**The Thesis Committee for Jennifer Tatiana Brenner**
**Certifies that this is the approved version of the following thesis:**

# One Step Ahead, Not Two Steps Behind:
# The Fight to Protect Our Identities

**APPROVED BY**
**SUPERVISING COMMITTEE:**

**Supervisor:**

K. Suzanne Barber

Michael McCallum

# One Step Ahead, Not Two Steps Behind
# The Fight to Protect Our Identities

**by**

**Jennifer Tatiana Brenner, BBA**

**Thesis**

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

**Master of Science in Engineering**

**The University of Texas at Austin**
**May 2014**

# Dedication

I dedicate this thesis to my son, Adrian. He was the driving force behind my decision to return to school for this degree. Words really cannot express the love I have for my son and how he has fueled my desire to be the best possible version of myself.

# Acknowledgements

Above all else, I would like to thank God for the strength he has given me.

To my family and friends, thank you for playing an integral part in all I have accomplished by always pushing me to work harder and believe in myself.  I wanted to say a special thanks to Yongpeng for being an amazing friend throughout my time at The University of Texas at Austin.

I wanted to thank Dr. Barber for her help, inspiration and guidance over the past couple of years.  She has made me realize a passion for identity and security that I never knew I had.  To Mr. McCallum, thank you for your help and guidance throughout the writing of this thesis.  Both your experience and assistance were invaluable.

# Abstract

## One Step Ahead, Not Two Steps Behind
## The Fight to Protect Our Identities

Jennifer Tatiana Brenner, MSE

The University of Texas at Austin, 2014

Supervisor: K. Suzanne Barber

This thesis reviews different types of identity theft and conducts and in-depth review of the threats to our personally identifiable information (PII). There has been an alarming increase in the availability of industry applications that aggregate our PII with the promise of convenience. This paper deeply explores three data aggregators: Google Mobile Wallet, COIN and PayPal Beacon, to understand what they are, potential security implications and how widespread data aggregation may alter the identity landscape as a whole. Discussion of common technologies leveraged by these data aggregators help illustrate the vulnerability of the data consumers are willingly sharing. In an attempt to better understand the crimes that steal and fraudulently use PII, this thesis introduces the ITAP, the Identity Theft Assessment and Prediction tool to illustrate why it is important to study theft and fraud as a business process. The paper presents a small, independent study conducted to emphasize the validly of both the business process ideology and usefulness of the results. Closing thoughts are presented to speculate what the future of identity could look like and how consumers may need to use the information gathered from tools such as the ITAP to shape best practices. The goal is to be two steps ahead instead of one step behind.

# Table of Contents

# List of Figures

# 1. The Big Picture of Identity Theft

## 1.1 Identity Theft Defined

The term *identity theft* was first coined back in 1964 [1] long before the existence of Facebook, Twitter, or even the Internet itself. According to the Harvard Journal of Law and Technology, "identity theft is a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity, usually as a method to gain access to resources or obtain credit and other benefits in that person's name."[2][3] Although the term has retained meaning, it is carried out much differently now with the advancements in technology. There are in fact, three main types of identity theft, financial, child and medical. Since 2005, there have been 4,253 recorded breaches and 591,606,915 records exposed. [4] This is an astoundingly high number; and at the current pace, the question will soon be, "when will my identity be stolen" not the statement "if my identity gets stolen". A new report compiled by the Justice Department's Bureau of Justice Statistics (BJS) found that an estimated 16.6 million people (or roughly 7 percent of all Americans age 16 or older) experienced some form of identity theft in 2012. [5] The three main types are explored in great detail in the coming sections.

## 1.2 The Current Problem Landscape

Financially motivated identity theft is what comes to mind when most hear the term "identity theft." This type of fraud involves stealing someone's personally identifiable information for purely financial gain. Malefactors often piece together profiles on potential victims by manipulating vulnerabilities and daisy chained information available in the public sphere. Leveraging these victim profiles, mortgages and lines of credit are being opened and cars are being purchased. In some cases, a fraudster may go under the radar for years before the victim discovers their credit history is in shambles. According to The United States Department of Justice, in one notorious of "identity theft, the criminal, a convicted felon, not only incurred more than $100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and handguns in the victim's name, but called his victim to taunt him -- saying that he could continue to pose as the victim for as long as he wanted because identity theft was not a federal crime at that time -- before filing for bankruptcy, also in the victim's name. While the victim and his wife spent more than four years and more than $15,000 of their own money to restore their credit and reputation, the criminal served a brief sentence for making a false statement to procure a firearm, but made no restitution to his victim for any of the harm he had caused."[6] The potential for identity related frauds has drastically increased with widespread Internet access. It is estimated that roughly 21% of the entire world has Internet access. [53] "Remote internet access can enable anyone – even far removed from the United States – to obtain credit and other pertinent information and use that information to steal funds."[7] Identity Theft has become widespread, however, not only because of the nature of the information consumers are providing, but also because the companies that are soliciting information do not properly protect it. "A recent Verizon Business Solutions survey points out that less than 11% of non-financial firms have installed protections that meet minimum industry standards that industry cyber security experts assert are not now sufficient given current hacker technology."[7] The more rampant identity theft becomes, the more information companies are requiring of consumers and a cycle ensues. Consumers give more information to protect themselves only to be that much more vulnerable to an attack. The paragraphs to follow explore two specific types of identity theft, where the gains sought can go beyond just financial.

Child Identity Theft “occurs when a minor’s Social Security number is used by another person for the imposter’s personal gain.”[8] Although the perpetrator is typically a family member, some fraudsters specifically target children because their social security numbers do not have any information associated with them. In fact, “one in 10 children have a Social Security number that was used by someone else.”[9] Child Identity Theft is rapidly increasing in frequency and the danger lays in the inability or tendency to detect it. According to LifeLock “your child's clean and unmonitored credit file is a gold mine for identity thieves. Critical misuse and damage could go completely undetected for years.”[10] Like many security problems, the greatest obstacle is the overall lack of public awareness. Most parents do not believe their children are at risk and therefore do not keep a watchful eye on their child’s identity. The fact is, however, that “children are particularly vulnerable because their information is held in places with little or no cyber security, like schools and doctors’ offices,” says Lisa Schifferle, an attorney for the Federal Trade Commission. [9] Schools and doctors’ offices are not as careful as financial institutions are with potentially sensitive data. Financial institutions have the most restrictions on data management and handling. A child’s medical chart containing all of his/her vital identity data passes through many hands during just one visit. In response to the overall lack of information available to parents in this area, the University of Texas at Austin has created an online portal suggesting an “identity checkup” for children with an aim to empower parents to become more vigilant and proactive. Lastly, a very relevant and evolving space, the world of medical identity fraud is investigated.

Medical Identity Theft occurs when someone steals someone's personal information to obtain medical care, buy drugs, or submit fake billings to Medicare in the victim's name. [11] Whereas financial ruin and a damaged credit rating are detrimental, they can be fixed over time with help and persistence. Medical fraud, however, can be "life-threatening to you if wrong information ends up in your personal medical records." [11] According to the SANS-Norse 2014 Healthcare Report, "millions of healthcare organizations have likely had their networks exploited by cyber-criminals or infected with malicious software that can be used to steal patients' personal health information." [12] The report goes into gory detail about the widespread availability of the information in a patient medical record, including, but not limited to, social security numbers, billing addresses and personal details related to medical history. [12] The threat most likely feels unreal to anyone who has not experienced it firsthand or knows someone intimately who has been personally affected. WebMD details a chilling account of medical identity fraud involving a pregnant 28-year-old woman who used a stolen driver's license to gain access to a clinic for care. Once checked in, the fraudster, Dorothy Bell Moran, gave birth to a daughter whom she abandoned at the hospital after birth. "Several days later, when the hospital ran tests, the baby girl came up positive for methamphetamine."[13] At this point, the story really unravels. Anndorie Sachs, the woman whose license had been presented at the time of service, had four children of her own and was now being accused of abandoning a baby at the hospital and racking up a $10,000 hospital bill. DCFS agents went so far as to pull Anndorie's daughter from her first grade class to verify that her mother had in fact not given birth to a child a few days before. [13] Eventually, "the accusations were dropped and Sachs was cleared of paying Moran's hospital bills, but the ordeal wasn't over. Sachs's medical records had been altered to include the blood type and general health record of a complete stranger. The two hospitals assured Sachs that they'd fixed the problem, but she cannot be 100 percent sure because — in a catch-22 of utter insanity — they wouldn't let her see her own records, lest Moran's privacy rights be violated." [13] Despite the fact that Moran used a stolen driver's license to access healthcare, the victim, Sach, cannot verify that her own medical records are correct, because Moran still has a right to privacy. Although in this case, things were resolved quickly, in many cases the victim may be unaware that this has happened until irreparable damage has been done. In a worst-case situation, "insurance [is] maxed out to its lifetime limit, years [are] spent untangling paper trails, and medical records [are] permanently altered. Imagine what could happen if someone else's medical history was injected into your records: You could arrive at an ER and be given the wrong type of blood or be refused medication because your file says you are allergic". [14] At this point in time, medical identity theft is not as common as financial identity theft, but the repercussions can be life threatening.

With the coming, widespread implementation of electronic medical records, the concern revolving around an incorrect medical record greatly increases. In the aforementioned case, Sach's medical record was altered by Moran, but the situation was fairly isolated as the data was only altered at the two local hospitals where Moran specifically sought treatment. With the new, electronic-based system, Moran's information would have instantly been injected into Sach's overarching electronic medical record. This record would be accessible by every hospital. A victim could be rushed into an emergency room and, unaware their identity has been compromised, receive treatment based on another individual's health record. The possible aftermath is unforgiving. In 2015, the United States plans to have this idea of an electronic medical record fully implemented. Institutions that do not comply will suffer financial penalties in the form of reduced payments from Medicare and Medicaid. According to Engaget, Electronic Medical Records are supposed to "save up to $74 billion per year (or 5% of health care spending) in preventable procedures and efficiencies gained — not to mention saving the tens of thousands of lives lost due to preventable record keeping and charting errors."[15] Although this is a seemingly beneficial process with instant access to aggregated medical data, questions of privacy are already being raised. According to a recent survey by the Federal Trade Commission (FTC), "3 percent of U.S. identity-crime victims had someone use their personal information — a Social Security number, an insurance policy ID, even a mere driver's license — to obtain medical services or to profit from filing false claims in their name. That means nearly 250,000 Americans may be victims each year". [14] Despite the scope of this thesis focusing primarily on the United States, the desire to take medical records online is international in scope. "The UK government is currently building a database called care.data that will contain all of England's medical records. It's being promoted as providing valuable information for healthcare management and medical researchers that will lead to improved treatment." [16] The main cause for concern is that once medical data is electronic it is more accessible to both fraudsters and those who wish to capitalize on our illnesses and medical history. The article goes on to explain that "drug and insurance companies will from later this year be able to buy information on patients — including mental health conditions and diseases such as cancer, as well as smoking and drinking habits — once a single English database of medical data has been created."[16] The article furthers that police and government bodies will also have access to the data in the UK. The main question then becomes, both here and internationally, who will be building the database that houses and aggregates all of this highly sensitive data and what will keep them from using it commercially? Will consumers start receiving targeted ads for medications treating diseases thought to be proprietary? Will there be any privacy in healthcare?

Regardless of the specific type, victims of identity theft expense a tremendous amount of resources and time seeking resolution. Now that the three main verticals of identity theft have been explored, the coming section presents both the motivation for the thesis as well as an outline of the sections to come.

### 1.3 Paper Motivation and Outline

Identity theft has plagued society due to the lack of information surrounding present vulnerabilities. Authorities are typically two or three steps behind a fraudster and become aware of the how fraud took place only in hindsight. Society has long failed to capitalize on the knowledge of how things took place. Despite regularly reading articles on identity theft, until fraudulent circumstances are mapped out as a progression of purposefully executed steps, it is difficult to get a clear vision of exactly how things progressed. The hope is to better understand present vulnerabilities as well as a fraudster's behaviors in order to make connections and visualize patterns based on past identity theft attacks. It is time to learn from past fraud in order to finally be one step ahead. The next section examines the big research questions explored in this paper. Section three dives into the identity landscape as a whole, including, a look at the rise of both social media and data aggregators. Section four introduces the ITAP, The Identity Theft Assessment and Prediction Tool. Section five summarizes the results from a sampling of data in order to illustrate the importance of understanding the identity theft process. Section six explores the future of identity by looking at what consumers can do proactively and what companies are doing. Closing thoughts are presented in section seven.

## 2. Big Research Questions

Throughout the thesis, several questions are explored in order to better understand the identity landscape as a whole, its evolution and the importance of theft and fraud as a business process.

The following are the big research questions:

1. What are the most common resources fraudsters are using to commit fraud?

   The first question seeks to understand what resources, or tools, fraudsters are using most often when committing fraud. Anything that assists in the accomplishment of a fraud can be considered a resource. Typically, without this resource, the fraud would not have been able to take place.

2. What PII seems to be most exploited to commit fraud?

   Question two aims to understand what pieces of personally identifiable data seem most vulnerable to attack. What are some of the creative methods that fraudsters are using to get a hold of this information?

3. Why is it important to study Identity theft as a business process?

   This question looks at the importance of why fraud should be treated like a business process. What knowledge can be gained from studying fraud scenarios in this manner?

4. How can data aggregators change the identity landscape?

   Question four explores how data aggregators, tools that localize sensitive data, have changed the identity landscape. What types of problems do data aggregators cause in terms of protecting personally identifiable data?

5. What can consumers do to be more vigilant?

   Lastly, question five explores what consumers can do to better protect the information that is vital to their well-being.

Each of the questions above will be addressed in the thesis as a means of gaining greater understanding about identity and identity theft as a big picture. This domain is evolving at an incalculable speed as technologies become more advanced and hackers develop more sophisticated methods for immobilizing security barriers and stealing PII. That being said, anything that is surmised may not be fully applicable in six months. The essential notion, however, is to understand trends and patterns as well as how consumer PII is being used as a means of being more informed about potential shifts in the paradigm. The coming section takes a big picture look at some prevalent threats to consumer PII.

# 3. The Threats to Our Personally Identifiable Data

A variety of factors have led to an overall increase in the availability of sensitive consumer data. Specifically, this section discusses how social media has assisted in identity theft by publicizing identities, the prevalence of data aggregation and related implications, as well as how sensitive data is being handled by data aggregators. The leveraged technologies, near field communication and Wi-Fi, are also discussed because any potential security issues can threaten an identity both within the realm of data aggregation and independently, when these technologies are leveraged elsewhere.

## 3.1 The Rise of Social Media

Social media "refers to the interaction among people in which they create, share, and/or exchange information and ideas in virtual communities and networks."[17] Facebook and Twitter are notably the most popular spheres where information is voluntarily shared in the form of status updates and profiles. "Status updates posted on Twitter, Facebook and many other social media sites can be used by criminals. If you post that you're out of town on vacation, you've opened yourself up for burglary. If you mention that you're away on business for a weekend, you may leave your family open to assault or robbery. When it comes to stalking or stealing an identity, use of photo- and video-sharing sites like Flickr and YouTube provide deeper insights into you, your family and friends, your house, favorite hobbies and interests." [18] It is absolutely shocking the amount of information the average person divulges through social media channels. A 2010 survey by ID Analytics found that almost 20 million Americans have revealed the names of their pets on social networks. [19] Moreover, ID Analytics and Harris Interactive also found that over 70 million adults publicly share their birthplace on their social network profiles. [19] A small nugget of information like a pet's name could be a fraudster's best friend. Social Media sites make it easy for just about anyone to piece together a potential victim's profile. "Despite all the awareness that people have about identity fraud and privacy on social networks, there is a disconnect between what people are disclosing in online space and social environments and what they may be using in other places of their lives," says Thomas Oscherwitz, chief privacy officer for ID Analytics, a San Diego-based consumer risk management firm [20]. Later, the thesis explicitly discusses how these morsels of information publically shared on social media sites are used to destroy security layers and access PII.

### 3.2 Rise of Data Aggregators

There has been an alarming increase in the availability of industry applications that aggregate consumer PII with the promise of a seamless and quick payment transaction. The premise is that with all credit and debit cards, preferences and shopping habits tightly knit in one place, shopping experiences will be fast and customized to meet a consumer's personal needs. This paper will now deeply explore three data aggregators: Google Mobile Wallet, COIN and PayPal Beacon, in order to understand what they are, any potential security implications and how they may alter the identity landscape as a whole.

First, Google Wallet, the most notorious of the mobile wallet applications currently available is analyzed. The application boasts the ability to completely replace the need of a conventional wallet. "Mobile wallets help retailers provide consumers with rich and personalized experiences that build loyalty," said Jack Philbin, co-founder and CEO of Vibes, a mobile marketing technology leader. [21] Google describes the application as a “free digital wallet that securely stores your credit cards, debit cards, offers and more.” [22] The convenience factor is high and research suggests that, “85 percent of consumers - specifically smartphone users - see the benefits of storing mobile-wallet content”. [21] The important question, however, is how many people understand the true implications of what it means to store content on Google Wallet or any related mobile application?

A closer look reveals an application that is both effortless to use and convenient, so the widespread adoption is anything but surprising. In order to use Google Wallet, the user creates an account by linking an established Google account or creating a new one. Furthermore, the addition of credit and/or debit cards allows for purchases to be made both online and in-store. The user can also load loyalty cards and discount offers for easy retrieval.

What kind of data is Google wallet collecting? Google is gathering many of the critical pieces of personally identifiable information consumers use to establish an identity. The following data could potentially be gathered and stored depending on an individual’s payment preferences: first and last name, full billing address, birthdate, credit card number, credit card expiration date, bank account number and routing number, CVC (security code), shopping habits, purchase history, phone number, and backup email. Essentially, all the critical and sensitive information consumers aim to keep secure.

During setup, the user secures the account information by creating a 4-digit security PIN. Once the application is active, “each time you open your Google Wallet app, you will be prompted to enter your 4-digit security PIN.” [22] While the average person may feel their Google Wallet is amply safe with the addition of a 4 digit PIN, Google provides additional safety features meant to ease any lingering worries. “Not only can you deactivate the application remotely should you misplace your phone, Google’s Purchase Protection also covers you against unauthorized Google Wallet transactions reported within 180 days of purchase.” [22]

Google is a reputable company who has set up several precautionary security measures in an attempt to make the mobile wallet as secure as possible but, nothing is 100% secure. It is important to consider here that once content enters the virtual realm, it is stored in a database and not out of reach. Many companies, in fact, store consumer data on multiple servers in multiple locations. Typically, this is not highly publicized but consumers should be aware that their data could be stored on servers outside the country where US laws on identity theft and fraud have no jurisdiction. Most companies claim that their servers are secure, but a proactive consumer should research where servers are held before providing sensitive information. “Google Wallet stores your credit and debit cards on secure servers and encrypts your payment information with industry-standard SSL (secure socket layer) technology. Your full credit and debit card information is never shown in the app and won't be shared with the merchant.” [22] In essence, when a user walks into a store and pays with Google Wallet, Google pays the merchant for the goods and/or services and then squares away with the user behind the scenes with the payment methods stored in the user’s account. The secure element is how Google physically keeps the data secure. According to IGI Global, the secure element is “the NFC architecture component responsible for storing applications or data with high security requisites.” [23] NFC, explored deeply later in the thesis, is a technology that allows enabled devices within close proximity to communicate. Google explains its utilization of the element by stating that it “is separate from the phone’s main operating system and hardware, which enables encrypted protocols to enforce access control. There are multiple levels of protection for data stored on the Secure Element and it is protected at the hardware level from snooping or tampering.” [22]

Despite these claims, research suggests that the application is not as secure as their marketing team would have consumers believe. “After conducting some extensive research, the security experts at ViaForensics concluded that Google Wallet is not as secure as it should be. In particular, their analysis shows that the mobile payment platform stores too much personal data on the smartphone.”[24] The danger in having so much sensitive data on a mobile device is that there are many sophisticated ways to steal it. According to ViaForensics, “Google does not have the best track record for security in their App marketplace”. Users can download applications containing malware, making their entire phone, including data stored by other applications such as Google Wallet, immediately vulnerable. During the application’s lifetime, several people have found weaknesses and vulnerabilities that have allowed access to the data that is supposed to be secure. Although Google promptly fixed the flaws as they were exposed, the relevance is that hackers are becoming increasingly sophisticated in their abilities to break down any security barriers. If consumer information is made available, it will be accessible as vulnerabilities are exploited. No system is 100% secure. Google will fix flaws once exposed, but at that point, information may already rest in a hacker's database. Although mobile wallet is convenient, there may be a cost associated with such convenience in the form of PII.

Unlike Google Mobile Wallet, the two payments devices discussed below have yet to be launched for widespread consumer use. That being said, each one is still explored to understand what it is and how it groups together PII. The aim is to gain a holistic view of how prevalent the aggregation of data has become before implications are discussed.

The COIN digital credit card is the new "all-in-one" card currently in its beta stages to be released in the summer of 2014. "Coin packages up to eight cards (debit, reward, membership, etc.) into one "coin" swipeable card."[25] Cards can be added to the device via a mobile application, which allows the user to "add, manage and sync cards. The process of adding card information to the mobile app is very simple and is done by taking a picture or two and swiping your Coin through a small device [they] provide you with". Despite looking and feeling like a regular credit card, COIN actually provides the user with the ability to make purchases with several cards via a selection display. "Coin is very easy to set up and use. After uploading credit cards onto the device, the user only needs a Coin and smartphone to make a purchase."[25]

Much like Google Wallet and other data aggregators, COIN pulls together a user's personal and financial data. In terms of security, COIN explains that "maintaining the integrity of your Coin's data is critical to your peace of mind. That's why our servers, mobile apps and the Coin itself use 128-bit or 256-bit encryption for all storage and communication (http and Bluetooth). Additionally, Coin can alert you in the event that you leave it somewhere."[26] Further safety features include the "auto-deactivate" feature, which allows the COIN to be rendered useless in the event it is lost or stolen and the fact that COIN servers only store non-sensitive card details when a purchase is made. The website then goes on to explain that "a Coin is no less susceptible than your current cards to other forms of skimming that capture data encoded in the magnetic stripe as the card is swiped."[26]

Although this may initially seem harmless, the fact that Coin has access to not one credit card, but all the ones loaded, is unsettling. Coin's susceptibility being similar to that of a regular credit card does not help its' case as there have been massive cases of credit and debit card skimming even recently with the Target Data Breach in early 2014. A fraudster who is able to skim and capture the data encoded in the magnetic stripe has hit the jackpot, potentially stealing data pertaining to several cards at once.

The Coin has not yet been made available mainstream so there is little known about exactly how fraudsters will attempt to exploit it. The portal to manage the card is accessed via a mobile application, which presents several potential security issues as well. Most importantly, like the Google Wallet, loyalty cards and preferences are also combined with financial data on the COIN. Combining this data on any application is dangerous because of what it allows a fraudster to learn about a potential victim. The dangers of this are discussed in section 3.3.

Lastly, the third and final mobile payments player discussed is the PayPal Beacon. The Beacon is a hardware device that runs on its own Wi-Fi. It is plugged into a wall socket or a laptop at a merchant site and "serves as a 'beacon' to other connected devices."[27] Developed in January of 2013, the Beacon utilizes "Bluetooth Low Energy, which allows connected devices to communicate with each other while keeping the energy consumption by the devices at a very low level."[27] The device promises the ultimate shopping experience where a customer can "order and pay for lunch hands-free, open a tab, and get special offers – all without lifting a finger."[28] Additionally, much like the mobile wallet, the experience helps merchants "bring in new customers and give them a true VIP experience, again and again."[28] Any consumer who is interested in using the Beacon can download the PayPal app and opt into the service, which allows purchases to be made hands-free using voice authentication. After opting in, when walking into a store, the technology will "trigger a vibration or sound to confirm a successful check in (this happens in milliseconds), your photo will then appear on the screen of the merchant's Point-of-Sale system so you can be greeted by name." [27] In order to make this work, the application does not need to be open on your smartphone. The customer receives a receipt automatically in his/her email for purchases or services rendered. In terms of privacy, the company "warns that it is aware of the potential privacy issues so PayPal Beacon won't constantly track your location unlike other technologies."[28] The company then furthers that if the check-in is ignored, no information is transmitted to either PayPal or the merchant and there will be no ads served via the platform. The convenience is admittedly both alluring and amazing. The thought that a consumer's name could automatically be added to a waitlist for a table at a restaurant or that a pharmacy could populate prescriptions automatically, seems too good to be true. As the consumer shops around the store, the prescriptions are filled and by the time they make it to the pharmacy, everything is ready to go. In a world where people are busier than ever, any time saved can help improve a consumer's quality of life.

Like the other two above-stated data aggregators, convenience and seamlessness are the primary motivators for consumer adoption. Convenience, however, is often the result of a direct tradeoff with security. Often, the “easier” it is to conduct a payment transaction, the more likely it is to be unsafe. This is not always the case but with ease often comes a circumvention of necessary security precautions. The dangers of conducting financial transactions over Wi-Fi are well known and will be discussed in more detail later in the thesis. Additionally, “what if a third party accesses the network simply by being in the device’s general vicinity during a transaction? What about vendors making unauthorized transactions without the customer’s knowledge? Is a Beacon user’s financial information truly safe?”[29] These are all questions that are being asked by the community. PayPal, however, insists the device is safe to use. The company has explained that users can add different businesses into a database of stores they frequent often that are considered “safe”, giving only these stores access to their PayPal information. “Businesses that aren’t on this list will require approval from the user before a transaction can go through, a feature that will also prevent accidental purchases from being made.”[29]

Because the Beacon has yet to be fully launched, there is little known about the specific vulnerabilities that will become exposed as merchants and consumers embrace and use the service. Since the Beacon is ultimately linked to a user’s PayPal account, the data flowing during a transaction includes, at minimum, a photo of the user, the user’s PayPal email address as well as any information associated with the user’s shopping habits and preferences. On the back end, PayPal stores a plethora of financial and personal information as money is transferred from credit and debit cards as well as directly to and from bank accounts within the platform. It is yet to be seen exactly how much and what type of data will be exchanged during a Beacon transaction. The fact remains, however, that a tremendous amount of data pertaining to a consumer's identity is being housed together, once again, with other financial data.

The next section discusses the overall dangers associated with all data aggregators due to the nature of how the transfer of information is conducted and how victim profiles are typically compiled.

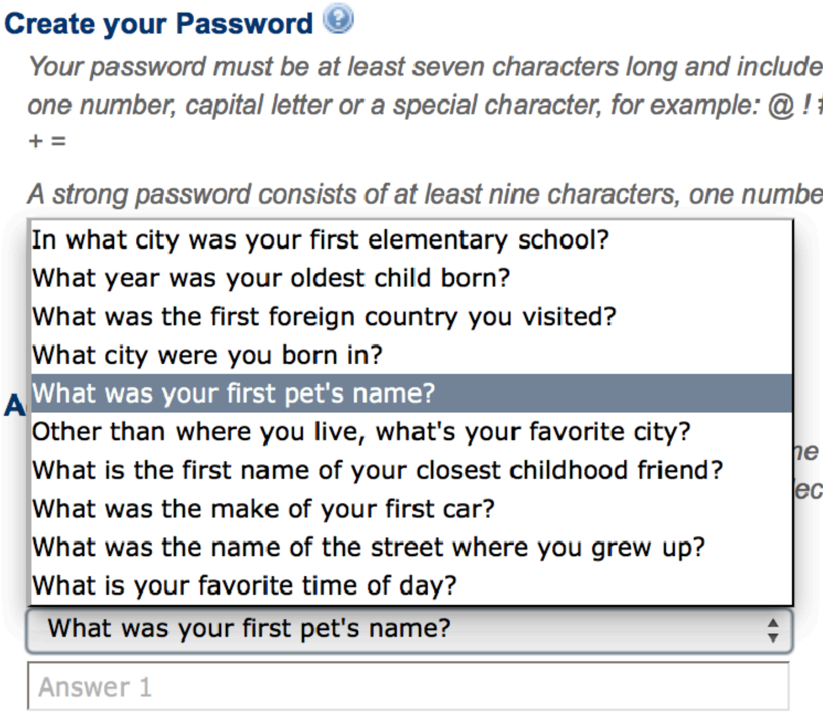
### 3.3 Why the Aggregation of Data Can Be Dangerous

It is important to examine what the repercussions are of aggregating the data that consumers use to both identify and protect themselves. This segues into the fourth research question, "How can data aggregators change the identity landscape?" This accumulation of personally identifiable information is increasing at an alarming pace and has shaped the identity landscape as whole. In the past, a fraudster was actually required to piece together the digital life of a victim via illegal skip tracing sites and paid searches. They had to scour online databases and hack into low security accounts in order to "get to know" the intended victim. Now, however, in conjunction with social media sites, data aggregation tools are giving fraudsters access to pools of data about potential victims. Essentially, consumer identities have been wrapped in a package with a bow and left on an aptly labeled shelf for any hacker to pick up and use as they see fit. Effectively, these applications have paired not only physical debit and credit card numbers but also, shopping habits, behaviors and special interests. But this is harmless data, right? Well, the short answer is no. Most of this data is used as a second layer of defense on a consumer's most important personal accounts, namely, in the form of security questions. A security question is used as an authenticator by banks, cable companies and wireless providers as an extra security layer. [30] Typically, during the account creation process, security questions are selected and answered in addition to providing a password. This enables a consumer to authenticate him or herself in the event the password is forgotten for the account.

The following are commonly utilized security questions:

- What is your favorite restaurant?
- What is your pet's name?
- What is your favorite book?
- What is the name of the road you grew up on?
- What is your favorite place to vacation?
- What is your favorite food?
- What is your mother's maiden name?
- What is the name of the road you grew up on?
- What high school did you attend?
- Father's middle name.

Figure 1[10] below is a screen shot from the account registration page of LifeLock, an identity theft protection service that monitors use of both personal accounts and the subscriber's social security number. [10] Even a site whose sole purpose is to protect identity uses security questions full of information any diligent hacker could uncover by trolling Facebook and/or twitter or by gaining access to your PII via an aggregator.



**Create your Password**

*Your password must be at least seven characters long and include at least one number, capital letter or a special character, for example: @ ! # $ % ^ + =*

*A strong password consists of at least nine characters, one number, one*

- In what city was your first elementary school?
- What year was your oldest child born?
- What was the first foreign country you visited?
- What city were you born in?
- What was your first pet's name?
- Other than where you live, what's your favorite city?
- What is the first name of your closest childhood friend?
- What was the make of your first car?
- What was the name of the street where you grew up?
- What is your favorite time of day?

What was your first pet's name?

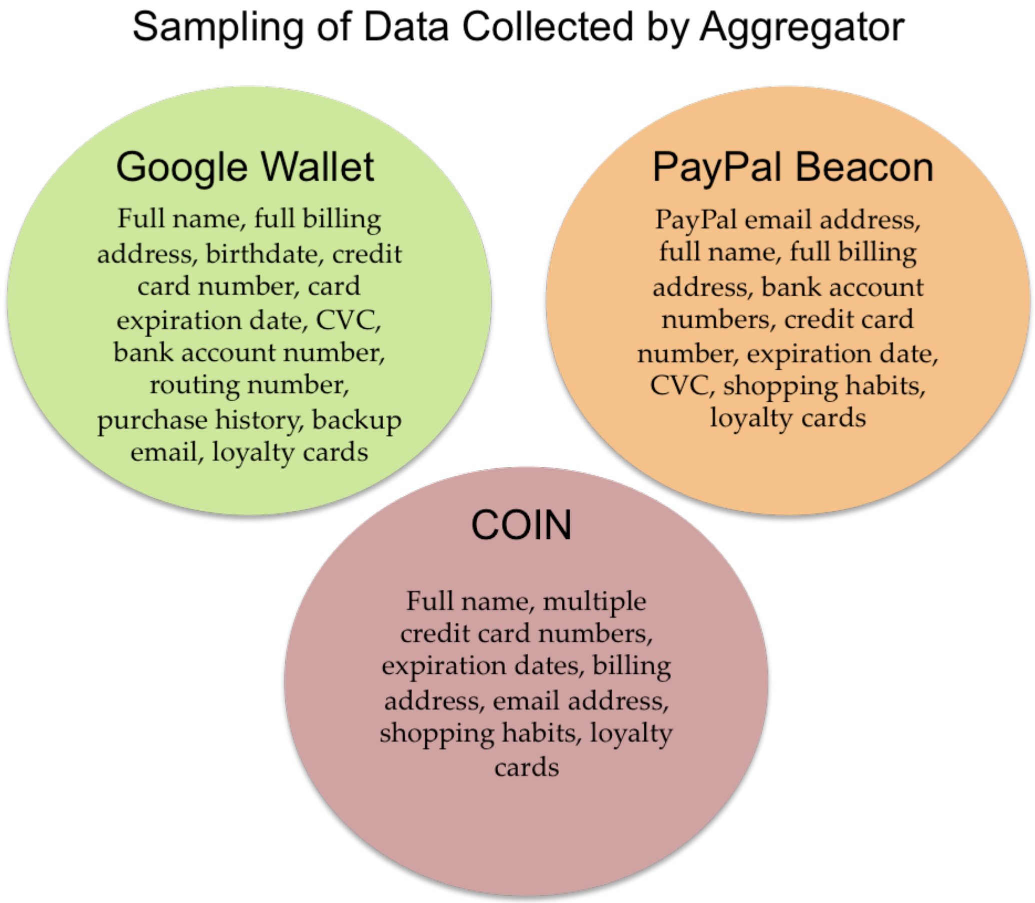
Answer 1

Figure 1: LifeLock Registration Screen Shot

Utilizing this as a gold standard as far as security questions go, given the website's purpose, it is shocking to reveal how easily this information can be sourced. Looking to the first security question on the image above, *In what city was your first elementary school*, it is seen that this information can often be found on Facebook. Facebook features a "hometown" section where users put in the city where they grew up. Many people attended elementary school in their hometown. Moreover, most of a consumer's former addresses can be found in public databases and some Facebook users even list the schools they've attended on their profiles. The next question, *what year was* *your oldest child born,* can also be deduced via Facebook lineage or Ancestry.com which allows users to establish a family tree. Family members, children included, could have their birthdates listed on their profiles, which would make this question pretty straightforward to answer. In theory, most, if not all of the questions could be discovered via the manipulation of public data, social media or aggregated data. There are some questions, however, that are definitely more favorable. Of all the questions LifeLock lists above, the most secure are the ones that are arbitrary or subjective in nature. For example, the questions, *What is your favorite time of day* or *What was the first foreign country you visited* are perhaps better candidates because they require information that may not be readily available. Anything that can change over time or is a "feeling" rather than a fact is preferable answer over a concrete one that can be verified.

It is important for consumers to be mindful of the security questions selected. This simple precaution may prevent hackers from gaining access to certain accounts. The true danger, however, lies in what can be discovered from analyzing the "subjective" data that surrounds consumer activities and the habitual decisions made on a regular basis. Questions inquiring about a favorite restaurant may easily be discovered using Google Wallet information, where all loyalty cards are stored in one place. Or, perhaps, the consumer checked into "Red Lobster" 10 times last month and paid using PayPal Beacon. This would be a great guess as to that consumer's favorite restaurant. Most people may not even realize how often they perform certain activities and how these activities are tied to their identity. The danger is not necessarily in one piece of data but in what individual pieces of data become when used to create a profile of a potential victim. This type of compiled profile is typically how frauders carry out large scale theft resulting in hundreds of thousands of dollars being stolen.

Data aggregation also permits cross-site manipulations to occur. This is where a fraudster compromises multiple accounts using known, linkable vulnerabilities across the targeted platforms. This became epically obvious in the article "How Apple and Amazon Security Flaws Led to My Epic Hacking". In the article, writer and victim Mat Honan explains in grave detail, how easily his digital life was destroyed via information manipulation. He begins the article by explaining that, "in many ways, this was all my fault. My accounts were daisy-chained together." [31] The author alludes here to the dangers of data aggregation. Although in this specific case the fraudster did not have access to a profile of the victim, the victim had much of his data tied together. Once the fraudster infiltrated one area, he was able to hop from one piece of information to the next by manipulating vulnerabilities in both the Amazon and Apple platforms. Although there are several measures he could have taken to protect himself overall, the illustrative point is that when Mat's attacker needed to gain access to his Apple Account, all that was needed were the last four digits of a credit card listed on the account. The fraudster knew that the same last four digits of a credit card are readily displayed in an Amazon account. The hacker gained access to Mat's Amazon account first, viewed the four digits and then used that to authenticate himself and reset the password on the Apple account. If an attacker has access to pools of consumer data, it becomes significantly easier for inherent platform vulnerabilities to be manipulated, enabling this type of access. [31] Consumers do not have control over these inherent software vulnerabilities nor are they always aware they exist. It is important to minimize this "daisy chaining" whenever possible to make it more difficult, and therefore potentially less rewarding for a hacker to steal data. Figure 2 below depicts all of the consumer data that is collected by each of the aforementioned data aggregators.



Sampling of Data Collected by Aggregator

Google Wallet

Full name, full billing address, birthdate, credit card number, card expiration date, CVC, bank account number, routing number, purchase history, backup email, loyalty cards

PayPal Beacon

PayPal email address, full name, full billing address, bank account numbers, credit card number, expiration date, CVC, shopping habits, loyalty cards

COIN

Full name, multiple credit card numbers, expiration dates, billing address, email address, shopping habits, loyalty cards

Figure 2: Data Aggregation Figure

The subsequent sections round out the study of the personal identity landscape by exploring the potential security flaws of near field communication and the dangers of transmitting personally identifiable data via Wi-Fi. All of the previously discussed data aggregators leverage at minimum one of these technologies when transmitting data between a customer and a merchant. The pitfalls of Wi-Fi are important to ruminate on, as users are susceptible anytime they access sensitive data over any network.

### 3.4 How Near Field Communication Worsens the Problem

A common thread among data aggregators is their dependence of Near Field Communication technology to transfer PII. Near Field Communication, or NFC, is "a set of standards for smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into proximity, usually no more than a few inches". [32] To ensure security, NFC utilizes encryption whenever it sends sensitive data from one device to another through a secure channel. Entities who use NFC claim it is secure, however, there have been many reports that indicate otherwise. In 2012, Security Researcher, Charlie Miller, publically proved that NFC was not safe. During the Black Hat Briefings conference, Miller presented nine months' worth of research explaining how he was able to exploit NFC to compromise two smartphones. "Miller's work, however, wasn't about stealing data such as payment information, but instead focused on gaining full control over another phone via NFC. His goal was to show how an attacker could, for example, force the compromised phone to launch a browser and navigate to a malicious website."[33] Miller illustrated that a cell phone can be completely taken over using NFC. At that point, the more data housed on a mobile device, the greater the potential ramifications.  Some data aggregators, namely Google Wallet, do just that.  Miller explains further "this is all about the attack surface the phone introduces.  NFC strictly reads 100 bytes-per-second. It's totally possible to write code that securely parses 100 bytes. It's well within our engineering abilities as a group. But I was surprised to know it opened up this huge other attack surface, like opening browsers or parsing documents or images."[33] Moreover, "Miller initially believed he would find enough security vulnerabilities to work with on the lower levels of the NFC code stack, but he struck gold with the higher-level protocol layers. It's there where initialization and activation take place; where command sets -- such as *read* and *write* -- are located; where files and data are found, and the area where peer-to-peer exchanges take place". [33] Miller's demonstration is referenced as a means of illustrating one of the many potential scenarios where having a quantifiable amount of sensitive data on a phone could be dangerous.  Like any other technology, NFC is also vulnerable, and data aggregators elevate the potential damage that can be done.

### 3.5 WHY WI-FI CAN BE UNSAFE FOR DATA TRANSFER

Moreover, Wi-Fi is the second component that allows for the data exchange. Consumers very often access personal information over Wi-F.  Coffee shops, restaurants, the gym, hotels; establishments need Wi-Fi in order to stay competitive and the public desire to be constantly connected fuels this fire.  Often, highly sensitive data is accessed over Wi-Fi with the assumption that the network is both reputable and safe.  Likewise, the usage of mobile applications for conducting financial transactions is becoming commonplace.  The convenience of accessing account balances, depositing checks and making transfers on mobile devices is undeniable. According to the Consumers and Mobile Financial Services 2013 report by the Federal Reserve, "48% of smartphone owners have used mobile banking in the past 12 months, up from 42% in December 2011."[34] Because technology, speed and convenience are deep-seated in society, the transfer of data via networks is only going to increase over time.

The question then becomes, is it even safe to bank mobility or on public Wi-Fi networks? Is it prudent to deposit checks by mobile device? Darren Kitchen, a hacking researcher, explains in the article *Is It Safe To Bank on Public Wi-Fi? How Not to Get Hacked*, that "accessing your sensitive financial data via computer can be dangerous. One well known computer virus that steals banking logons and passwords is thought to have infected over 3 million computers in the US alone, siphoning at least $70 million dollars from consumers". [35] In order to illustrate his point, Darren and author of the article, Becky Worley of Upgrade Your Life, decided to conduct an experiment to illustrate just how unsafe Wi-Fi can be. The article describes Becky logging into the Wi-Fi provided free at a local café and pointing her browser to her banking site. On her trusted banking site, she enters her username and password. "In real time, Darren intercepted the logon info."[35] Darren, like many hackers, brought his own router into the coffee shop and set it up to provide an open connection with a commonly used network name. Often, hackers will give the network the name of the coffee shop in order to confuse potential victims. "Even more deviously, Darren can create a Wi-Fi signal called Linksys, T-Mobile, ATT Wireless or Gogolnflight. If your computer has ever connected to those legitimate networks in the past, it will be fooled into thinking it already has permission to connect — and does so through Darren's router." [35] Darren then furthers that once someone has connected to his router, he can see everything that person is doing and at that point, he can mimic a banking site in every way to garner login credentials. Although Becky sees the legitimate front end of her banking website, Darren is actually mimicking her actual bank's website. The article furthers that phones using "Wi-Fi to connect to the Internet are susceptible to hacks just like the Wi-Fi café." [35]

The thesis now makes a pinnacle shift from understanding how things are to what can be done. The dynamics of the existing menaces has been explained and now it becomes critical to understand the appropriate responses and actions. According to a 2014 article in the New York Post, "four years ago, the number of identity-fraud victims was 1 in 9, and last year it was 1 in 3."[36] This topic is no longer avoidable and those who are knowledgeable and well equipped will know how to be vigilant as the sharing of data becomes more difficult to prevent. The next section dives deeply into the ITAP, the Identity Theft Assessment and Prediction tool built by the University of Texas for visualizing thefts as a business process.

# 4. The ITAP: Identity Theft Assessment and Prediction Tool

This section will provide an overview of the ITAP, including, an end-to-end example of an identity theft scenario, an explanation of the rationale behind studying theft as a business process as well as a look at the ITAP model. The section closes out with a thorough look at what analytics the research will gain from the ITAP and the contributions of the tool.

## 4.1 The ITAP Overview

A recent article in the New York Post stated, "a stranger takes over someone's life about once every two seconds."[36] Over the past decade, the Federal Government and most states have passed legislation to impose criminal sanctions on identify theft. The government has recognized the severity and prevalence of identity theft but most advice is reactive at best. Efforts to combat identity theft have been hampered, however, by the elusiveness of the definition and its overlap with the elements of many other crimes. Additionally, the long-term and multi-jurisdictional nature of identity theft and the looming question as to whether law enforcement agencies or financial institutions are better equipped to combat it, add to the inability to fully contain the problem [37]. Despite understanding there is a problem, it appears as though no one is quite sure who should take ownership in solving it. Likewise, little time has been spent researching the process behind how identity theft occurs. Readily available are best practices and prevention tips from security companies and government agencies alike. Most information available is helpful once identity theft has occurred, but does not help in the thwarting of future thefts. What is void, however, is a pool of data surrounding the process involved in stealing an identity.

The Center for Identity at The University of Texas at Austin is developing a repository of knowledge to better understand the business processes used by identity thieves and fraudsters. The aim is to understand the criminal's business process, the vulnerabilities that allow the crime to take place, the resources that facilitate it and what, if anything, can be done to prevent it. Armed with this knowledge, a shift in the definition and use of credentials may be explored to decrease identity theft and fraud vulnerabilities. Conversely, it may be simply an increased awareness of what exploited vulnerabilities often result in an attack. In order to better analyze dependencies, The Identity Threat Assessment and Prediction (ITAP) tool is piecing together a business-like model of theft scenarios, criminal methods and techniques. This tool will allow for a better understanding of a fraudster's behaviors in order to make connections and visualize patterns based on past identity theft and fraud attacks. As more information is funneled into the tool, the ITAP will deliver actionable knowledge that is grounded in the study of past thefts and frauds. The big questions the ITAP hopes to answer in the near future are: How are these perpetrators gathering information, i.e. through what vulnerabilities? What resources are being used to overcome security hurdles? What process steps are being taken to steal someone's identity? Should the understanding of what credentials are considered safe be redefined? The coming section walks through an example of identity theft as a means of better understanding the power of the ITAP.

## 4.2 Identity Theft Scenario Example

In order to more concretely illustrate the ITAP model and its utility, a real occurrence of identity theft is closely examined. In a larger-than-life example involving home equity loans, one man steals millions by carrying out a series of well-articulated steps, equipped with both resources and readily available data. Figure 3 below illustrates the entire home equity fraud process from start to finish.

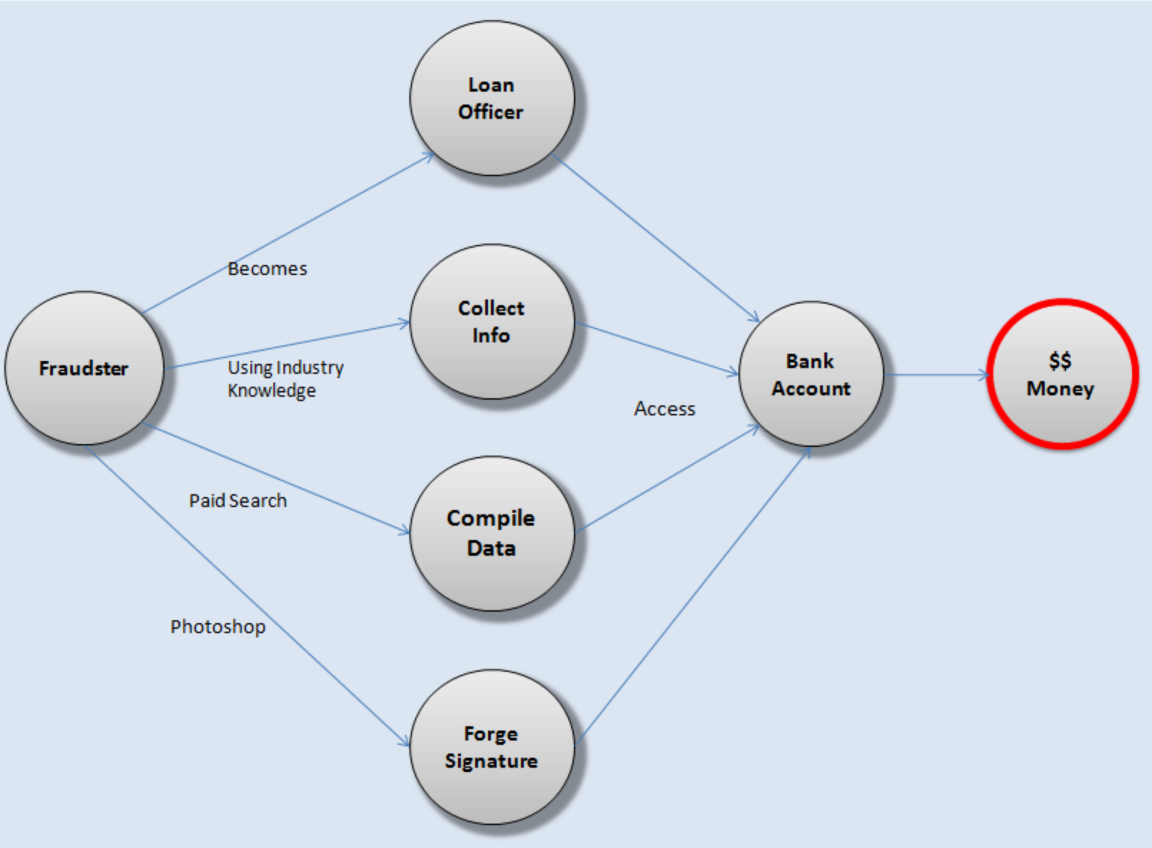


Figure 3: Home Equity Fraud Process

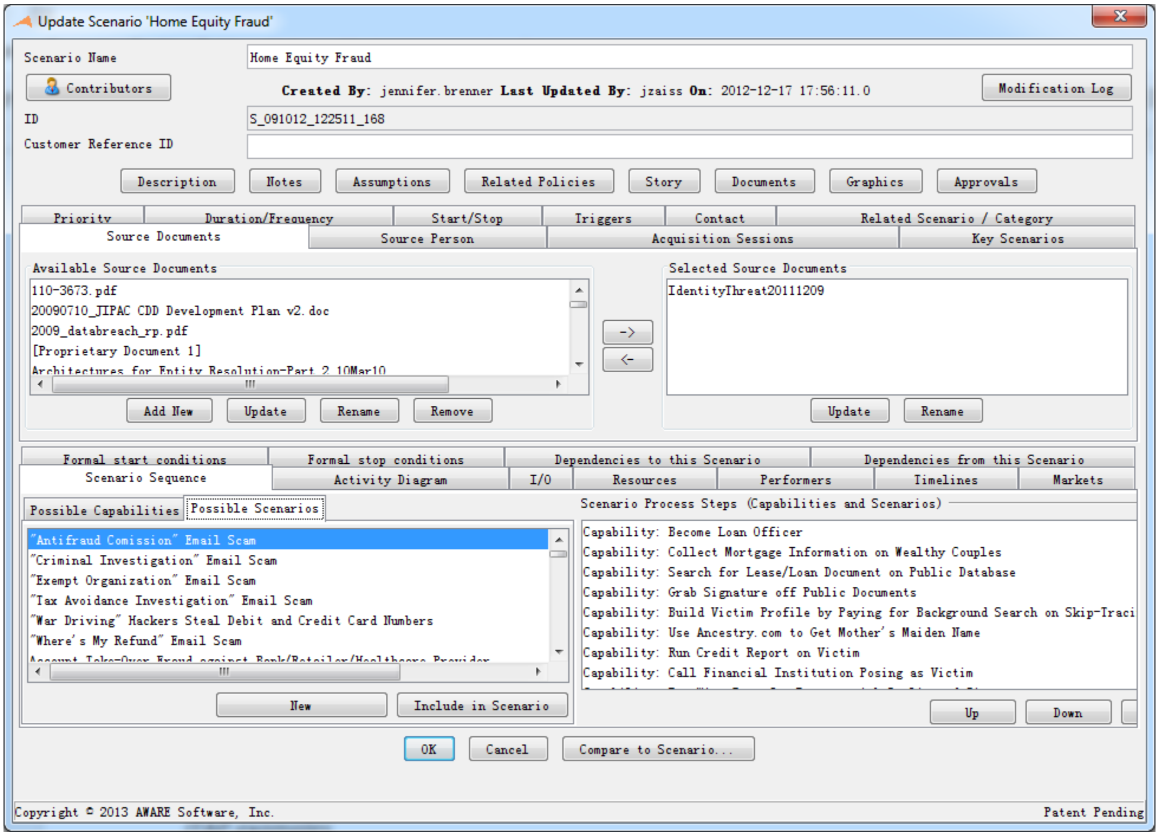
The first step the fraudster took to complete the fraud was to become a loan officer. He did this in order to learn the inner-workings of loan processing. This proved to be critical knowledge for him as he utilizes it throughout the fraud. Furnished with this industry knowledge, he knew how and what mortgage information would be needed in order to commit this type of fraud. With wealthy couples as his primary target, he then searched for lease and loan documents in public databases. He knew exactly where to look and what type of victims would make sense given his experience working in the industry. One he had located an appropriate victim and their loan document; he used a readily available resource called Photoshop to grab the victim's signatures from the documents.

Next, the fraudster compiled profiles of the victims via paid searches on skip-tracing sites, gathered credit reports from Experian, and obtained authentication information from Ancestry.com. The compilation of this profile is what historically has made large-scale fraud more tedious. This is why data aggregation is a legitimate concern. Whereas in this case, a profile was created leveraging numerous online sources, many data aggregators could potentially lump this information together, in one place. This could make committing fraud a process involving very few steps. Fewer steps mean fewer opportunities to stop the fraud from happening. Experian, Ancestry.com and public databases gave the fraudster access to the victim's addresses, phone number, mother's maiden name and birthdate.

With an arsenal of information, the fraudster was well positioned to carry out the remainder of the fraud, which involved the processing of new, fraudulent loans. When it came time to processing these documents, the fraudster never physically walked into the financial institution conducting the transaction. Due to his knowledge of industry protocols, he specifically targeted credit unions and smaller banks in order to ensure a process that did not require an in-person appearance. First, he would call the victims' bank with a resource called SpoofCard. This allowed him to pose as the victim by projecting the victim's phone number to the financial institution. Cleverly, he used this as an additional means of validating his identity when requesting to wire transfer money. He completed these transfer documents by applying the photoshopped signatures and faxing them back. Lastly, he worked with several international partners to launder the money by sending it internationally and paying his partner to return it minus a transaction fee. In total, he stole roughly $7 million dollars every two weeks for over a year.

Perhaps the most unsettling part of this fraud is that the fraudster did not begin the fraud with a wallet, access to a bank account or a credit card number. These are the things typically associated with identity theft. This fraudster began this highly elaborate, highly lucrative fraud with nothing. Through the manipulation of various vulnerabilities, online databases and financial institutions, he was able to use resources to build profiles on victims until millions were stolen.

Figure 4 below depicts the aforementioned Home Equity Fraud example as it appears in the ITAP. The capabilities, or steps, are listed in the order they took place during the course of the fraud. This helps visualize what progression took place and any dependencies between steps.



Scenario Name: Home Equity Fraud

**Created By:** jennifer.brenner **Last Updated By:** jzaiss **On:** 2012-12-17 17:56:11.0

ID: S_091012_122511_168

Customer Reference ID:

Available Source Documents

110-3673.pdf
20090710_JIPAC CDD Development Plan v2.doc
2009_databreach_rp.pdf
[Proprietary Document 1]

Selected Source Documents

IdentityThreat20111209

Possible Scenarios

"Antifraud Comission" Email Scam
"Criminal Investigation" Email Scam
"Exempt Organization" Email Scam
"Tax Avoidance Investigation" Email Scam
"War Driving" Hackers Steal Debit and Credit Card Numbers
"Where's My Refund" Email Scam

Scenario Process Steps (Capabilities and Scenarios)

Capability: Become Loan Officer
Capability: Collect Mortgage Information on Wealthy Couples
Capability: Search for Lease/Loan Document on Public Database
Capability: Grab Signature off Public Documents
Capability: Build Victim Profile by Paying for Background Search on Skip-Traci
Capability: Use Ancestry.com to Get Mother's Maiden Name
Capability: Run Credit Report on Victim
Capability: Call Financial Institution Posing as Victim

Copyright © 2013 AWARE Software, Inc. Patent Pending

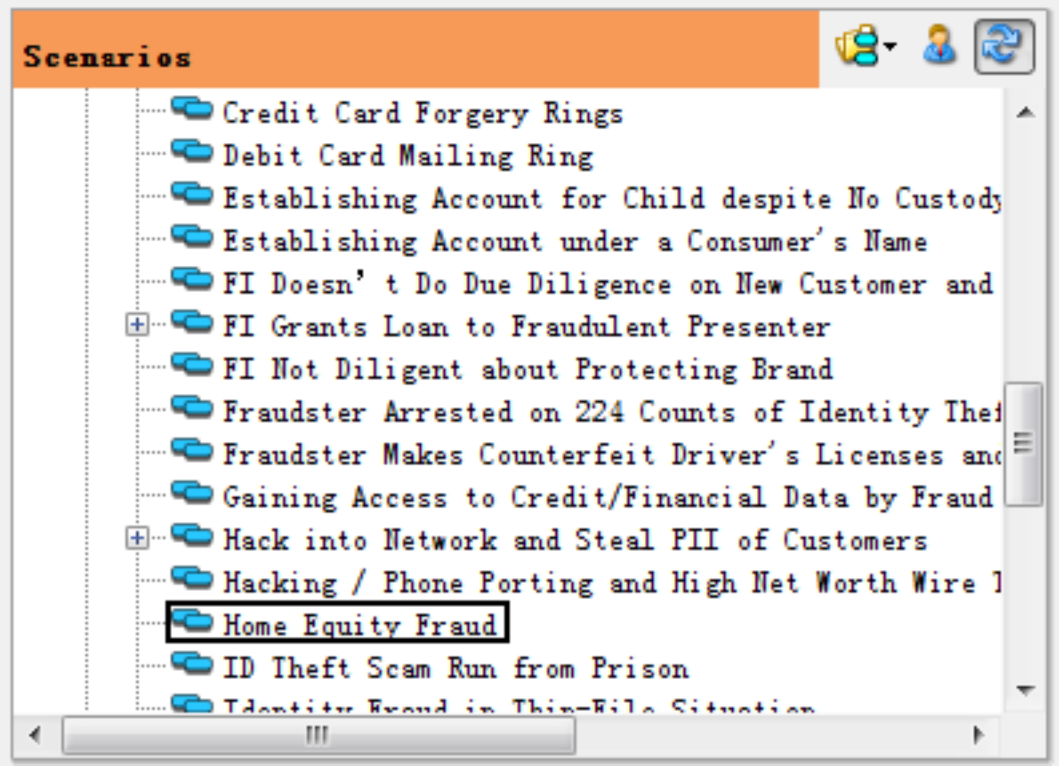
Figure 4: Home Equity Fraud Scenario inside the ITAP [39]

Section 4.3 describes the ITAP model representation and closely examines each component in order to see how the data in each scenario, such as the example above, is filtered into the ITAP for further analysis.

## 4.3 The ITAP Model

"A business process is defined as a collection of related, structured activities or tasks that produce a specific service or product (serve a particular goal) for a particular customer or customers. It often can be visualized with a flowchart as a sequence of activities with interleaving decision points or with a Process Matrix as a sequence of activities with relevance rules based on data in the process"[38]. This brings this thesis to the third research question, why is it important to study identity theft as a business process? The answer is simply that the process of committing identity theft mirrors a typical business process, in that each step is methodical and serves a particular goal. Resources as well as input and output data elements allow the fraudster to advance from one step in the process to the next. As with any business process, if a critical step is missing or cannot be completed, the business process as a whole is halted. By viewing identity theft as a business process, ITAP provides a better insight and understand of how these crimes are committed on a granular level. This helps develop an understanding of the most critical part of the process. This could be either a pinnacle step or a resource, that without access, would have stopped the fraud at that point and rendered the fraudster unable to continue. With this invaluable information potential countermeasures can be shaped to prevent this step or deny access to this resource.

Each piece of the ITAP model is now discussed in detail. Understanding how the pieces come together is critical to understanding the business process ideology. The ITAP model consists of several components, which are used to describe and analyze the different parts of the whole identity theft process. Figure 5 below looks at the section within the ITAP housing the different scenarios.


Scenarios

- Credit Card Forgery Rings
- Debit Card Mailing Ring
- Establishing Account for Child despite No Custody
- Establishing Account under a Consumer's Name
- FI Doesn't Do Due Diligence on New Customer and
- FI Grants Loan to Fraudulent Presenter
- FI Not Diligent about Protecting Brand
- Fraudster Arrested on 224 Counts of Identity Thef
- Fraudster Makes Counterfeit Driver's Licenses anc
- Gaining Access to Credit/Financial Data by Fraud
- Hack into Network and Steal PII of Customers
- Hacking / Phone Porting and High Net Worth Wire T
- Home Equity Fraud
- ID Theft Scam Run from Prison
- Identity Fraud in Thin-File Situation

Figure 5: ITAP Scenarios [39]

Figure 5 depicts a snapshot of the scenarios, or stories, currently in the ITAP. A scenario is an "operational process involving a sequence of steps to be executed by a human user, an automated system, or some combination of both. A step in a scenario is either a step in the criminal's business process or another scenario. Although any given scenario can be broken down into a sequence of steps, in some cases, it is convenient to treat a particular sub-sequence of those steps as constituting a scenario in its own right; in such cases the latter scenario can be called a sub-scenario of the given scenario."[39] Dependencies between the capabilities within the scenario are used to connect steps within the scenario. Understanding dependencies can really shape our understanding of what is required for the scenario to take place. This modeling approach and representation has its foundation in traditional business process modeling. Specifically, this research leverages an implementation of the scenario and business process modeling found in the AWAREness modeling methods and tool suite.[39]

“Two or more scenarios with partly overlapping sequences can be related in such a way that one scenario is said to be the “normal course” and each of the others either an “alternate course” (a different way the scenario can play out) or an “exception course” (an error-registering flow that ends without accomplishing the intended goal) to the normal course. Sometimes a normal course scenario and its alternatives and exceptions are grouped together as a use case. For example, in a “Drive to Work” use case, the process of driving to work via a usual route could be seen as the normal course scenario, taking a detour on the way to work because of road construction would be an alternate course, and having a mechanical breakdown on the way to work would constitute an exception course”. [39]

Figure 6 below shows a snapshot of the data, events and reports section of the ITAP. Data, events, and reports are types of information that are exchanged between steps, between scenarios, or between the system and its users.

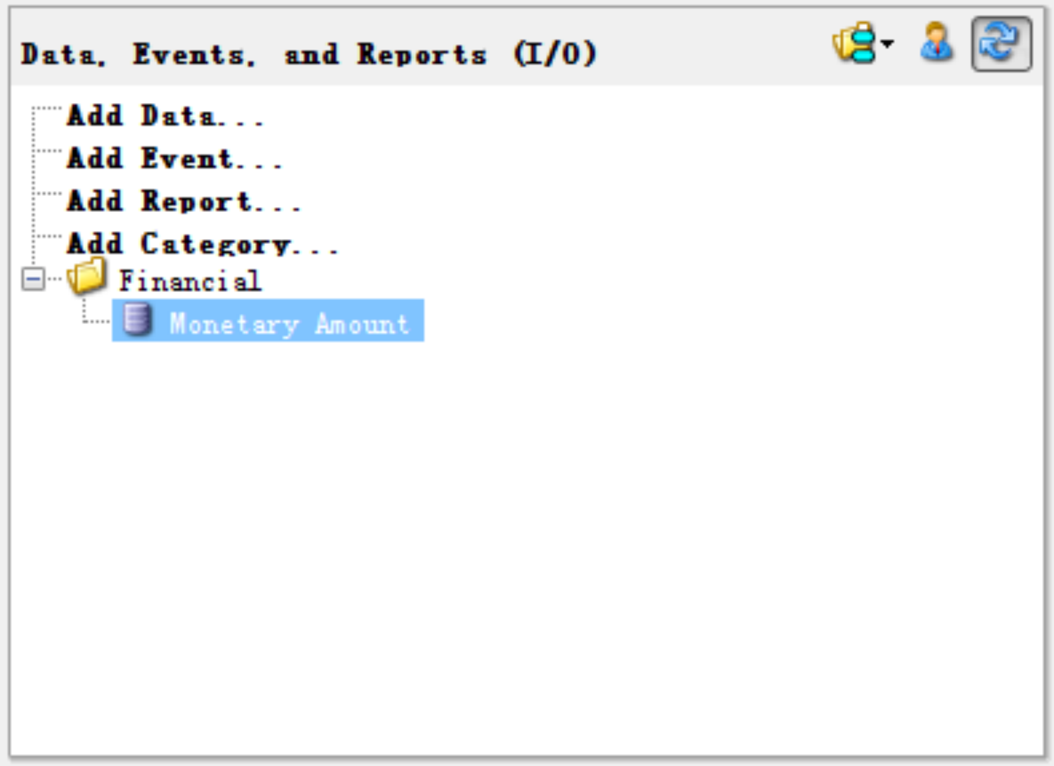
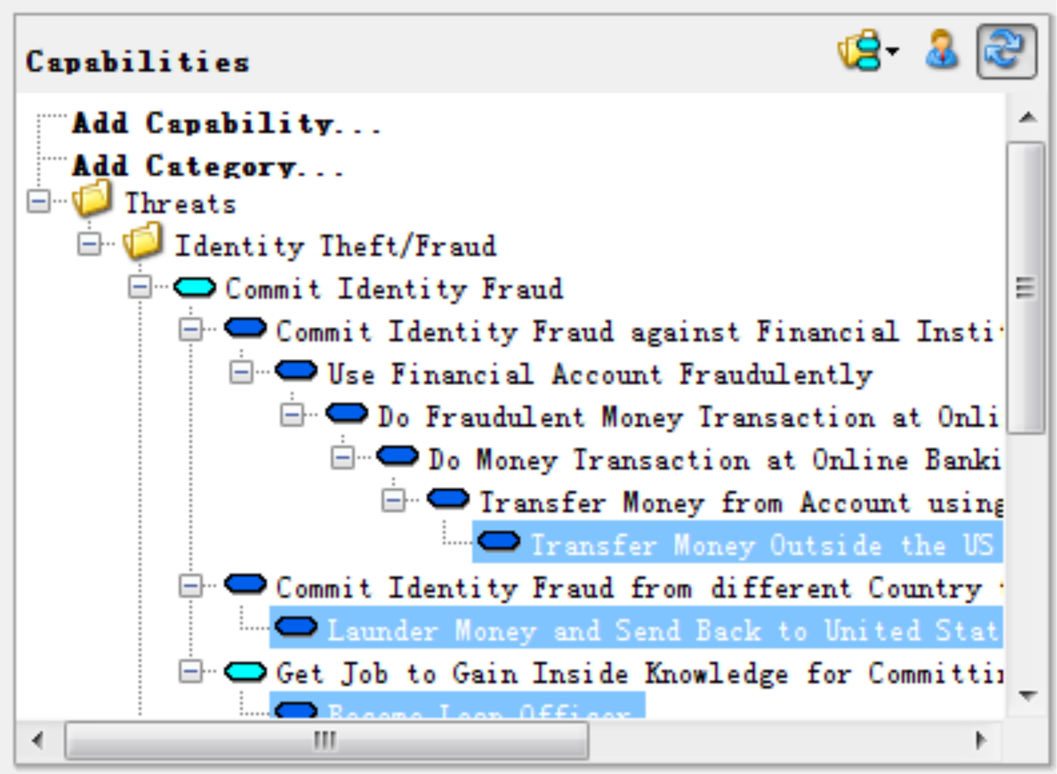


Figure 6: ITAP Inputs and Outputs (Data, Events, Reports) [39]

A data element "is a machine-readable piece of information with a relatively stable value, an event is a transitory piece of information to the effect that a certain system event has just occurred, and a report is a piece of information intended to be interpreted and understood by a human being (e.g. a chart or an email message). A data item or report might be simple (e.g. an integer or a string) or it might be composite, having a structure built from other data items". [39] As a reference, in the home equity fraud example described above, the fraudster determined which victims he would pursue by pulling each couple's HELOC eligibility details. The HELOC details, or Home Equity Line of Credit details, provide information on a specific type of loan the fraudster used to carry out his scam. This document is an example of the type of data elements logged in the ITAP since it was how the fraudster determined the eligibility of a potential victim.

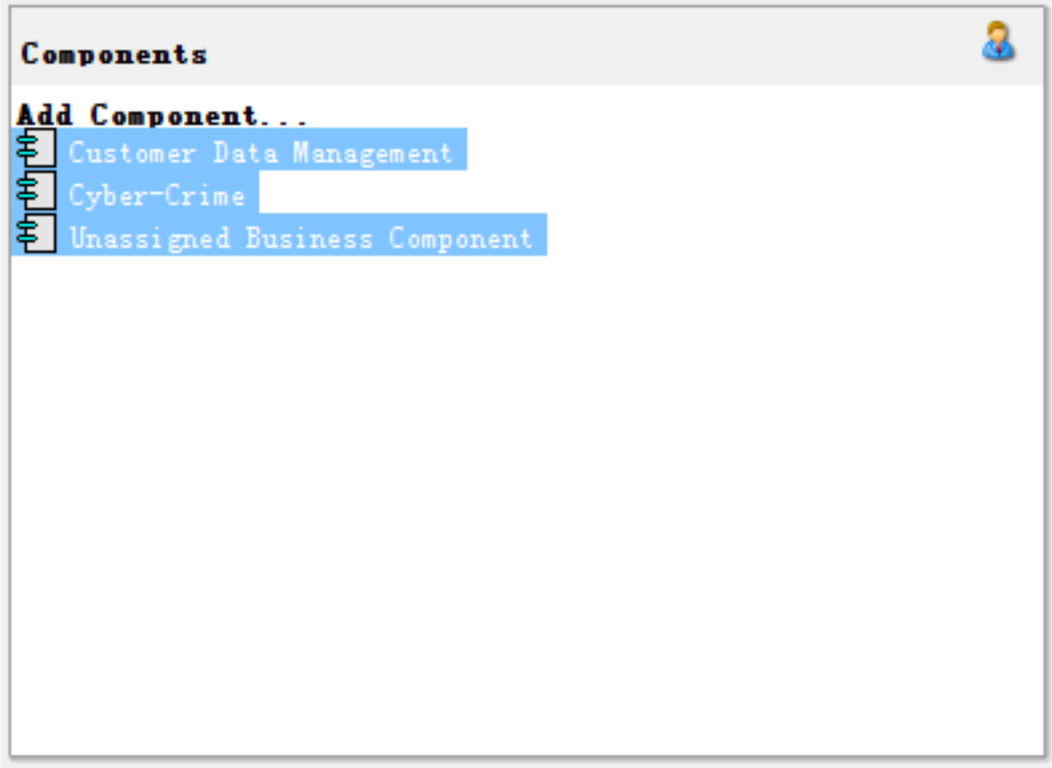


Capabilities

- Add Capability...
- Add Category...
- Threats
  - Identity Theft/Fraud
    - Commit Identity Fraud
      - Commit Identity Fraud against Financial Insti
        - Use Financial Account Fraudulently
          - Do Fraudulent Money Transaction at Onli
            - Do Money Transaction at Online Banki
              - Transfer Money from Account using
                - Transfer Money Outside the US
      - Commit Identity Fraud from different Country
        - Launder Money and Send Back to United Stat
      - Get Job to Gain Inside Knowledge for Committi
        - Become Loan Officer

Figure 7: ITAP Capabilities [39]

Figure 7 shows the structure of the capabilities in the ITAP. Capabilities are the actual steps, or things the fraudster had to be capable of doing, in order to carry out the overall fraud. Looking back again to the Home Equity fraud example described, the fraudster's first step was to obtain a job as a Loan Officer. He used this to learn the internal processes involved in processing loans. This was a crucial step in the overall scheme since the knowledge acquired here allowed him to move meticulously towards his end goal. He was able to learn exactly what the proper procedures were in handling loan documentation, how financial institutions handled authentications as well as which types of banks were the easiest targets.  Without this prior knowledge, he may not have been successful in such an elaborate scheme.  How can this knowledge be capitalized on? Is it feasible to make it more difficult for these types of jobs to be acquired? Multiple steps in the fraud relied on the data acquired at this point.  It may be advocated that whatever knowledge learned at this juncture could be learned online, and this may be true, but understanding what can and cannot be prevented is also an important part of analyzing the information in the ITAP.  There will be steps that can be waived as red flags and others for which there is no practical means of preventing.



Components

Add Component...

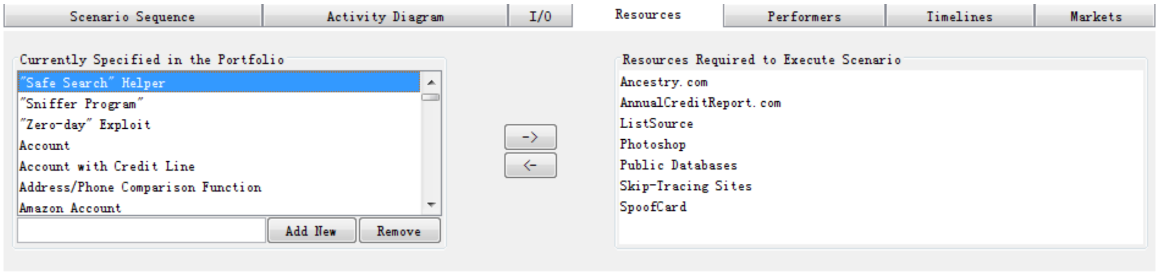
Customer Data Management

Cyber-Crime

Unassigned Business Component

Figure 8: ITAP Components [39]

Figure 8 above depicts the components section of the ITAP. A component "is a logical collection of capabilities (steps) and its associated inputs and outputs. Each component is composed of functions, data, reports, and events." [39] This allows us to group frauds as a means of understanding trends across an entire vertical, such as Data Management. The more trends that are seen, the more dots that can be connected which may prove useful in theft and fraud prevention.



Currently Specified in the Portfolio

"Safe Search" Helper
"Sniffer Program"
"Zero-day" Exploit
Account
Account with Credit Line
Address/Phone Comparison Function
Amazon Account

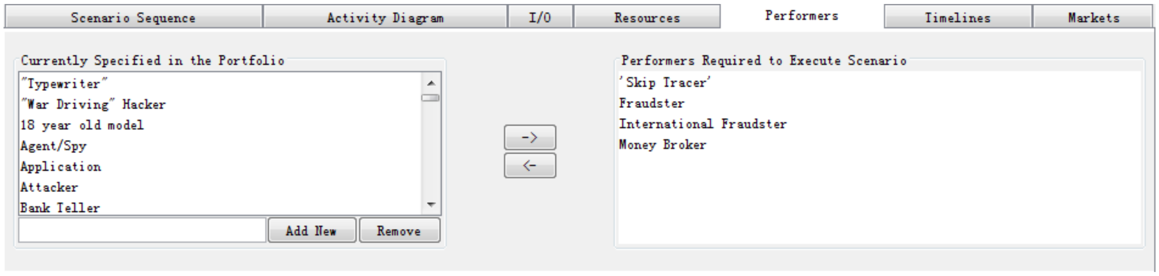
Resources Required to Execute Scenario

Ancestry.com
AnnualCreditReport.com
ListSource
Photoshop
Public Databases
Skip-Tracing Sites
SpoofCard

Figure 9: ITAP Resources [39]

Fraudsters use resources to complete each step and often, resources prove critical to the completion of the fraud itself. A resource, shown in figure 9 above, can be anything from malware code or credit card skimmers to easily accessible software, such as Photoshop. Anything that the fraudster physically uses can be considered a resource, and unfortunately, our research indicates that many of these resources are readily available. In the home equity example, many resources were used to commit the fraud described. A *call spoofer* was used in order to provide a second layer of identity verification. Photoshop played arguably the most significant part in the fraud because it allowed the fraudster to sign the financial documents using stolen signatures. Without Photoshop, the fraud may not have been able to take place. The question then is, can access to Photoshop be limited? Well, it is a commercial product so it is not likely that individual access to it can be limited. Once aware of what resources are commonly used in identity theft, the research may help in the proper raising of red flags where feasible. For example, should the ITAP be able to fuse a direct connection between blank Visa & MasterCard gift cards and identity theft, state governments may be compelled to take action. These gift cards are commonly used to enable theft and fraud by providing the ability for credit card skimmers to make physical copies of a card. These cards are then used to make big ticket purchases. Government actions could include limiting the number of cards any one person can purchase at one time or requiring the gift cards to be linked to a valid form of ID. Even small restrictions such as these could make purchasing these cards more of a hassle and inevitably, slow fraudsters down. Understanding what can be feasibly resolved and what cannot be resolved is critical because it is the first step in devising a strategy.

Figure 10 below depicts the section of the scenario where any performers, or accomplices, of the fraud are accounted for. This helps pinpoint what types of people helped in the advancement of the actual steps. Performers are those who played a great part in executing a scenario or completing a step. Did this result from an internal leak of information? Was an employee involved? Was it a hacker? Was it a skimmer? Did someone internationally play a part?



Currently Specified in the Portfolio

"Typewriter"
"War Driving" Hacker
18 year old model
Agent/Spy
Application
Attacker
Bank Teller

Performers Required to Execute Scenario

'Skip Tracer'
Fraudster
International Fraudster
Money Broker

Figure 10: ITAP Performers [39]

It is very important to assess who the key players are at each step. Doing so provides a view of the big picture of how many and what types of people were necessary in carrying out the attack. In the home equity example analyzed throughout the discussion of the model, although there was one major fraudster, he did receive assistance internationally. He worked with both an international fraudster and broker when transferring the stolen money outside the US. This performer's help is what allowed him to keep the money he stole. Without laundering it, he never would have been able to go as long as he did without being caught.

The ability to associate precedence is a principal feature of the ITAP. This is accomplished by the linking of specific steps together through the addition of START and STOP conditions. What this does is allows for steps to be linked together in the event that one step is absolutely required to be completed before the next step can begin. For example, in the case study, the fraudster needed to run the victim's credit report in order to gain access to specific HELOC details. Because the data input to running the credit report required knowledge of the victim's address, date of birth and social security number, the preceding step was critical. This preceding step, which involved building the victim's profile by paying for a background search on a skip-tracing site, is thus a necessary START condition. Meaning, the fraudster needed to complete the background search step prior to being able to access the credit report. Steps are linked together, if and only if one would always follow the other. This allows true connections to be developed between the steps themselves to better understand the dependencies between them. The hope is that upon further analysis, similar pairs of steps occurring in conjunction signal potentially looming identity fraud or theft. Clear connections can be made on how the information is flowing and what the dependencies look like. This type of pattern detection will prove invaluable in predicting future identity theft scenarios.

The ITAP tool seeks to decompose each incident of identity theft in such a way as to understand on a detailed level how things occurred. Common steps and dependencies between those steps as well as any resources and/or data elements that were indispensable are highlighted by the ITAP. The next two sections investigate the analytics of the ITAP, the information the research intends to amass as the ITAP grows, and the overall contributions the ITAP will make to the community.

## 4.4 The ITAP Analytics

The data gathered by the ITAP should help paint a better "big picture" of how thefts are occurring. Currently, the research team funnels identity theft related articles gathered from online news engines into the ITAP and properly categorizes them so that connections are modeled and patterns are explored. There are several things the research team hopes to understand as more and more data is amassed.

First, the research effort is seeking to the most common data inputs required for any given step within a scenario to occur. Establishing the most common data inputs required to complete a capability is critical to understanding and potentially thwarting an identity attack. Without this initial piece of data, many attacks may not take place. What information did the fraudster already have on hand? Did the fraudster have access to an email account? Was he/she able to view the victim's place of birth on Facebook? Understanding what fraudsters have in the beginning at their disposal may shape and alter the consumer's perceptions of how they should identify themselves. The truth is, personal lives are no longer very personal. Identities are now being heavily publicized by the usage of social media, and therefore, verifying a date of birth is probably no longer a secure form of verification since this data is readily available. This is exactly what the research is trying to discover. What elements, if any, are no longer secure? With the proper data, the research can hopefully make the general public aware that a different element should be used for purposes of identification. The data items long thought to be secure may not be anymore. There are many such credentials that people do not currently feel the need to safeguard, such as their phone number or email address. Based on this research, however, better education can be provided regarding the protection and security of personally identifiable information.

Second, this research effort wants to understand exactly what the fraudster hopes to accomplish in each given scenario. Is there a specific data element the fraudster completed the step in hopes of acquiring? Showing the most common data output resulting from certain steps that are taken helps create a full picture of the entire business process. Often, the data output in one capability is a necessary input to the next step. What are the most common data outputs? Although big picture this seems fairly obvious, it is important to ascertain explicitly what the fraudster hoped to accomplish at each step.

This will provide a better understanding of exactly *how* the criminal is getting their hands on certain pieces of information. How exactly did fraudster from the home equity example end up with the victim's Mother's Maiden Name? He was able to Google information and use it as input on Ancestry.com. Sites such as Ancestry.com pose a significant challenge because the entire purpose of the site is information discovery. How are fraudsters accessing other people's Ancestry.com accounts? Understanding what data is known or being acquired is critical to understanding the entire process.

Third, the research effort aims to use the ITAP to detect any repetitive groupings that exist between steps in the scenarios. Understanding if there are groups of capabilities that often work together, may help visualize patterns emerging once a string of events occur. Are there two or three steps that typically follow each other across multiple scenarios? Could these steps, when completed in conjunction, signal that identity theft may be amiss? The research suggests this. Because the ITAP makes connections between steps through START and STOP conditions and relating steps together, the ITAP uses this information in further pattern detection.

Lastly, this research effort wants to analyze resources that are commonly used across scenarios. Detecting frequently used resources helps materialize how fraudsters are gaining access to sensitive information or infiltrating institutions with our data. What are the most common resources being used to commit identity theft and fraud? Can access to these very common resources be limited or, at a minimum, can the resource providers be made aware? Often times, these resources are principal to the completion of the step. Any analysis done in this area could significantly advance identity theft detection and prevention. It may also help to view prevalent resource usage across industry verticals or market segments. What resources are aiding specifically in medical identity theft? To stop identity theft and fraud, the tools used must both discovered and studied. Just as it is important to understand the what, it is paramount to understand the how. How is our data taken? How are institutions being penetrated?

### 4.5 THE ITAP CONTRIBUTIONS

As an analytical repository, ITAP provides a view of identity solutions pertinent to the identities of people, organizations, and devices across multiple domains. The model's representation of past threats and potential responses, or countermeasures, helps in the understanding and analysis of the current threats and solutions. From the analytics, ITAP is amassing, the most vulnerable entry point to a person's identity information can be discovered. This is typically the information that is most easily acquired and used by fraudsters. Moreover, correlations between the compromised identity data and gains reaped by fraudsters can be discovered to better understand which identity data is the most valuable. This allows for a shift in the community's thinking in what information should be protected and whether different credentials may be preferable as means of identification. The trends on threat resources and compromised identity attributes can also be found by using the ITAP. A collection of recommendations and proactive measures to guide the average consumer in vigilant protection of their identity will emerge as the ITAP becomes increasingly robust.

Although in time the ITAP will deliver trends compiled by thousands of theft occurrences, the following section discusses a small study meant to illustrate the power of such knowledge. The following section takes a look at a sample of news articles in order to draw illustrative conclusions as to what the most used resources and most vulnerable data elements are in identity theft scenarios.

# 5. The Data and Results

In addition to funneling data into the ITAP and helping to develop its utility, this research effort also conducted a small study in order to comment on the first and second research questions. In reviewing the articles, the aim was to understand what fraudsters are commonly using as resources as well as what data seems most vulnerable. Section 5 provides a brief overview of the tool developed as part of this thesis research, DataImporter, and discusses the results.

## 5.1 The Tool, DataImporter

All of the data analyzed in the study was processed through the tool built in Python called the DataImporter. DataImporter used the Bing API to search the web for news articles related to identity theft and stored those articles to be later parsed by DataImporter. Several different types of searches were attempted and the results were filtered manually. This manual filtering helped ensure that articles that did not provide valuable information were not included in the study. Many articles failed to actually discuss what data elements and resources the fraudsters used to commit the crime or how the crime was actually committed.

To ensure that each article was unique, it would be checked against articles that were already processed by the tool. If there was a match, the article was ignored in order to prevent duplication and a potential inflation of a certain resource or element. Once the article was deemed relevant, it would be parsed to extract the key information. First, the entire article was tokenized. Then, each word is stored in a dictionary and then stored again by concatenating it with the next word. This would occur until every 4 words were concatenated together. Four was selected because most resources and data elements were four or fewer words in length. This number could be easily varied in the algorithm for future experiments. This process allowed for resources like “vehicle registration license plate” to be recognized since “vehicle”, “vehicle registration”, “vehicle registration license” and “vehicle registration license plate” are all stored in the dictionary due to the repetitive concatenation.

At this point, a predefined list of resources and data elements was pulled from the ITAP, tokenized and stored in a separate dictionary. The two dictionaries were then compared in order to see if any of the tokens pulled from the article, matched the tokens in the ITAP dictionary. The results are then tallied to see which resources and data elements occurred most prevalently in the set.

### 5.2 The Results

After analyzing100 articles, this thesis comments on the first and second research questions presented in the paper.

In terms of the first question, *What are the most common resources fraudsters are using*, the data showed that the most common resource utilized by fraudsters to commit theft was a credit card skimmer. Credit card skimmers are often used in conjunction with fraudulently obtained credit card numbers in order to create counterfeit cards that can be swiped. Recent breaches, like the ones experienced by both Target and Neiman Marcus, involved the theft of “credit card numbers and personal information of tens of millions of customers during the 2013 holiday season.” [40] Target has publically stated that the “hack cost the company as much as $61 million in the final months of 2013.” [40] Although isolated knowledge of a credit card skimmer’s prevalent usage does not provide a resolution, in conjunction with the additional information gathered by the ITAP, the hope is to formulate an understanding as to how or where credit card skimmers are being acquired, where they are being used and other data that may prove useful in theft prevention.

Question two asked, *What personally identifiable data seems to be most exploited?* Based on the results, the most compromised data element is the social security number. Many cases of theft and fraud began with an employee or insider stealing medical records, patient information or consumer data and then selling the data to fraudsters. It is fairly common knowledge that a social security number is a sensitive piece of data, however, the ITAP will gather further information to understand other ways which social security numbers are being obtained.

Although this is a limited example, on a large scale, the ITAP will examine nationally, what the trends are across thousands of scenarios. This data will be magnified, resulting in a clearer vision of how scenarios are unfolding through the robustness of the ITAP. The next section looks into the future of identity by examining new methods of identification, what consumers can do to protect themselves and what companies are doing.

# 6. The Future of Identity

This section investigates the future of identity by looking at a few alternate methods of identification. These alternative methods such as retinal scans, voice authentication, and fingerprint scanning may help provide a glimpse into the future of security. Although these alternatives are discussed, they are not without fault and are by no means 100% secure. Ultimately, consumers should always be heedful in self-protection. Section 6.2 and 6.3 look at what can be done to increase caution and what companies are doing as well. The central thing to note is that this space is constantly evolving and best practices will change often. At minimum, it is critical to be aware of what personally identifiable information is vulnerable. It is unrealistic for consumers to expect those that gather PII to care about its security as much as the consumer who provides it.

## 6.1 New Methods of Identification

There are several alternative forms of authentication, such as fingerprint scanning, retinal scans and voice recognition that are promising consumers heightened levels of security. Although an entire paper could be written about the benefits and potential pitfalls of the different biometric forms of authentication, this section is a survey of things to consider.

Fingerprint scanning technology has existed for some time. Despite its history, not everyone is convinced it is safe. “Skeptics point to the security vulnerabilities and long-term reliability issues associated with fingerprint readers that shipped with laptop computers, like IBM ThinkPads as well as mobile phones from the likes of Motorola and LG." [41] Apple recently decided to implement fingerprint technology, Touch ID, on the iPhone 5 in order to give users easier access to the device while also providing an additional layer of safety. The idea is that because fingerprints are unique to each person, this will augment the security of the device. A recent article in Engaget explains why the Touch ID is safe by offering some insight into how the technology works. The article explains, "Each A7 chip has a unique secure space that neither the A7 nor Apple can read, and every authentication session is encrypted end-to-end." [42] The article furthers that "the print only lasts in memory until it's turned into a decryption key." [42] Like many other technologies, the initial reviews and company disclosures are typically very optimistic about safety. In a recent article on the same topic, "Hamburg Commissioner for Data Protection and Freedom of Information John Caspar believes that the use of biometric technology for the sake of consumer convenience could become a hacking treasure trove, granting them access to permanent data which cannot be deleted or changed". [43] Although Apple alleges that the data will be only stored locally and encrypted, Caspar remains unconvinced, saying that while the "iPhone's fingerprint readings would only be stored on the device and not on centralized servers, cyber attackers who compromise a smartphone through malicious applications would still be able to access the biometrics". [43] At first look, the idea of fingerprint scanning appears secure since fingerprints are unique to each individual. But this fact is exactly what makes this idea unnerving. While the vulnerability of a given technology is often left up to debate until a large-scale breach occurs, the vulnerability of a fingerprint is inherent and the actual security benefits are unclear. Is it in fact worth it? Is the consumer truly more secure? A consultant for Security firm Neohapsis said to CNN late last year, "There should always be some concern with new technologies or functionality that has such a large base of users." He continues, "the fingerprint reader is more of a sales tactic than a strong security enhancement."[44] The security of the system lies in the weakest link and on the iPhone the fallback is just the 4-digit pin code. The iPhone has prompted users to exchange a very sensitive biometric for mere promises of additional security. Ultimately, a copy of our fingerprint is made. Although Apple assures consumers this will not happen, this blatant assurance is very typical of companies when they are introducing new technology. It is a new technology and only time will tell how hackers will attempt to exploit it and often times, these exploits are so creative, there is no way to prepare until it is too late. Unlike a debit card that can be cut up and thrown away if it is counterfeited, a fingerprint cannot be altered or deleted.

Retinal scanning is probably the most well known type of biometric authentication yet probably the least widely used. [45] It is used prevalently in government realms but has yet to reach mass consumer usage as a form of authentication. The idea of retinal identification is to map the patterns of the eye, which are unique to each individual with little room for error. "Retinal scan is a highly dependable technology because it is highly accurate and difficult to spoof, in terms of identification". [45] The lack of widespread usage could be because "it can be a difficult process to provide sufficient data for matching to take place." This results in a large quantity of false negatives. Although it is not currently being used actively, similar concerns are raised when considerations are paid to the thought of having an image of the unique patterns of an eye stored in a database somewhere or even on a phone.

The last of the biometrics explored is speaker recognition, which is the ability to identify a person by the characteristics of their voice. According to Opus Research, "voice biometrics is part of the ideal authentication solution that "balances both ease of use and security concerns. Voice authentication works in real-time (meaning it's fast)." [46] There are now flurries of companies that have built their business on creating voice authentication software. Some institutions are adopting this for widespread usage. "New Zealand's Inland Revenue Department recently declared that 400,000 people (that is one in ten New Zealanders) have registered to use their system that checks users voice to confirm their identity."[47] Voice authentication Nuance Voice Biometrics, a company specializing in voice authentication software explains, "Voice Biometrics authenticates your customers through natural voice patterns, not robotic PINs, passwords, and questions. It's a level up in security. It's a brand new user experience. By giving them the freedom to speak, you let the customers be themselves." Is voice then the way of the future in terms of authentication? Experts feel the industry is at least a decade away from reliable voice authentication. [48] A cost benefit analysis between reliability and cost seem to be what companies use in the decision making process that determines if a new technology makes sense. In terms of voice authentication, if it is implemented as a means of making personal data more secure, advancements need to be made in ensuring reliability since the stakes are high. Like the other biometrics discussed, the high likelihood of a copy of our voices, raises serious security concerns. But just how likely is it that someone could steal our "voice-print"? According to a recent article in BT Let's Talk by Alex Noble of Cisco, "unique 'voice-print' is much harder to replicate and, as long as the technology works, is much more secure."[49] He furthers in the article that "huge developments in voice recognition technology are revolutionizing some of the most security conscious customer service processes around."[49] The article goes on to explain that powerful voice recognition technology is required for the process to be effective.

### 6.2 WHAT CAN CONSUMERS DO?

The world of identity is evolving and consumers need to be mindful. The main takeaway of this thesis should be that the current consumer perception of what can be used for identification purposes is also changing. This section of the paper offers suggestions on how to better protect PII. Looking now to the last research question, *what can consumers do to be more vigilant?*

Firstly, consider choosing fake answers to security questions. An answer that is not true will be that much harder for someone else to guess, since the data is not readily available. How can a fraudster compile a profile on to find out a potential victim's mother's maiden name, if a different name is used? [19] This is something that can be done to be more proactive in assuring that the layer of security between a hacker and PII is less penetrable. It might be wise for consumers to develop a fictional alias and create answers to common security questions that are not true but can be remembered via this alias. The lack of concreteness in the data is what makes this more secure.

Second, be wary of overexposing on social networks. Increase the privacy of all social and personal accounts. Make use of two-step authorizations where it is applicable. Although making profiles private on Facebook does not make data inaccessible, it does make it harder to access. Do not friend unknown people on Facebook. This may give a potential hacker instant access to personal data. Be careful what is share and don't use that same information later as a means of identification. If something is a well-known fact, do not use it as the answer for the security question. As discussed in previous sections, many common security questions contain everyday information that is shared on social media sites. While this ensures that the information is easy to remember, this also increases the probability of discovery. Understand that the information divulged on Facebook and Twitter can be found and does not disappear. All of this data is stored in a database and can be accessed. Be wary of this and remember that no system is 100% secure. Even security companies like RSA are not impervious to getting hacked. In one capacity, RSA provides secure means for employees to access employer networks remotely. "A number of governmental organizations, defense contractors, and corporations use RSA SecurID authentication tokens to allow employees to access sensitive data."[50] Despite security being the premise behind the company, they too were hacked. The point is that no entity is immune.

Third, be careful with "simple" accounts that work as access points to more important accounts. Overall consumer security is only as strong as the weakest link. Often, hackers gain access to less important accounts with "easier" passwords in order to gather information before hacking into financial accounts with more robust passwords. Because nearly anything done online now requires registration, accounts are often created in low security places with a default, easier password. This could be a "go-to" password used when the data is perceived as "not that sensitive". Although no financial data is available at this access point, there are other pieces of data such an email address, name, address, birthdate, which are often required for registration that can serve as the first step in amassing a victim profile. These non-financial accounts are typically less secure and a starting point for hackers who will perform large-scale hacks down the line.

Lastly, know which attributes of an identity are most vulnerable and push back when those are requested. Be inquisitive as to why a specific data element is required and why another, less intrusive method of identification won't suffice. Intrusive data is requested of consumers quite often. Earlier this year, a friend visited a local furniture store where she had made a purchase in the past. At the time of her original purchase, she opened a store credit card for a discount incentive. During this recent visit, she decided to purchase an additional piece of furniture and wanted to add the new purchase to the store card she had opened in the past. The only problem was, Cynthia no longer had the card in her possession. At this point, the store already has a tremendous amount of Cynthia's personally identifiable information. Minimally, they have on hand, her full address, complete name, birthdate and all the data surrounding her historical purchases. Most critically, the store has the credit card number associated with her account. When Cynthia was ready to make her new purchase, she asked the store representative if they could look up her account. Immediately, he responded, "Can I please have your social security number to perform the account lookup?" There are several things wrong with this picture, but noteworthy is how a sensitive piece of data is requested when a less sensitive piece may have sufficed. Why did this sales associate jump to one of the most intrusive data elements to lookup her account? Why couldn't he find her account details by her name and address and have her verify her identity with her driver's license photo ID? And most importantly, why did the system even have a search by social security number? This implies that employees of this store were constantly handling customer's social security numbers not just at the point of account creation, but any time another purchase was made.  Per the results discussed in section 5, employees were often the providers of this sensitive data that resulted in data breaches. This type of scenario is typical and part of our job as consumers is to push back.

## 6.3 What Are Companies Doing?

Although a consumer can be cognizant and cautious, it is inevitable in today's world that at least some personally identifiable data will reside in a company's database. Unless a switch is made to live completely on cash, consumers do rely on banks and other institutions on a regular basis.  But what are companies doing to increase security precautions and better protect data?

After sitting down for an interview with a former Security Consultant, Tom Striping, I quickly realized that the industry trend seems to be shifting away from trying to build an impenetrable system, towards architecting systems with the assumption that data will be stolen.  The focus then becomes risk mitigation and seamless recovery.  In theory this makes sense, plan for the worst and hope for the best, but as immutable forms of authentication are introduced, as discussed in the previous section, how exactly is risk mitigated?  Is there a way to recover from a data breach that results in a photocopy of a consumer's fingerprint?

Despite this trend, credit card companies still seem to be investing in prevention. In light of the recent data breaches at Target and Neiman Marcus, an article from March 2014 in Reuters stated that, "Visa Inc and MasterCard Inc said they had launched a cross-industry group to improve security for card transactions and press U.S. retailers and banks to meet a 2015 deadline to adopt technology that would make it safer to pay with plastic.” [51] This new group includes a gamete of financial institutions and “will initially focus on the adoption of 'EMV' chip technology.” [51] The EMV chip technology is a step in the right direction because the information is stored on computer chips rather than on traditional magnetic strips, making them harder to counterfeit. Credit cards currently carry all pertinent data on the strip in the form of magnetic data. With an EMV chip, a fraudster would require a key to access the encrypted data on the card. Attacks involving a skimmer, which was identified as a critical resource in identity theft related attacks, would no longer work on credit cards embedded with the EMV chip.

# 7. Closing Thoughts

2013 proved to be a year full of technological advancements and the harsh realization that these "advancements could make us even more vulnerable. Despite all of the security measures companies take, attackers find ways to penetrate defenses and access sensitive information." [52] Twitter was breached early in the year resulting in the exploit of emails, passwords and usernames of 250,000 users. Facebook was also hacked in June and "6 million email addresses and telephone numbers were taken." [52] Evernote suffered a massive data breach requiring them to "reset the passwords of all its 50 million users." When LivingSocial was breached, over "50 million people had their names, email addresses and date of birth exposed." [52] Unfortunately, this is but a sampling of the companies affected and the number seems to be growing.

As the world becomes more connected, the identity landscape is changing. Malefactors are more creative. Consumers are increasingly exposed. Data aggregators have made the job of stealing our identities easier by pulling data credentials together into one place. The only feasible answer to this growing problem is to study identity theft scenarios as a business process as a means of better understanding how theft is occurring. It is paramount to learn from the scenarios that have previously occurred in order to adapt thinking and best practices accordingly. This could mean changing the way certain data is viewed, or perhaps, using different credentials for identity validation. Consumers may also need to push back when the most intrusive data is immediately required for purposes of authentication. The ITAP has started creating this repository in order to deliver actionable knowledge to the community so that consumers are equipped with the information needed to make better choices. In the meantime, however, it is important to take into account how historically safe credentials may no longer be safe due to an increase in social media and the overall interconnectivity of the world. Like any good strategy, it is important to make calculated steps based on current, relevant data, and if necessary, change course and adapt. Identity theft is more rampant and it is time to stop and reevaluate what is "secure" and what is not given the current identity climate. Ultimately, the goal is to be one step ahead and not two steps behind.

# Reference list

[1] "Oxford English Dictionary online". Oxford University Press. September 2007. Archived from the original on 2012-07-08. Retrieved 27 September 2010.

[2] “Synthetic ID Theft.” *Cyber Space Times*. Accessed December 10, 2013. http://www.unc.edu/~dubal/idtheft/synthetic.htm.

[3] Hoofnagle, Chris Jay. *Identity Theft: Making the Known Unknowns Known*. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network. Accessed March 27, 2014. http://papers.ssrn.com/abstract=969441.

[4] “Data Breaches.” *Identity Theft Resource Center*. Accessed January 5, 2013. http://www.idtheftcenter.org/id-theft/data-breaches.html.

[5] Davis, Matt. “New DOJ Study Says 16.6 Million Cases of Identity Theft in U.S. Last Year.” *Identity Theft Resource Center*, December 18, 2013. http://www.idtheftcenter.org/id-theft/data-breaches.html.

[6] “Identity Theft and Identity Fraud.” Government. *The United States Department of Justice*, n.d. http://www.justice.gov/criminal/fraud/websites/idtheft.html.

[7] “Data Breaches and Data System Risks - Economics - AEI.” October 3, 2013. http://www.aei.org/article/economics/financial-services/data-breaches-and-data-system-risks/.

[8] “American Shredding | Types of Identity Theft |.” Accessed November 10 , 2013. http://americanshredding.com/american-shredding-types-of-identity-theft/.

[9] “What to Do If Your Child Is a Victim of Identity Theft.” *Real Simple*. Accessed March 27, 2014. http://www.realsimple.com/work-life/family/kids-parenting/child-identity-theft-00100000095315/index.html.

[10] “Identity Theft Protection - Avoid ID & Credit Fraud | LifeLock.” Accessed Jan 3, 2014. http://www.lifelock.com/nh/.

[11] “Medical ID Theft/Fraud Information.” Government. *Office of Inspector General*. Accessed October 1, 2013. http://oig.hhs.gov/fraud/medical-id- theft/index.asp.

[12] “The Next Data Theft Target: Your Medical Records.” Accessed September 10, 2013. https://www.yahoo.com/tech/the-next-data-theft-target-your-medical-records-77113382628.html?soc_src=mags.

[13] Engeler, Amy. “The Identity Theft You Haven’t Heard of...Yet.” *WebMD*. Accessed December 1, 2013. http://www.webmd.com/health-insurance/id-theft-you-havent-heard-yet.

[14] Rys, Richard. “The Impostor in the ER.” *Msnbc.com*. Accessed September 18, 2013. http://www.nbcnews.com/id/23392229/ns/health-health_care/t/impostor-er/.

[15] Ricker, Thomas. “Digital Medical Records by 2015?” *Engadget*. Accessed February 27, 2013. http://www.engadget.com/2005/07/05/digital-medical-records-by-2015/.

[16] “UK Police And Companies Will Have Access To Database Of All England’s Medical Records.” *Infowars*. Accessed February 10, 2014. http://www.infowars.com/uk-police-and-companies-will-have-access-to-database-of-all-englands-medical-records/.

[17] Ahlqvist, Toni; Bäck, A., Halonen, M., Heinonen, S (2008). "Social media road maps exploring the futures triggered by social media". *VTT Tiedotteita – Valtion Teknillinen Tutkimuskeskus* (2454): 13. Retrieved 9 December 2012.

[18] Lewis, Kent. “How Social Media Networks Facilitate Identity Theft and Fraud.” *Entrepreneurs’ Organization*, n.d. http://www.eonetwork.org/knowledgebase/specialfeatures/Pages/social-media-networks-facilitate-identity-theft-fraud.aspx.

[19] LMcpherson. “The 10 Most Common Password Security Questions.” Accessed December 27, 2013. http://stumbleforward.com/2012/08/20/the-10-most- common-password-security-questions/.

[20] “Stay Safe on Facebook: How to Manage Privacy Settings.” *Reader’s Digest*. Accessed February 26, 2014. http://www.rd.com/advice/be-a-savvy-facebook-user/.

[21] “The ABCs of Google Wallet and Apple’s Passbook.” *CIOL Bureau*, February 6, 2014. http://www.ciol.com/ciol/resource-center/208448/the-abcs-google-wallet-apples-passbook.

[22] “Google Wallet.” *Google*. Accessed March 1, 2014. http://www.google.com/wallet/.

[23] “What Is Secure Element.” *IGI Global*. Accessed December 9, 2013. http://www.igi-global.com/dictionary/secure-element/34892.

[24] “Google Wallet Is Not as Secure as It Should Be, Suggest Forensics Experts.” *Phone Arena*, December 13, 2011. http://www.phonearena.com/news/Google-Wallet-is-not-as-secure-as-it-should-be-suggest-forensics-experts_id24677.

[25] “Bitcoin vs. Coin: Which Will Have Most Success in 2014?” *The Next Web*. Accessed March 2, 2014. http://thenextweb.com/insider/2014/03/01/bitcoin-vs-coin-success-2014/.

[26] “Coin.” Accessed December 27, 2013. https://onlycoin.com.

[27] Rao, Leena. “PayPal Debuts Its Newest Hardware, Beacon, A Bluetooth LE Enabled Device For Hands-Free Check Ins And Payments.” *TechCrunch*. Accessed March 1, 2014. http://techcrunch.com/2013/09/09/paypal-debuts-its-newest-hardware-beacon-a-bluetooth-le-enabled-device-for-hands-free-check-ins-and-payments/.

[28] “PayPal.” *PayPal*, n.d. https://www.paypal.com/us/webapps/mpp/beacon.

[29] H, Jon. “What You Need To Know About PayPal Beacon.” *ChinaGeoPark*, November 22, 2013. http://www.chinageopark.com/what-you-need-to-know-about-paypal-beacon/.

[30] Levin, Josh (2008-01-30). "In What City Did You Honeymoon? And other monstrously stupid bank security questions". Slate.

[31] Honan, Mat. “How Apple and Amazon Security Flaws Led to My Epic Hacking | Gadget Lab | Wired.com.” *Gadget Lab*. Accessed February 27, 2014. http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/.

[32] "What is NFC?". NFC Forum. Retrieved 14 June 2011.

[33] Mimoso, Michael. “Black Hat 2012: On-Stage NFC Hack Highlights NFC Security Issues.” *SearchSecurity*, July 26, 2012. http://searchsecurity.techtarget.com/news/2240160292/Black-Hat-2012-On-stage-NFC-hack-highlights-NFC-security-issues.

[34] *Consumers and Mobile Financial Services 2013*. Federal Reserve, March 2013. http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201303.pdf.

[35] “Is It Safe To Bank On Public Wi-Fi? How Not To Get Hacked!” *Yahoo News*. Accessed March 1, 2014. http://news.yahoo.com/blogs/upgrade-your-life/banking-online-not-hacked-182159934.html.

[36] Bresiger, Gregory. “Identity Theft Exploding with Massive Data Breaches.” News. *New York Post*, February 23, 2014. http://nypost.com/2014/02/22/identity-crisis-exploding-with-massive-data-breaches/.

[37] Identity Theft - A Research Review, National Institute of Justice. July, 2007.

[38] Paul Harmon, (2007). Business Process Change: 2nd Ed, A Guide for Business Managers and BPM and Six Sigma Professionals. Morgan Kaufmann

[39] AWAREnes User Guide, AWARE Software, Inc., Austin Texas, 2014.

[40] Lobosco, Katie. "S&P Downgrades Target for Data Breach." *CNNMoney*. Accessed March 30, 2014. http://money.cnn.com/2014/03/28/news/companies/target-downgrade/index.html.

[41] "Voice Biometrics Are on the Rise for Authentication Purposes |." Accessed March 30, 2014. http://www.psshelp.com/voice-biometrics-move-to-consumer-devices/.

[42] 192, at 12:39:00 am ET. "Apple Explains How the iPhone's Fingerprint Sensor Keeps Your Info Secure." *Engadget*. Accessed March 26, 2014. http://www.engadget.com/2014/02/27/apple-touch-id-white-paper/.

[43] 17, Charlie Osborne for Between the Lines | September, and 2013-- 09:53 Gmt. "Apple iPhone Fingerprint Scanner Raises Security Worries." *ZDNet*. Accessed March 26, 2014. http://www.zdnet.com/apple-iphone-fingerprint-scanner-raises-security-worries-7000020767/.

[44] "How Secure Is Your iPhone 5S Fingerprint?" *CNN*. Accessed March 26, 2014. http://www.cnn.com/2013/09/12/tech/mobile/iphone-fingerprint-privacy/index.html.

[45] King, Rawlson. "Explainer: Retinal Scan Technology | BiometricUpdate.com," July 12, 2013. http://www.biometricupdate.com/201307/explainer-retinal-scan-technology.

[46] Schelmetic, Tracey. "Voice Print Technology Means Fast and Reliable Customer Authentication." *Workforce Optimization Solutions*, September 25, 2013. http://www.tmcnet.com/channels/workforce-optimization/articles/354277-voice-print-technology-means-fast-reliable-customer-authentication.htm.

[47] "Voice Authentication for Financial Services - ArmorVox$^{TM}$." Accessed March 26, 2014. http://www.armorvox.com/voice-authentication-financial-services/.

[48] "Opinion Piece : Reliable Voice Recognition for Authentication Is at Least a Decade Away." *SecurityPark*. Accessed March 30, 2014. http://www.securitypark.co.uk/opinion-piece-reliable-voice-recognition-for-authentication-is-at-least-a-decade-away/.

[49] Talk, BT Let's. "How Voice Recognition Is Keeping Vital Processes Secure." Accessed April 1, 2014. http://letstalk.globalservices.bt.com/en/2013/06/how-voice-recognition-is-keeping-vital-processes-secure/.

[50] 13, Tom Espiner | November, and 2011-- 12:00 Gmt. "RSA: Hack Was like 'a Spy Novel.'" *ZDNet*. Accessed March 30, 2014. http://www.zdnet.com/rsa-hack-was-like-a-spy-novel-3040094384/.

[51] "MasterCard, Visa Form Group to Push for Better Card Security." *Yahoo News*. Accessed March 8, 2014. http://news.yahoo.com/mastercard-visa-form-group-enhance-payment-security-160801064--sector.html.

[52] "Top Data Breaches in 2013." *Scribd*. Accessed March 30, 2014. http://www.scribd.com/doc/169662654/Top-Data-Breaches-in-2013.

[53] "Internet Users in the World." *Internet World Stats*, Accessed April 3, 2014. http://www.internetworldstats.com/stats.htm.