opportunities for obtaining credit, a number of steps have been taken to specifically protect and educate college students about the dangers associated with identity theft.[13]

The elderly as victims

Whereas the elderly may not be specifically targeted, they are a particularly vulnerable population in general. Specifically, they are "less likely to engage in credit dependent transactions on a frequent basis and therefore are less likely to become immediately aware that they are victims of an identity thief".[14].

Repeat victimization

In relation to vulnerability, the term "repeat" or "multiple victimization" begins to take on a whole new meaning in the realm of identity theft offenses. In addition to the individual victim, several corporate victims may be involved; and any given victim may be "violated" any number of times in any number of different ways. [15].

Conclusion

As a result of conducting this study, identity theft was clearly defined, it suggested ways to prevention and mitigation of identity theft in all forms of online spaces.

Recommendations

This study not only identified the available research on identity theft, it also identified in some areas where research is still needed. The issue of reporting and recording identity theft by local police departments emerged as a major issue in need of research.

References

1. Graeme R. Newman, Megan M. McNally. Identity Theft Literature Review July 2005. Document No.: 210459. https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf. Accessed on 11/01/2022
2. Guidance on the Protection Personal Identifiable Information. US Department of Labor. https://www.dol.gov/general/ppii. Accessed on 11/01/2022
3. Wiam Younes. Identity Theft. Information Security Office (ISO) Computing Services. www.cmu.edu/computing. Accessed on 11/01/2022
4. https://www.lifelock.com/learn/identity-theft-resources/what-is-criminal-identity-theft. Accessed 11/01/2022
5. https://www.citrincooperman.com/infocus/identity-theft-tax-and-financial-consideration. Accessed 12/01/2022
6. https://www.investopedia.com/terms/i/identitytheft.asp. Accessed 11/01/2022
7. Graeme R. Newman and Megan M. McNall, July 2007. Identity Theft – A Research Review. https://www.ojp.gov/pdffiles1/nij/218778.pdf
8. Graeme R. Newman, Megan M. McNally. Identity Theft Literature Review July 2005. Document No.: 210459. https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf. Accessed 11/01/2022
9. Foley, L. (2003b). Identity theft: The aftermath 2003. Identity Theft Resource Center. http://www.idtheftcenter.org/idaftermath.pdf
10. Swartz, N. (2003). "Want the CIA Director's address? Get it for $26 online." Information Management Journal, 37(6): 16.
11. Synovate. (2003). Federal Trade Commission – Identity Theft Survey Report. McLean, VA. http://www.ftc.gov/os/2003/09/synovatereport.pdf
12. O'Brien, T.L. (2004, October 24). "Identity theft is epidemic. Can it be stopped?" New York Times, Section 3: 1,4.
13. "Legislators try to shore up campus data security holes." (2004). Recruitment and Retention in Higher Education, September:5-6.
14. Florida, Sixteenth Statewide Grand Jury. (2002, January 10). Statewide Grand Jury report: Identity theft in Florida. First Interim Report of the Sixteenth Statewide Grand Jury. http://www.idtheftcenter.org/attach/FL_idtheft_gj.pdf
15. Mativat, F., and P. Tremblay (1997). Counterfeiting Credit Cards: Displacement Effects, Suitable Offenders, and Crime Wave Patterns. British Journal of Criminology 37(2):165–183.