The University of Texas at Austin
Center for Identity

Economics of Cyber Crime: Identity Theft and Fraud

Razieh Nokhbeh Zaeem
K. Suzanne Barber

UTCID Report #20-06

MAY 2020

Economics of Cyber Crime: Identity Theft and Fraud

Razieh Nokhbeh Zaeem* and K. Suzanne Barber

Synonyms

Identity theft, fraud, abuse, and exposure.

Definitions

Identity theft and fraud is the unauthorized use of Personally Identifiable Information (PII), usually to gain financial advantage in the name of the PII owner.

Background

Identity theft, fraud, abuse and exposure involves the misuse of a victim's identity, particularly the use of the victim's personally identifiable information, without permission. There are a variety of different ways in which a one's PII can be compromised. There might be a data breach at an organization that maintains personal information. Physical theft of one's mail, wallet, purse, or laptop can result in his PII falling into the wrong hands. Social engineering techniques, such as e-mail phishing or telephone scams, are often successful in duping victims into revealing personal data. Old-fashioned snooping, such as overhearing another's telephone conversation, going through their trash bins, or looking over someone's shoulder at an ATM can yield sensitive personal information.

Once compromised, a person's PII can be misused in various ways. To name a few of the most common: An identity thief might put fraudulent charges on existing accounts or open new accounts in the victim's name; the accounts in question might be

* corresponding author

financial (e.g. credit cards or loans) or utility-based (e.g. electric or telephone) Romanosky et al (2011). With a few choice bits of another person's PII, fraudsters can file a tax return (and collect a refund), obtain health-care services, or get a job in that person's name.

The potential harms to victims of identity theft and other forms of PII compromise are multi-fold. They include: invasion of privacy, financial loss, loss of physical or intellectual property, reputation damage, effort and money spent to recover from the incident and prevent further misuse of the compromised PII, and emotional distress (over any or all of the above) Milne (2003).

Identity theft, fraud and related crimes are increasingly common occurrences. According to the 2016 U.S. National Crime Victimization Survey by United States Department of Justice (2019b), at least 25.9 million Americans were affected by identity theft and fraud in the previous year. In the consumer sentinel network from the Federal Trade Commission (FTC), identity theft and fraud are one of the top categories of scam reported to the agency, to which people lost more than $1.9 billions in 2019. Identity theft is a costly problem with constantly evolving patterns of criminal tactics and behaviors Van der Meulen (2011).

As more businesses and people become victims of identity crimes, it is increasingly important to better understand the crimes of identity theft, fraud, and abuse in an effort to reduce or even halt this crime. While statistics have been gathered regarding the number of exposed records or the financial loss to individuals Identity Theft Resource Center (2019); Privacy Rights Clearinghouse (2019), few efforts have researched how identity theft actually occurs. There are best practices and prevention tips from security companies and government agencies available FTC (2019); United States Department of Justice (2019a); LifeLock (2019). However, there is a lack of aggregated data detailing the process of stealing someone's identity. Most information available focuses on reactive measures, which are helpful once an identity is stolen, but brings us no closer to ending identity-related crimes or, at least, making identity theft more difficult for the criminal.

Collection of Identity Theft and Fraud Data

Previous work has introduced several avenues of collecting identity theft data.

Agency Data

The first commonly used source of identity theft data is gathered from agencies Consumer Sentinel Network (2019); Allison et al (2005); Harrell et al (2015). For example, the FTC's Consumer Sentinel Network (2019), established in 1997, is a database which collects identity theft complaints from FTC's telephone- and web-based complaint systems in addition to more than one hundred federal and state organizations. While comprehensive, this database is available only to law enforcement. Even though some have raised concerns (e.g., Newman and McNally (2005)) towards the representativeness of Con-

sumer Sentinel Network and other agency data, researchers still use agency data widely, while making an effort to manage the amount of data in such databases Quick and Choo (2016, 2014).

Surveys

Synovate on behalf of the FTC, Javelin Strategy and Research (2014), and several other universities and research organizations have conducted national surveys about identity theft and fraud. Apart from great variance in their sample sizes and some differences in methodologies, such surveys have been criticized (e.g., by Newman and McNally (2005)) for issues such as non-response bias, difficulty to contact victims (especially because victims of identity theft sometimes have to change their contact information), and relying solely on the memories of victims.

Interviews

Interviews with victims is a primary means of collecting identity theft data for research in academia Mancilla and Moczygemba (2009); Betz-Hamilton (2020); Anderson et al (2008).

There is some research that is based on interviews with identity thieves and fraudsters Copes and Vieraitis (2009). Such interviews can provide great details about the methods these criminals use. Still, this type of research is likely to be limited by small sample sizes (59 offenders were interviewed by Copes and Vieratis) and skewed by the fact that their subjects are all perpetrators who were caught, incarcerated, and willing to be interviewed.

News Stories

News stories have been used for identity theft data collection Morris (2010); Zaiss et al (2019); Zaeem et al (2017). News stories have several important characteristics that make them an appropriate source of data: There is a tremendous amount of news stories about identity theft; They are widely available, as opposed to agency data that is difficult to obtain from government agencies or corporations; Finally, most news stories are reliable and trustworthy since the news media is responsible for providing accurate information to the public and are held accountable. This source complements other sources by focusing on news articles that narrate a wide range of identity theft stories, from victims, law enforcement, and companies. This source, too, has some bias. The news media tends to report stories that are considered newsworthy.

Reports from Affected Organizations

Organizations affected by data breaches that lead into identity theft and fraud sometimes report their own data. Examples are Gemalto (2017); Baker et al (2011).

Anecdotal Information

One other source of data about identity theft is through victim case studies. While this source highlights the worst possible scenarios, it is the least reliable and most biased.

Open problems and Future directions

The above-mentioned sources of identity theft and fraud data are usually in human-readable formats. Structuring and automating the extraction of identity theft and fraud data is a promising research avenue that is gaining traction. Furthermore, these data sources are commonly collected independently and separately. The data sources can complement one another if combined or collected in tandem.

Cross-References

Privacy metrics and data protection: Personally Identifiable Information

References

Allison SF, Schuck AM, Lersch KM (2005) Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. Journal of Criminal Justice 33(1):19–29

Anderson KB, Durbin E, Salinger MA (2008) Identity theft. Journal of Economic Perspectives 22(2):171–192

Baker W, Goudie M, Hutton A, Hylender CD, Niemantsverdriet J, Novak C, Ostertag D, Porter C, Rosen M, Sartin B, et al (2011) 2011 data breach investigations report. Verizon RISK Team, Available: www verizonbusiness com/resources/reports/rp_databreach-investigationsreport-2011_en_xg pdf pp 1–72

Betz-Hamilton A (2020) A phenomenological study on parental perpetrators of child identity theft. Journal of Financial Counseling and Planning

Consumer Sentinel Network (2019) Data book for January - December 2019. URL https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf

Copes H, Vieraitis LM (2009) Understanding identity theft: Offenders accounts of their lives and crimes. Criminal Justice Review 34(3):329–349

FTC (2019) Federal trade commission consumer information. URL hhttp://www.consumer.ftc.gov/features/feature-0014-identity-theft

Gemalto N (2017) Mining for database gold: Findings from the 2016 breach level index,

Harrell E, Bureau of Justice Statistics, US Dept of Justice, Office of Justice Programs (2015) Victims of identity theft, 2014

Identity Theft Resource Center (2019) Data breaches. URL http://www.idtheftcenter.org/id-theft/data-breaches.html

Javelin Strategy and Research (2014) Identity fraud report: Card data breaches and inadequate consumer password habits fuel disturbing fraud trends

LifeLock (2019) Lifelock. URL http://www.lifelock.com/nw

Mancilla D, Moczygemba J (2009) Exploring medical identity theft. Perspectives in health information management/AHIMA, American Health Information Management Association 6(Fall)

Van der Meulen NS (2011) Bettween awareness and ability: Consumers and financial identity theft. Communications & Strategies 81:23–44

Milne GR (2003) How well do consumers protect themselves from identity theft? Journal of Consumer Affairs 37(2):388–402

Morris RG (2010) Identity thieves and levels of sophistication: Findings from a national probability sample of american newspaper articles 1995–2005. Deviant Behavior 31(2):184–207

Newman GR, McNally MM (2005) Identity theft literature review. United States Department of Justice: National Institute of Justice

Privacy Rights Clearinghouse (2019) Privacy rights clearinghouse. URL https://www.privacyrights.org

Quick D, Choo KKR (2014) Data reduction and data mining framework for digital forensic evidence: storage, intelligence, review and archive. Trends & Issues in Crime and Criminal Justice 480:1–11

Quick D, Choo KKR (2016) Big forensic data reduction: digital forensic images and electronic evidence. Cluster Computing pp 1–18

Romanosky S, Telang R, Acquisti A (2011) Do data breach disclosure laws reduce identity theft? Journal of Policy Analysis and Management 30(2):256–286

United States Department of Justice (2019a) Identity theft. URL http://www.justice.gov/criminal/fraud/websites/idtheft.html

United States Department of Justice (2019b) National crime victimization survey: Identity theft supplement, 2016. DOI 10.3886/ICPSR36829.v1

Zaeem RN, Manoharan M, Yang Y, Barber KS (2017) Modeling and analysis of identity threat behaviors through text mining of identity theft stories. Computers & Security 65:50–63

Zaiss J, Nokhbeh Zaeem R, Barber KS (2019) Identity threat assessment and prediction. Journal of Consumer Affairs 53(1):58–70

WWW.IDENTITY.UTEXAS.EDU