Identity Theft - Detection, Mitigation, and Protection

Ashley Aguilera Rico, Raveen Bryant, Ryan Foster, Yen Hsieh Hsu, Abby Nguyen
University of Louisville
CIS 481
Professor Andrew Wright
August 9, 2022

Table of Contents

Identity Theft - Detection, Mitigation, and Protection

Identity theft is when an individual's private information (ex: social media login, social security, etc.) is acquired fraudulently by another person or organization, and then used for their own personal gain, despite what consequences it might cause to the individual whom they stole from. It is a serious crime and the effects it has on its victims are hard to reverse. It costs a lot of money and time to be able to prove your innocence to crimes committed by someone else using your identity, and it can affect your reputation as people can maliciously ruin your appearance on social media sites. On average, identity theft takes 6 months to resolve and recover from, and sometimes the damage is irreversible. It is important to keep your personal information private, and be wary of anything that asks for personal information, or of keeping your private information secure and not easily accessible to others. Some things as simple as throwing away a bank statement in the trash, can lead to someone using your funds after finding your private information in the trash. Identity theft is easy to fall victim to, but there are ways to prevent it, especially as things become more digital and the issue becomes more common. It is important to recognize and learn about the causes and effects of identity theft, and what an individual can do if they were to fall victim to it.

Background

Identity theft has been an ongoing problem ever since the 1960s and has only gotten worse once the pandemic hit. It affects thousands of Americans across the country, with an estimate of 2.8 million frauds reported in 2021, and will only continue to affect people around the world, not only Americans. People are only aware of certain cases of identity theft, such as credit card fraud and bank account fraud, but there are other ways that identity theft can happen and the effects that it can have on someone's life. There isn't a lot of awareness about the impact of identity theft and how it can affect someone's entire life. The lack of emphasis on the importance of identity protection is part of the reason that people fall victim to identity theft. As the problem becomes more prevalent, we must analyze the causes, the effects, and the actions that are taking place due to identity theft. Entering more of the digital era has advanced ways in which identity theft can happen, but also means that there have been more developed ways to protect your information and identity.

How Does Identity Theft Happen?

Identity theft can happen in a myriad of ways. Depending on what part of your identity was stolen can help identify what kind of identity theft can occur, or will occur. An example of this, is if your bank account information was compromised, then more than likely the thief will liquidate your funds, or use them for their own benefit. Most identity theft occurs over the internet, through phones, and sometimes in-person through odd methods. Some ways that identity theft can happen is through phishing, data breaches, skimming, dumpster diving, wifi-hacking, phone scams, malware, and mail theft (*Identity theft: What is it and how to avoid it*, n.d.). All these methods are utilized in order to gather private information from an individual whether it be something as simple as a birthday, or as complex as a whole document(s) such as medical records or a birth certificate. This is why it is very important to maintain private information private and accessible to very few and in a secure area. It does not take a lot of private information for your identity to be compromised, so it's always important to be diligent about what information is shared and where it is placed.

What Demographics are Most Targeted by Identity Theft

While it is extremely true that anyone can be a victim of identity theft, including businesses and organizations, criminals like to target vulnerable demographics to maximum theft potential and result. Many of these populations do not understand they are disproportionately at risk nor are they aware of the steps to take to prevent this.

Senior Citizens

Senior citizens over the age of 60 make upward to 20% of annual identity theft. One of the reasons why senior citizens are targeted is because they are more trusting and usually are more likely to need assistance with even basic personal and technical demands. This increases their interactions with ill intentioned people disguised as offering genuine aid and assistance. They are also targeted as they are usually more financially stable with multiple assets that they may not monitor frequently. Many people not raised in this generation of technology often do not understand how sophisticated criminals and hackers have become. This also means they do not commonly participate in preventive action as they simply are uneducated on the risks. This also means they are less likely to have electronic accounts that would help detect fraudulent activity for

them. They usually rely on physical documents or in person visits to synchronize and help maintain their accounts. This unfortunately may not be done frequently and increases the window of damage and infiltration.

Children

Another demographic unfortunately targeted by identity theft are children. Now while children usually do not have many accounts the one's they do have may not be monitored well as their parents are preoccupied and since they usually lack financial independence they are unaware as well. Something more disheartening about identity theft involving children is that it is usually someone they know personally and trust. So a parent, foster parent or legal guardian, and any other family with access to the child's personal identification records are more likely to attempt fraud using their information. Not only is this a disgustingly cruel betrayal especially to a child, many children are unaware that this event occurred until they are old enough to check their own credit and personal records and see interactions they do not recognize. This often puts them in a terrible position where they are left to clean up the consequences or they can report said activity and family as fraudulent.

Young Adults

This may be surprising but young adults who are a part of "tech savvy" generations are also victims of identity theft at alarming rates. This may come at a shock as though many of these young people grew up when identity theft protection, prevention, and mitigation was actively being denounced and taken as the threat it truly presents. This can be because young adults have much larger digital footprints via multiple social media's and webpages unintentionally leaking personal details to be exploited by criminals looking to take advantage of them. Some young adults are confident in their own downfall thinking they can never be a victim of this crime until it unfortunately happens and they wish they were more preventative.

Types of Identity Theft

Given the prevalence of Identity theft in the modern era there are numerous different ways of stealing the identity of an individual or even impersonating or stealing the information of companies in some way or another. The most prevalent and widespread forms of identity theft include, but aren't limited to: Financial Identity Theft,

Tax Identity Theft, Medical Identity Theft, Employment Identity Theft, Criminal Identity Theft, Synthetic Identity Theft, and Child Identity Theft (*Types of Identity Theft,* n.d). There are many other forms of Identity Theft that are known but the ones listed above are the most widespread in their use and are very difficult to find and protect against.

Financial Identity Theft

Financial Identity Theft is likely the most basic form of identity theft as it is the most primal reason for committing the crime in the first place: to obtain financial information and funds illegally from another individual ("Financial Identity Thefts Still Exist.," 2009). Financial Identity Theft is by far the most common form of Identity Theft and can be done in the cyber world of the internet or it can be done offline with more basic ways such as mailing fraud and phishing attacks against naive individuals. Two examples of Financial Identity Theft would be: the direct theft of a credit card to make illegal purchases using your credit card and stealing a social security number of an individual to open accounts or apply for loans in the individual's name. Both of these are forms of identity theft and damaging to an individual. Both of these can also be done in the cyber realm; credit card information can be stolen using various hacking means such as hacking a website and gaining access to credit card information or sending out false emails to a naive and unsuspecting individual asking for their social security number ("Financial Identity Thefts Still Exist," 2009).

Tax Identity Theft

Tax Identity Theft is simply when a criminal or fraudster files a tax return in the name of an individual whose information they have stolen through various different means, most likely they will make falsified claims about inflated income to try to receive a larger than normal refund from the IRS (Falsetta, 2020). This can be considered something of a "Second Step" Identity Theft type since it requires some information to be stolen from an individual that has already, currently, or will be used for other forms of Identity theft such as Financial Identity Theft. Scammers may make attempts to call an individual and pretend to be from the IRS to elicit information from the unsuspecting individual or to convince the individual not to file a tax return or not to expect one that year. This may be to cover the tracks of the fraudster and prevent two different tax returns from arriving at the IRS which would be flagged quickie for investigation. Mail

Fraud could also be used to obtain information from individuals. There could be receipt of unfamiliar tax documents, transcripts, or other various forms that should be heavily scrutinized. There must also be great caution when choosing a tax preparer, always watch if the preparer signs the documents or has the inability to explain discrepancies as this will be an indicator of possible tax fraud in your name. One of the most dangerous aspects of non tax compliance through identity theft is the reduction in trust of the IRS, as trust in the premier tax authority deteriorates then compliance will also falter and will create long term issues with general taxation (Falsetta, 2020).

Medical Identity Theft

Medical Identity Theft is when a criminal or fraudster will steal medical information using various different means such as phishing, dumpster diving, hacking attempts, and other means, to receive medical benefits in your name or apply for rebates and reimbursement for services rendered or prescriptions filled (Levin, 2015). A thief typically will pose as an individual whose identity they have stolen in order to receive medical treatments or even receive surgery. This is especially hard to detect since you won't know there has been fraud until you receive a bill in the mail but the real danger may come from the fact that fake treatments become part of your permanent record which may result in misdiagnosis later in life. Medical Identity Theft is one of the costliest types of identity theft as more than two-thirds of victims report losing more than $13,500 on average (*Medical Identity Theft: Stop Insurance Fraud - Debt.Com*, n.d.).

Employment Identity Theft

Employment Identity theft is when fraudsters or criminals will use an individual's personal information stolen through various means to apply for and obtain a job; this can be especially irritating for the victims since they will receive communication from the IRS about discrepancies in their tax return and will have to show they did not receive the additional wages as well as prove the fraud (Schreiber, 2016). Great caution must be taken when applying for a job, stay alert for any sharing of bank account information with employers that you have yet to have an interview with and only ever give personal information to employers after you have performed your own due diligence on the company. This type of identity theft is assumed to be on the rise with the proliferation of

the “remote working” culture, this makes it much easier for fraudsters to appear legitimate as they need not show physical assets or physical interviews.

Criminal Identity Theft

Criminal Identity Theft is an interesting type of identity theft as this one pertains exclusively to another crime already being performed and your personal information is used in lieu of their own to place the responsibility of the consequences of the previously mentioned crime on you, the unsuspecting victim (Perl, 2003). Perpetrating crimes as the victim can cause irreparable damage to a victim in numerous ways: there can be severe backlash in the victim’s local community as word spreads of misdeeds that they never actually perpetrated, employers can be made aware of the crimes that were falsely committed in the victim’s name which will cause confusion or loss of employment, some crimes that require fines to be paid may never be discovered by the victim until there are warrants out for their arrest due to the unpaid fines, and wages or other monetary penalties could be garnished due to certain kinds of crimes committed in the victim's name (Perl, 2003). Criminal Identity theft is another form of secondary identity theft as it requires the personal information to already be acquired and used in order for it to be effectively used in a crime. The fraudster must also be rather competent and have the stolen identity well made or suitably changed to their environment in order to get past the investigations of law enforcement officers, even if it's only a routine traffic stop.

Synthetic Identity Theft

Synthetic Identity Theft is another interesting form of identity theft and is one of the more recent variations of it. Synthetic Identity Theft is when fraudsters or criminals create an entirely new pseudo-individual using various different forms of real information from many different people. They may use the social security number of one person, the name of another person, the address of an additional person, and the bank account information of a fourth person to form something of a “frankenstein” fake person (Lutz, 2017). Synthetic Identity Theft is extremely difficult to combat since it requires lenders and other institutions to look through each individual piece of personal information on its own and validate individually. This is very time consuming and there’s now a growing trend of fraudster “piggybacking” on consumers credit scores; the consumer will simply

add the fraudster to their credit profile or file and any checks into that fraudsters credit will reflect the consumer's credit history and be passed through inspection (Lutz, 2017).

Child Identity Theft

Child Identity Theft is mostly when children under the age of 16, who don't have credit reports, have their information stolen which is then used to open accounts in their name such as credit cards, bank accounts, loan applications, and other forms of financial services (Woolley, 2017). This is very difficult to detect because, as stated previously, children don't have credit reports or credit files and it can be a decade before a child or the parents first discover that the child's identity has been stolen, typically when the child gets their first job or when they make applications for scholarships only to find they have an extensive credit history from the time they were two years old. There's not much to be done to detect Child Identity Theft other than the parents to be proactive. They must search their child's social security number and other information through the credit reporting agencies to determine if there is anything suspicious. Parents should check their children's information at least once a year to ensure their children's identity is safe.

Identity Theft Detection

Identity theft detection has many different aspects to consider. Given that there are many different forms of identity theft, you must take certain steps depending on what kind of identity theft has occurred. Financial identity theft requires the constant overwatch of your bank accounts, credit cards, and other personal financial information. Tax Identity Theft requires you to be prompt in your tax filings and maintain a watchful eye on their IRS reports. Medical Identity theft requires that an individual keep their personal medical records in a secure place and review the Explanation of Benefits from any statements from a medical institution. The first time a bill of unknown origin for medical services arrives, then immediately notify the hospital and seek assistance.

Employment Identity Theft can, again, be detected only after receiving unknown correspondence from an employer or checking the federal government's E-Verify ite to see what employers have checked records. Criminal Identity Theft is detectable when warrants or summons for court arrive, it is very difficult to detect and fight. Synthetic Identity Theft is detectable along the lines of other identity theft types, once a financial

statement arrives in the mail or there are irregularities in financial information there is little time to find it and mitigate the damage. Child Identity Theft is the most challenging to detect as it can go on for decades with a child not having a credit report until the age of 16 in most cases. This means a fraudster can effectively use a child's identity since birth without much worry for the next 16 years.

Individual and Business Responsibility in Identity Theft Mitigation & Protection

Individuals and business have an intrinsic responsibility to assist in the mitigation and protection of identity theft in all of its forms. Businesses especially have a responsibility to protect their consumers from data breaches and other forms of Identity theft. The Federal trade Commission (FTC) gives the following guidance to assist business and individuals in making smart and informed decisions when identity theft occurs. Notifying Law enforcement of the theft as a compromise could very well result in harm to an individual or business, the FTC recommends finding the nearest office of the Secret Service or the Federal Bureau of Investigation (FBI) and inform them of the details. Businesses also have an obligation to notify any individuals and give any kind of recompense resulting from their lack of data protection; this can be hard to prove as gross negligence must be proven in order to be reimbursed for any damages or potential damages (*Data Breach Response*, 2019). Businesses have a responsibility to take measures in keeping up their protections from data breaches with updated technology and methods. And finally, individuals have a personal responsibility to make getting their data as difficult as possible with their own personal protections and being aware that their information is valuable and never safe.

Strategies to Combat Identity Theft

As mentioned previously, identity theft is an ongoing global problem that has been getting worse. Throughout the years, with the increasing use of technology and the rise of identity theft, there have been many methods to detect, mitigate, and protect against identity theft, yet no actual solution has been found that can eliminate the problem. Even though there is no solution, there are different strategies to combat identity theft, in addition to the ones that were mentioned above.

Identity theft has several stages in its life cycle, and each of those stages must be attacked. Some of these stages include the moment the identity thief attempts to

acquire someone's personal information, when they attempt to use the information, and after the information has been used by the identity thief. Based on the book *Combating Identity Theft: A Strategic Plan* (2007), the federal government has suggested some strategies that address the above mentioned stages: to keep sensitive data away from identity thieves, making it difficult for identity thieves to obtain consumer data, assist victims of identity theft, and deterring identity theft with lawful punishments. Below are some of the suggested measures detailed in the book.

Protecting Consumer Data in the Public and Private Sector

To protect consumer data, is to keep the information out of the hands of criminals. Identity theft can only happen when identity thieves obtain the information. The first step to reducing identity theft is to reduce the opportunities identity thieves have to obtain the data. For this to happen, governments, businesses and organizations, and consumers are all responsible and play a role in protecting the data.

Identity thieves tend to look for places with a rich amount of consumer data. Data breaches are the most common way consumer data gets leaked and for identity thieves to obtain the consumer data. Depending on the type of data leaked, some consumers may be exposed to the threat of identity theft. Although there is no such thing as a perfect security or a real solution to identity theft, entities such as governments, businesses, and organizations should take steps to ensure that sensitive consumer information is protected. There are a lot of inexpensive and readily available options that can be used to maintain security, and with new developments in security technologies, data compromises can be lessened. But, there are still some entities that fail to implement basic security measures, which results in security and data breaches.

Both public and private organizations tend to collect a lot of consumer information. Public entities especially, such as federal agencies, may collect more personal information that can often be used to commit identity theft if the thieves get access to the information. There are now laws and policies that have organizations assume responsibility in protecting the information and guarding against the misuse or unauthorized disclosure of the personal information. An example of this would be the well-known HIPAA, which protects health information collected by private entities. In case a data or security breach happens, it is also the responsibility of the organization

to inform consumers if the particular breach may pose a risk for them (*Combating identity theft: a strategic plan*, 2007, pp.27-32).

Decreasing Unnecessary Use of Social Security Numbers

Social Security Numbers are valuable to identity thieves. SSNs were originally created back in 1936 to track a worker's earnings and to obtain benefits. Throughout the years, the use of SSNs have increased rapidly, and are relied on extensively by the federal, state, and local governments. Currently, SSNs are a key piece of information used to authenticate the identity of consumers, where the numbers are matched with records and databases. As SSNs are widely used, the information is also readily available for identity thieves. Identity thieves are able to use a stolen SSN to open accounts, apply for credit cards and loans, or obtain other benefits, goods, or privileges.

It cannot be denied that SSNs are necessary and beneficial in many cases, but there are also some uses that are out of convenience or habit. These types of uses are unnecessary and are an added risk that can lead to becoming a victim of identity theft. Changes regarding reducing the unnecessary use of SSN have already started in the mid-2000s. The International Association of Chiefs of Police (IACP), with the help of the Social Security Administration Office of the Inspector General (SSA OIG), ended the practice of displaying SSNs in written materials, such as in a missing person's poster, back in 2005. Later, the Department of Treasury's Financial Management Service also no longer used personal identification numbers on checks issued for benefit payments, tax refund payments, and payments to businesses for goods and services provided to the federal government (*Combating identity theft: a strategic plan*, 2007, pp. 23-26). These all limit unnecessary use of SSNs, but more can be done such as reviewing the use of SSNs and offering substitutes for identification numbers that may come across as less valuable to identity thieves.

Educating Consumers on Protecting Personal Information

Consumers being aware of identity theft and taking reasonable precautions to protect their information can help combat and reduce the incidence of identity theft. A majority of the consumers do not take steps in protecting their personal information, such as the lack of a firewall on the computer, or leaving important mail with sensitive information in the mailbox. This gives identity thieves the opportunity to obtain their

personal information. Several agencies, such as the Federal Trade Commission, have tried to raise awareness of the problem through campaigns. These campaigns encourage habits that decrease identity theft, help with monitoring for identity theft, and to reduce the damage caused if the consumer falls victim to it. Apart from campaigns, educational materials regarding the protection of personal information are also available in government offices, police stations, and online (*Combating identity theft: a strategic plan*, 2007, pp. 39-41). Some recommendations for educating consumers about this issue is to increase the number of awareness campaigns, increase outreach, and to provide more identity theft educational resources online.

Implementing Authentication Methods

Consumer data can still happen even with precautions taken. As this important information falls into the identity thieves' hands, another part of the strategy is to make it harder for the identity thief to use the data. This can be done with additional methods of authentication. For example, if an identity thief wants to open a new bank account in the victim's name, apart from the stolen information, the bank can ask for photo identification, SSN, or other kinds of proof to ensure that the person is who he or she claims to be. This method is feasible, but currently apart from banks, not many other organizations adopt the method and are not required to use this method.

The method above may be able to reduce chances of an identity thief succeeding, but there are also times where documents can be falsified. This is where multifactor authentication can come into use. After verifying an individual's identity, there can be an added layer of security such as providing some sort of credential. The credential can be something that the individual is (fingerprints, iris, and face), something the individual has (smart cards or tokens), and/or something that the individual knows (passwords and security questions). A combination of two or more methods mentioned above can ensure some kind of protection against identity theft, but there are still many individuals who do not use multifactor authentication on important data and accounts. It may be recommended to increase awareness on this method, and also encourage the use of it.

Victim Assistance and Recovery

Victim recovery is a crucial step in helping victims of identity theft to repair their lives. Identity theft can still happen unexpectedly even with all the security measures in place, and falling victim to identity theft can oftentimes ruin a person's life. Letting consumers know and be aware of the existence of this type of assistance is important in starting the recovery process.

A few examples of assistance would be from the FACT Act, Privacy Rights Clearinghouse (PRC) and Identity Theft Resource Center (ITRC), Identity Theft Assistance Center (ITAC), and from the FTC. The Fact Act allows victims to place alerts on their credit files, request copies of documents used by the thief, and request that the credit reporting agencies block fraudulent tradelines on credit reports. For the FTC, they advise victims on what to do when they fall victim to identity theft. The FTC provides step-by-step information on identity theft recovery for victims on their website, www.ftc.gov/idtheft. Assistance from non-profit groups such as the PRC and ITRC would include counseling and other assistance for those going through the recovery process. Lastly, the ITAC helps victims with account disputes and reports. Other businesses, organizations, and agencies have also set up hotlines, informational materials, and other forms of services for the victims (*Combating identity theft: a strategic plan*, 2007, pp. 45-52). All of these assistance options are available, but not many people know of its existence. Identity theft can leave a huge damage to its victims and take time to recover. Many victims end up spending a lot of time and resources in an attempt to recover from the harms caused by identity theft, and receiving some type of assistance is always helpful. That is why there should be more effort in increasing the awareness of these services.

Working With Law Enforcements Internationally

With ecommerce getting increasingly popular, there have been more complaints from consumers where either their information was stolen by an identity thief from another country, or transactions were made by someone located overseas. As these cases rise, it is necessary to develop and promote a universal identity theft report form, and have a collective multinational information and intelligence sharing system designed to monitor and prevent identity theft (*Combating identity theft: a strategic plan*,

2007, pp. 57-59). Cooperation with foreign law enforcement is necessary in facilitating investigations and prosecutions of identity thieves outside the United States. Also, this encourages other nations to change their practices and help with combating cybercrime.

Laws, Regulations, and Guidelines Regarding Identity Theft

Federal Laws and Regulations

There are various ways our data as consumers is being protected. Some federal laws and regulations that are in effect are the Title V of GLB Act, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Section 5 of the FTC Act, the FCRA, and Drivers Privacy Protection Act (DPPA) of 1994. Title V of the GLB Act is mainly for financial institutions to protect consumer's personal information they collect. HIPAA is a well-known one that sets the standards for protecting sensitive patient information. Section 326 of the USA PATRIOT Act is also for financial institutions, where they are required to verify the identity of the person opening the account. Section 5 of the FTC Act mainly prohibits unfair or deceptive practices. The FCRA restricts access to consumer reports and regulates the way it is safely disposed of. Lastly, the DPPA of 1994, similar to HIPAA, is mainly to protect driver's personal information and prohibits disclosure of the information without permission (*Combating identity theft: a strategic plan*, 2007, p. 31).

International or Multinational Consumer Protection

As mentioned previously, a lot of identity theft originates from other countries with the rise of ecommerce. There have already been some efforts such as groups to increase awareness, privacy, and multinational consumer protection. Some of these groups include Organization for Economic Co-operation and Development (OECD), International Consumer Protection and Enforcement Network (ICPEN), Unsolicited Communications Enforcement Network (UCENET), International Mass Marketing Enforcement Network, and Asia-Pacific Economic Cooperation (APEC) Forum. The FTC also contributes by providing a platform, econsumer.gov, to report cross-border complaints. Additionally, the OECD has provided guidelines for ecommerce and

consumer fraud that includes information such as privacy and security risks, and payment protection (*International Consumer Protection and Cooperation*, 2022).

Reporting Identity Theft or Fraud

In case of becoming a victim to identity theft, the recommended actions to take are to report the identity theft to FTC via ftc.gov/idtheft and the local police department, place a fraud alert, freeze credit and bank accounts, and to contact the business or entity where the fraud occurred, if known. It is also recommended to contact creditors where fraudulent accounts were opened to start a dispute (*Combating identity theft: a strategic plan*, 2007, p. 46). For consumers with cross-border complaints, apart from doing the above, it is recommended to also report the complaint to econsumer.gov from the FTC (*International Consumer Protection and Cooperation*, 2022). For businesses that have lost important consumer information such as SSNs, they will have to contact major credit bureaus for advice on what to do, and inform the consumers. They should also contact law enforcement and consult on the next steps to take (Fair & Levine, 2022).

Conclusion

To conclude, identity theft is a multifaceted risk that can happen to anyone especially those unbeknownst to the nuanced theory of detection, mitigation, and protection. While there isn't one specific solution to the issue of identity theft, there are ways to prevent it, laws in place to protect those affected, and ways to detect the issue early on, before it becomes more of a problem. Identity theft is a growing issue and people must remain cautious and diligent, in order to reduce the number of victims of identity theft. It is important to understand what can cause identity theft and how to prevent it from happening. The key is to keep private information secure and private, and to dispose of it correctly, and to store it in an area that is not easily accessible to anybody. Take preventative measures to protect personal private information and take the necessary steps if one believes to have fallen victim to it. As more research and technological developments are made in the next few years, we will become more informed over how to fight the issue at the root of it, but for now we must take personal measures to make sure that our information is secured and protected, to prevent being a victim of identity theft.

References

Combating identity theft: a strategic plan. President's Identity Theft Task Force. (2007). Retrieved August 9, 2022, from https://permanent.fdlp.gov/lps82893/strategicplan.pdf.

Data Breach Response: A Guide for Business. (2019, April 29). Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business

Fair, L., & Levine, S. (2022, July 6). *Business guidance*. Federal Trade Commission. Retrieved August 9, 2022, from https://www.ftc.gov/business-guidance

Falsetta, D. (2020). Discussion of Trust and Compliance Effects of Taxpayer Identity Theft: A Moderated Mediation Analysis. Journal of the American Taxation Association, 42(1), 79–81. https://doi-org.echo.louisville.edu/10.2308/atax-52517.

Financial Identity Thefts Still Exist. (2009). *Security*, *46*(9), 16–16. Business Source Premier.

Identity theft: What is it and how to avoid it. Norton. (n.d.). Retrieved August 9, 2022, from https://us.norton.com/internetsecurity-id-theft-what-is-identity-theft.html#

IdentityTheft.gov—Warning Signs of Identity Theft. (n.d.). Retrieved August 9, 2022, from https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft

International Consumer Protection and Cooperation. Federal Trade Commission. (2022, March 4). Retrieved August 9, 2022, from https://www.ftc.gov/policy/international/international-consumer-protection-cooperation.

Levin, A. (2015). The Medical Identity Theft Apocalypse? Fear the Walking Files. *Forbes.Com*, 83–83. Business Source Premier.

Lutz, H. (2017). Growing threat to lenders: Synthetic identities. *Automotive News*, *92*(6794), 0024–0024. Business Source Premier.

Medical Identity Theft: Stop Insurance Fraud—Debt.com. (n.d.). Retrieved August 9, 2022, from https://www.debt.com/identity-theft/medical/

New data shows FTC received 2.8 million fraud reports from consumers in 2021. Federal Trade Commission. (2022, February 22). Retrieved August 9, 2022, from https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0.

Schreiber, S. P. (2016). TIGTA Finds IRS Failed to Act on Employment-Related Identity Theft. *Tax Adviser*, *47*(11), 48–48. Business Source Premier.

Types of Identity Theft | *Equifax*®. (n.d.). Equifax. Retrieved August 9, 2022, from https://www.equifax.com/personal/education/identity-theft/types-of-identity-theft

Woolley, S. (2017). How to protect your child from identity theft. *Bloomberg.Com*, N.PAG-N.PAG. Business Source Premier.