Frankenstein Fraud: The Rising Threat of Synthetic Identity Theft

By Kevin Naranjo
Tufts University
December 12th, 2018

Abstract

While the issue of identity theft has been around for several decades, these past few years have seen an evolution in the strategies used by its perpetrators. Traditionally, criminals performed what was known as true name fraud, where they stole a victim's personal information and impersonated them while making large purchases under their name. Eventually, credit lenders and banks caught on to what was going on and put into place security measures to decrease the likelihood of this happening. In response, these criminals moved onto a harder to detect scheme known as synthetic identity theft. This new strategy consisted of piecing together a fake identity using real information from several different victims, such as addresses and Social Security numbers. They then developed credit for this fake identity and proceeded to spend it all with no plans of ever repaying it. Since there is not a single concise victim, it is easier for the thieves to go undetected for longer periods of time. Recently, this method has become so popular among identity thieves that the Federal Trade Commission reported that it made up 80-85% of all identity theft in 2017[1]. Despite the rising number of occurrences, many people are still unaware of this new threat. This paper seeks to remedy that by discussing the details of synthetic identity theft and the steps people can take to prevent themselves from being victimized.

Introduction

The amount of damage caused by synthetic identity theft has been steadily on the rise for the past few years. A study done by Aite Group states that around $820 million have been lost to this type of fraud in 2017, which is a 17 percent increase from the $701 million loss in 2016[2]. To make matters worse, they estimate this amount will continue to increase so that by 2020 identity thieves will have stolen $1.2 billion. In reality, these numbers are likely higher since it is often difficult for lenders to tell the difference between when an actual borrower has defaulted on a loan versus when a fraudulent identity has gone out of commission. These numbers also do not consider the amount of time and effort expended by lenders trying to track down and collect from individuals who never existed in the first place.

There are several factors that contributed to the increased prevalence of synthetic identity theft. One of the first being the introduction of chip-enabled cards (EMV) back in 2015[3]. Since these new cards made point-of-purchase fraud increasingly difficult, many of the fraudsters had to adapt and find a new method to keep income coming in. By siphoning off the credit of fake

identities they created, they could easily circumvent this new security measure. The second contributor to the sudden rise in synthetic identity theft was ironically a change made by the Social Security Administration to reduce the amount of identity theft cases. Originally, Social Security numbers consisted of a three-digit geographic number, a two-digit age group number, and a four-digit serial number[4]. This made it easier for lenders to see if a potential borrower's date of birth and address matched up with their Social Security number. However, in 2011 the agency began to randomize the generation of new Social Security numbers so that fraudsters could not attempt to reconstruct peoples' numbers based on public records. This randomization now made it impossible for a lender to verify if a Social Security number truly fit with the other personal information provided by a borrower. So now that other methods of identity theft were becoming unsustainable and lenders were having a hard time verifying the legitimacy of new borrowers, it is no surprise that many fraudsters decided to migrate to creating fake identities.

To the Community

Often when the topic of identity theft is brought up, people do not consider themselves potential victims. However, according to a recent study, 16.7 million Americans fell prey to identity fraud in 2017[5]. Based on previous trends, there will be a lot more victims in the years to come. Therefore, it is a lot more likely to occur to a person than they might think. Even though it is only a fragment of a victim's identity that is used for the fraud, there are still large repercussions that can occur for the victim. For example, every synthetic identity fraud creates a fragmented credit file which consists of the credit history generated by the fake identity. This file is tied to the actual Social Security number of the victim[4]. So, if this file has negative information, such as a defaulted loan, it can negatively affect the victim's credit rating even though the name and date of birth do not match. The worst part is that fragmented credit files are usually not picked up by credit blocks and alert notification services. The process of getting this issue cleared up is typically a nightmare and is made worse the longer the pieces of the victim's identity were in use. It is impossible to defend against an unknown attack and since every person could be a potential victim, it is crucial that the entire community is made aware of the dangers that arise from synthetic identity theft.

Fraud Methodology

The first step a fraudster takes when performing synthetic identity theft is gathering the pieces of personal information they are going to use to craft their fake identities, such as addresses and Social Security numbers. Currently, the easiest way to do this is to search online for private records that were compromised during the thousands of data breaches that happen each year[6]. These criminals hit the jackpot in 2017 when Equifax was compromised, resulting in the exposure

of 145.5 million Social Security numbers among other things[7]. Once they have enough pieces of personal information from different people, the fraudsters can then stich together a cohesive synthetic identity to defraud lenders.

The next step is to use the fake identity to apply for some credit from a lender, such as a credit card. When this happens, the borrower's application is sent to the credit reporting agencies (CRAs) which are Equifax, Experian, and TransUnion. The CRAs then look for a credit file for the borrower, which includes their credit history and other financial information such as foreclosures. Since this identity is brand new, there will be no preexisting credit file, so the application will get declined. However, any application submitted to the CRAs will create a credit file if one does not already exist[8]. As a result, any future applications for credit made with the fake identity will return a credit file, albeit thin, which will increase the chances that the application gets accepted. Eventually, when they get a few small credit lines open, the fraudsters will legitimately use the credit cards and pay them off each month to establish good credit. They continue this façade until the limits on their credit accounts are high enough, after which they 'cash out' by quickly spending all the money on each account on things such as gift cards and expensive electronics which can be resold later. Some fraudsters even pay back the debt with fraudulent checks, and then proceed to 'cash out' again before the checks bounce[8]. This allows them to essentially steal twice the amount of cash they had on their lines of credit. Once that's done, they throw out the identity and move on to another one.

The main issue with the previous strategy is that it takes many months of diligent work to build up a decent credit score from nothing. To speed this process up, many fraudsters try to get added as authorized users on the accounts of people with excellent credit. After a short period of being an authorized user of a credit line, the credit lender reports it to the CRAs, which adds it to the fake identity's credit file. This essentially allows the fraudster's fake identity to inherit the good credit rating of the account they were piggy-backing off. Once they inherit the good credit, they can then be removed as authorized users but still retain the newly attained high credit score[8]. Fraudsters usually get added as authorized users by either paying others to let them join for a short period or pretending to be in dire need of credit repair assistance.

A more complex strategy is known as data-furnishing. To do this, the fraudster must have access to a fake business or a business that has been compromised by someone willing to commit fraud. The way it works is that the 'business' grants a credit line to the synthetic identity to pay off expensive merchandise from the store. The 'business' then reports to the CRAs that the synthetic identity has been making all of their monthly payments, which will in turn boost their credit score. Once their credit score is high enough, they'll be able to get other credit lines with relatively high limits, which they can proceed to max out like in the previous methods. One thing that can give this method away is if the synthetic identity has credit on the account that is worth a lot more than the products that the 'business' is selling[8].

Fraudsters typically use several fake identities at the same time to maximize their efficiency. Take for example a Georgia man who had over 300 synthetic identities, with each one having several credit accounts opened. In over the course of two years, this man managed to

defraud lenders out of $350,000[9]. Other fraudsters find it more beneficial to form a group where they collectively manage many synthetic together and share the profits. That was the case back in 2013, when the FBI shut down a fraud ring consisting of 18 people. Together they managed 7,000 fake identities and stole over $200 million from credit card companies[10].

Typical Victims

To maximize the amount of time they can operate undetected, synthetic identity thieves often target victims with thin or non-existent credit files that are unlikely to be monitored. Which is why, according to a study by CyLab, children are 51 percent more likely to have their Social Security number used for synthetic identity fraud[11]. Since children are not expected to have a credit file because they are too young to perform any of the actions that could generate one, many parents will not check. The real issues begin to arise years later when the child attempts to apply for a credit card or for college loans and they find out they already have a credit file that is several years old. Since Social Security numbers are randomized for children born after 2011, it is possible for fraudsters to make an identity using a child's social security number with the date of birth of a middle-aged man. Resolving that mess of identity theft would likely take months of work and years of credit repair. Therefore, it is the parent's responsibility to ensure that their child does not become a victim by looking out for any strange signs, such as credit card offers being sent to the child. However, just because a child is more likely to be targeted does not mean that adults are safe at all.

Action Items

To help reduce the number of synthetic identity theft cases, the government enacted the Economic Growth, Regulatory Relief and Consumer Protection Act last May. Under Section 215[12], a new mechanism was created for the Social Security Administration that allowed banks to electronically check the name and birth date associated with a given Social Security number, with responses being available in 24 hours. If this system is implemented correctly, it will become a major deterrent for synthetic identity theft.

However, it is still unknown how long it would take the government and the banks to implement such a system, so until then it is up to the consumer to take care of their own identity. The site *annualcreditreport.com* allows one free credit report from each of the 3 CRAs every year. Therefore, one's credit report can be checked every 4 months to ensure that there are no anomalous activities. Due to their high risk, children's credit reports should also be monitored as well. If there are strange charges, make sure to contact the credit agencies and dispute it.

Another thing to monitor is annual Social Security statements. If the fraudster uses the fake identity to acquire some form of employment, their income would be reported on the victim's statement. Therefore, it is important to make sure that the amount of income listed in the statement

matches up with the income earned for the year. If this is not the case, make sure to contact the Social Security Administration.

Lastly, don't always dismiss cases of mistaken identity so quickly. Constantly receiving somebody else's credit card bills in the mail might be a sign that the address is being used as part of a fraudster's fake identity. Better to be safe and contact the sender of the mail informing them of the situation.

Conclusion

It is clear now the threat that synthetic identity theft poses to both lenders and consumers. By taking personal information from consumers that becomes exposed during the constant data breaches, these fraudsters can cobble together their own fake identities. These usually cannot be detected by most lenders due to the lack of verification when it comes to matching Social Security numbers to other identifying information, such as name and date of birth. Typically, the way that identity theft gets reported is if the victim notices something suspicious is happening with their information, like new charges on their credit card or a new credit card in their name. However, with synthetic identity theft, there is no single victim whose entire identity is stolen, therefore, it is not likely that someone will discover what the thief is doing and report it. Sadly, due to their fresh record that will go unchecked for years, children often become the main target of these thieves. To make matters worse, the resulting consequences will not be apparent until years after the crime has already been committed. While it currently may not be possible to prevent one's information from being used if it has already been compromised, one is still able to ensure that whatever damage may come is mitigated by being careful and staying vigilant. Monitoring credit reports and spreading awareness are two of the best ways to combat the spread of synthetic identity theft which everyone should take part in.

References

1. Britnelll, Lanny. "The Changing Face of Identity Theft." *Federal Trade Commission*, www.ftc.gov/sites/default/files/documents/public_comments/credit-report-freezes-534030-00033/534030-00033.pdf.

2. Conroy, Julie. "Synthetic Identity Fraud: The Elephant in the Room." *Digital Banking Customer Engagement: Aite Group*, 3 May 2018, www.aitegroup.com/report/synthetic-identity-fraud-elephant-room.

3. Kossman, Sienna. “The Big Chip Card Switch: Living with EMV.” *CreditCards.com*, 29 Aug. 2017, www.creditcards.com/credit-card-news/emv-chip-cards-one-year-later-consumer.php.

4. “Synthetic Identities Are One of the Fastest Growing Forms of Identity Theft.” *National Credit Union Administration*, 20 Sept. 2018, www.ncua.gov/newsroom/Pages/ncua-report/2018/third-quarter/synthetic-identities-fastest-growing-forms-identity-theft.aspx.

5. Pascual, Al. “2018 Identity Fraud: Fraud Enters a New Era of Complexity.” *Javelin*, Greenwich Associates LLC, 6 Feb. 2018, www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity.

6. “Over 2,300 Data Breaches Disclosed So Far In 2018, Exposing Over 2.6 Billion 5ords.” *Risk Based Security*, 15 Aug. 2018, www.riskbasedsecurity.com/2018/08/over- 2300-data-breaches-disclosed-so-far-in-2018-exposing-over-2-6-billion-records/.

7. Chirgwin, Richard. “Equifax Reveals Full Horror of That Monstrous Cyber-Heist of Its Servers.” *The Register® - Biting the Hand That Feeds IT*, 8 May 2018, www.theregister.co.uk/2018/05/08/equifax_breach_may_2018/.

8. D'Alfonso, Steven. “Synthetic Identity Theft: Three Ways Synthetic Identities Are Created.” *Security Intelligence*, IBM, 28 Oct. 2014, https://securityintelligence.com/synthetic-identity-theft-three-ways-synthetic-identities-are-created/

9. “Identity Thief Sentenced for Using a New Form of Fraud ‘Synthetic Identities.’” *The United States Department of Justice*, U.S Attorney's Office, 28 Apr. 2017, www.justice.gov/usao-ndga/pr/identity-thief-sentenced-using-new-form-fraud-synthetic-identities.

10. “Eighteen People Charged in International $200 Million Credit Card Fraud Scam.” *FBI*, U.S Attorney's Office, 5 Feb. 2013, https://archives.fbi.gov/archives/newark/press-releases/2013/eighteen-people-charged-in-international-200-million-credit-card-fraud-scam.

11. Power, Richard. “Child Identity Theft.” *CyLab*, Carnegie Mellon, 2011, www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf.

12. United States, Congress, “Economic Growth, Regulatory Relief, and Consumer Protection Act (P.L. 115-174) and Selected Policy Issues.” 24 May 2018. 115th Congress, bill 2155. https://www.congress.gov/bill/115th-congress/senate-bill/2155