**The Report Committee for Misty Heaven Vasquez**
**Certifies that this is the approved version of the following report:**

# The Financial Crimes Management of Account Takeover Fraud

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

**Supervisor:**

Kathleen Suzanne Barber

Craig Blaha

# The Financial Crimes Management of Account Takeover Fraud

**by**

**Misty Heaven Vasquez**

**Report**

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 Identity Management and Security**

**The University of Texas at Austin**

**December 2017**

## Acknowledgements

I am indebted to so many for the encouragement and support throughout this journey. I would like to express my sincere gratitude to Dr. Suzanne Barber and Dr. Craig Blaha for their invaluable guidance through the process of researching and writing this report. To my colleagues, thank you for all your support along the way in my personal growth and development.

I am especially grateful to my parents for their selfless love and sacrifices they made to ensure that I had an excellent education. Thank you both for always giving me the strength and courage to pursue my goals, without whom I would never have enjoyed so many opportunities.

Finally, I owe a very special thank you to my loving husband and children for providing me with continuous and unfailing love, support, and understanding during my pursuit of this degree. This accomplishment would not have been possible without them.

# Abstract

## The Financial Crimes Management of Account Takeover Fraud

Misty Heaven Vasquez, M.S.I.M.S
The University of Texas at Austin, 2017

Supervisor: Kathleen Suzanne Barber

Account takeover can be a damaging and personally intrusive type of fraud occurring when an unauthorized individual obtains and uses another individual's personally identifiable (PII) information to gain unauthorized access to an existing account. Account takeover fraud continued to be a serious fraud threat in 2016 that affected millions of consumers resulting in billions in fraud losses. This research clearly defines account takeover fraud, investigates how account takeover incidents occur, describes the impact for both consumers and the financial industry, and offers mitigating tactics to combat and recover from account takeover incidents.

# Table of Contents

# List of Tables

# List of Figures

# List of Illustrations

## Overview of Account Takeover Fraud

The U.S National Institute of Standards and Technology (NIST) defines personally identifiable information (PII) as:

1. any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
2. any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (NIST, 2010, p. 13).

The United States government has developed many federal and state laws to protect the distribution and accessibility of PII because this information is so valuable and can result in severe repercussions for individuals if compromised. Compromised PII can be used to steal an individual's identity or money, also known as identity fraud. Identity fraud is a term used to describe when an unauthorized individual obtains and uses some portion of another individual's PII to commit fraud or deception for economic gain (Javelin Strategy & Research, 2017, p. 63).

Account takeover, also known as ATO, is a type of identity fraud that occurs when an unauthorized individual obtains and uses another individual's PII to gain unauthorized access to an existing account. Once an account takeover occurs, identity thieves can update the victim's personal information and proceed to gain access through the financial institution's online website, mobile app, or customer service representative channel.

## THREE PHASES OF ACCOUNT TAKEOVER INCIDENTS

Account takeover incidents occur in three phases: account takeover attempt, account takeover without money movement, and account takeover with money movement. An account takeover attempt occurs when an unauthorized individual attempts to access a victim's account without success. This situation is like a home burglar trying to open a door or window but has yet to enter the house. An account takeover without money movement occurs when an unauthorized individual successfully accesses a victim's account and may have updated personal information or security settings on the account, but has yet to conduct any type of money movement transactions. This situation is like a home burglar successfully entering an individual's home but has not yet stolen anything from the house. Account takeover with money movement occurs when an unauthorized individual successfully accesses a victim's account and has conducted at least one money movement transaction. This situation is like a home burglar successfully entering an individual's home and stealing items from the home.

A financial institution's overall goal should be to detect incidents within the account takeover attempt phase to avoid the account takeover incident from progressing any further. Mitigating tactics should continue to build at each phase of the event to help minimize the consumer impact and monetary losses to the financial institution. For example, mitigating tactics may consist of locking a customer's account, initiating security notifications to request the customer contact the financial institution, and updating accounts to prevent the withdrawal of funds. Financial institutions should also develop operational dashboards to measure the number of incidents:

- mitigated within the account takeover attempt phase.
- detected to include the fraud avoidance associated to the account takeover without money movement phase.
- detected to include the fraud loss associated to the account takeover with money movement phase.

An effective dashboard enables a financial institution to take both a broad look and a deep dive into data, evaluate the effectiveness of their tools and processes, and execute continuous improvements to detect activities associated with each phase.

## UNDERSTANDING THE THREAT

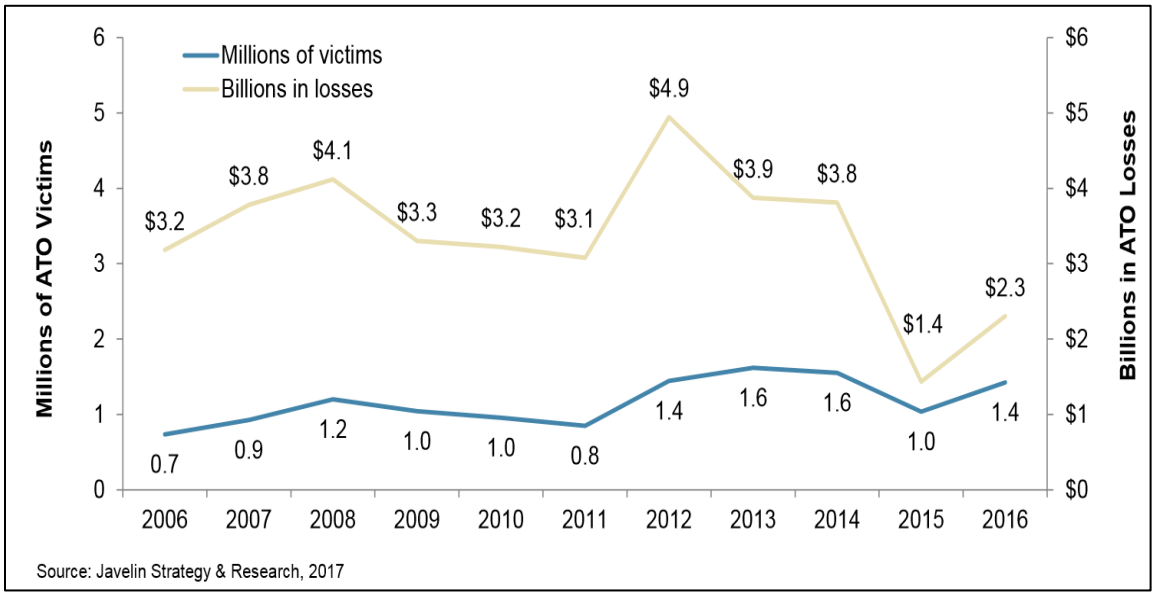
The *"Account Safety in Banking Scorecard"* study, released by Javelin Strategy & Research, proved that account takeover fraud continued to be a serious threat in 2016. According to Javelin, account takeover fraud affected 1.4 million consumers resulting in $2.3 billion in losses (Javelin Strategy & Research, 2017, p. 8). Losses increased from $1.4 billion to $2.3 billion, a 64% increase from 2015 to 2016 (see Illustration 1). The increased trend could be a result of the decrease in profitability of counterfeit card operations due to the financial industry's transition from magnetic stripe to a more secure chip enabled debit and credit cards. The transition from magnetic strip cards that stored static card information to chip enabled cards that generate a unique code for every transaction made it more difficult to counterfeit chip enabled cards.

Javelin's "*2017 Identity Fraud: Securing the Connected Life"* study found the top four types of accounts affected by account takeover incidents in 2016 consisted of checking or savings accounts, major credit card accounts, email accounts, and mobile phone

accounts (Javelin Strategy & Research, 2017, p. 6). Mobile phone account takeover incidents appeared to be an attractive target which nearly doubled from 7% to 12% in 2016 (see Illustration 2). Javelin also recognized an increase in cross-account takeover incidents in their "*Account Safety in Banking Scorecard"* study. Cross-account takeover incidents consist of having an external account, such as an email or mobile phone, taken over in addition to the financial institution account. In 2016, 18% of account takeover victims experienced a cross-account takeover incident resulting in a steady increase since 2014 (Javelin Strategy & Research, 2017, p. 9). Cross-account takeover incidents provide identity thieves the capability to intercept login credentials sent via email or text message.

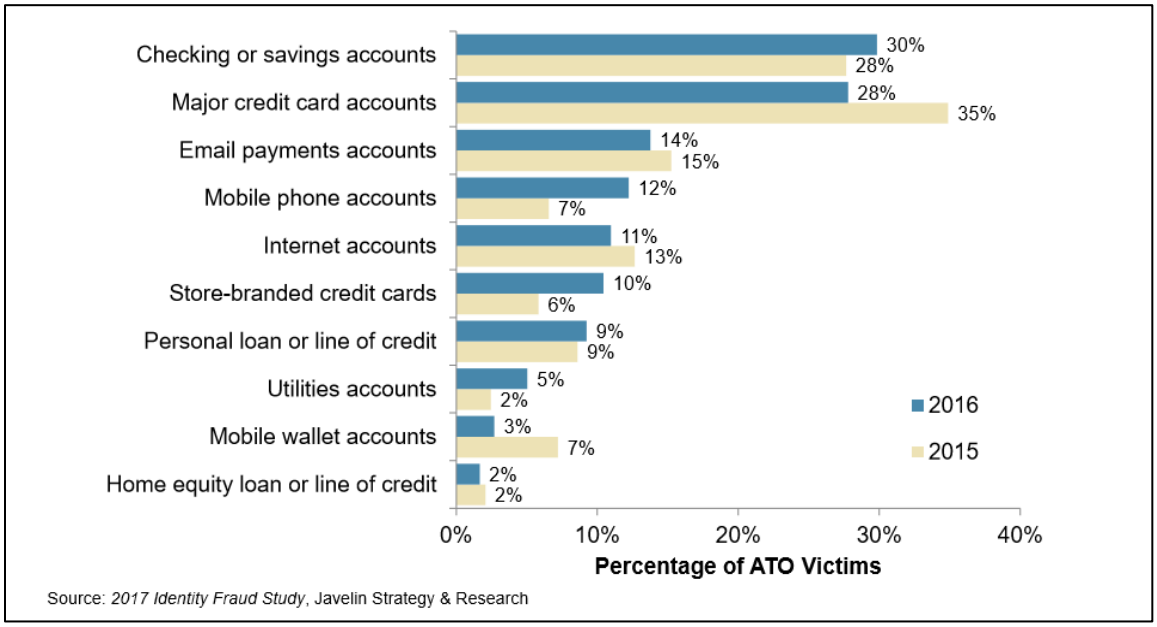
In addition, Javelin found that account takeover fraud continued to be a difficult type of fraud to resolve for both financial institutions and their customers in 2016 (Javelin Strategy & Research, 2017, p. 17 & 27). Javelin's research found that the average fraud amount increased from $1,424 to $1,984. The time to resolve account takeover incidents also increased over 40% from 14 hours to 20 hours for financial institutions due to the level of difficulty to confirm the activity as fraudulent. The increased level of difficulty is a result of financial institutions inadvertently contacting the identity thief first regarding the fraudulent activity due to the thief updating the victim's contact information as part of the account takeover incident. Account takeover victims also paid an average of $263 in out of pocket expenses per incident compared to the average of $48 per incident for other fraud types.

Illustration 1: Account Takeover Victims (Millions) and Losses (Billions)




Source: Javelin Strategy & Research, 2017, p.8

Illustration 2: Types of Accounts Taken Over 2015-2016




Source: Javelin Strategy & Research, 2017, p.26

## Anatomy of Account Takeover Attacks

Account takeover fraud is enabled by a variety of techniques including data breaches, social engineering, and victim's oversharing personal information on social network sites and the Internet. Data breaches continue to provide identity thieves access to exposed PII which can lead to account takeover fraud. Identity thieves are also known to use social engineering tactics to manipulate victims into releasing PII used to commit an account takeover. In addition to data breaches and social engineering attacks, the lack of consumer knowledge and education about the need to protect and how to protect their personal information on social network platforms will continue to fuel account takeover fraud.

### DATA BREACHES

A data breach is an incident in which an individual's PII is potentially at risk because of an exposure that occurred either electronically or in paper format. The exposed PII may consist of a wide range of information such as an individual's name plus a Social Security number, financial account information, medical information, or login credentials. Within minutes identity thieves can use the exposed PII to commit account takeover fraud. For example, consumers who were victims of the Yahoo data breach could be at risk of account takeover fraud if their Yahoo login credentials are the same credentials used to access their accounts at their financial institution. Consumers who have listed their Yahoo email account as a recovery option for obtaining or resetting their login credentials may also be at risk. Data breaches are increasingly common and will threaten an increasing number of consumers over time. See Table 1 for a list of some of the largest data breaches

that occurred in the 21st century.

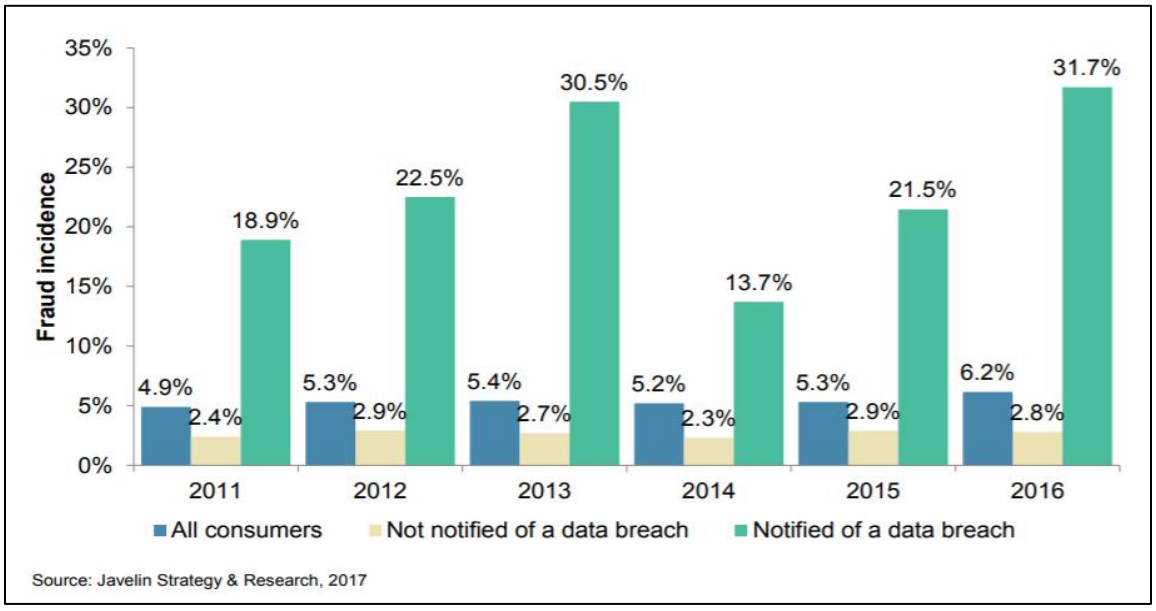
Table 1: Large Data Breaches of the 21st Century

| Company: | Date: | User Accounts Impacted: |
|---|---|---|
| Yahoo | 2013-2014 | 3 billion |
| Adult Friend Finder | 2016 | 412 million |
| MySpace | 2016 | 360 million |
| Equifax | 2017 | 145 million |
| LinkedIn | 2012 | 117 million |
| Sony's PlayStation Network | 2011 | 102 million |
| Anthem | 2015 | 80 million |
| National Archive and Records Administration | 2008 | 76 million |

Source: Palermo & Wagenseil, 2017

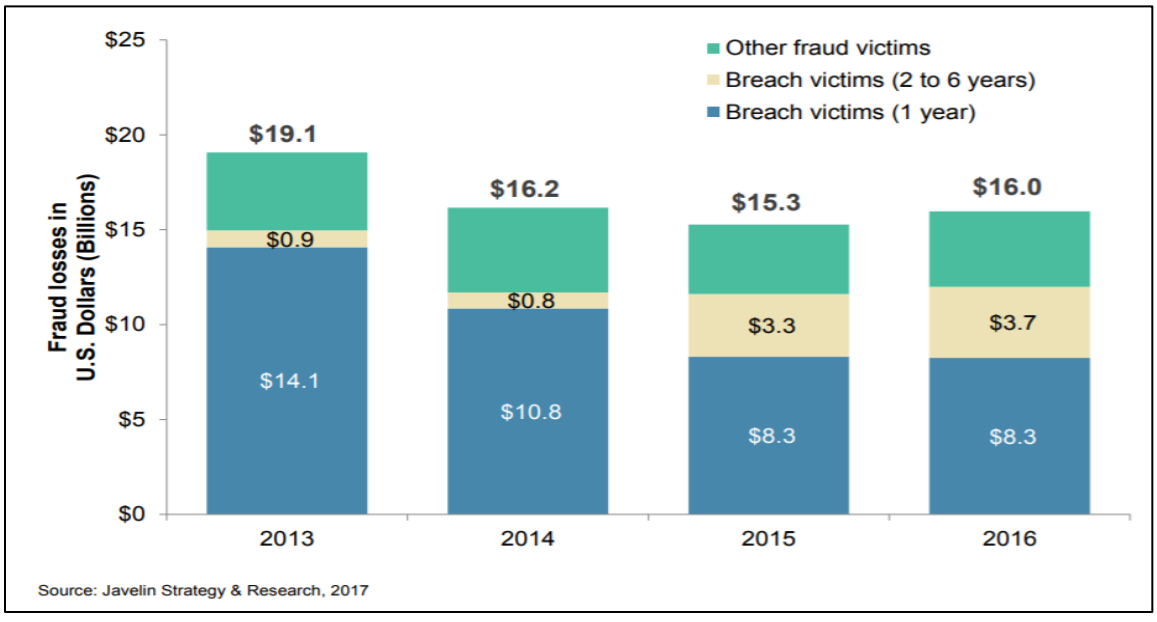
Javelin found that at least 1 in 3 of notified breach victims experienced fraud within the same year in their "*2017 Identity Fraud: Securing the Connected Life*" study (Javelin Strategy & Research, 2017, p. 7). Notified breach victims who experienced fraud continued to increase from 2014 to 2016, resulting in the highest rate of 31.7% (see Illustration 3). Javelin's *"Data Breach Fraud Impact Report: Going Undercover and Recovering Data"* study found that $8.3 billion dollars of fraud losses originated from victims previously affected by a data breach in the previous 12 months in 2016. An additional $3.7 billion dollars originated from victims affected by a data breach in the previous two to six years (see Illustration 4).

Illustration 3: Fraud Incidence by Breach Notifications Status, 2011-2016




Source: Javelin Strategy & Research, 2017, p. 12

Illustration 4: Fraud Losses Attributable to Breaches




Source: Javelin Strategy & Research, 2017, p. 9

Data breaches can be perpetrated by a malicious insider (insider theft or physical theft), a malicious outsider (hacking, skimming, or phishing), or in error (improper disposal, accidental loss, or exposure of PII). Gemalto's data analysis on security breaches identified 1,792 breaches occurred resulting in 1.4 billion data records were either lost, stolen, or compromised in 2016 (Gemalto, 2017, p. 2). The number of records exposed resulted in an 86% increase from 2015 even though 936 of the breaches had an unknown number of records compromised. Data breaches continued to prove that no industry is immune from an attack by malicious outsiders (See Illustration 5). Malicious outsiders accounted for more than two thirds of identified data breaches in 2016. Identity theft was the most common type of attack and accounted for 58.6% of the total breaches and 28.4%, nearly 400 million, of the records stolen.

Illustration 5: Number of Breach Incidents by Industry

| INDUSTRY | 2013 | 2014 | 2015 | 2016 |
|---|---|---|---|---|
| Healthcare | 345 | 448 | 445 | 493 |
| Government | 194 | 290 | 297 | 269 |
| Other Industries | 262 | 275 | 321 | 229 |
| Retail | 98 | 195 | 239 | 215 |
| Financial Services | 165 | 212 | 276 | 214 |
| Technology | 112 | 139 | 122 | 189 |
| Education | 35 | 174 | 165 | 157 |
| Hospitality | - | - | 1 | 26 |

Source: BREACHLEVELINDEX.COM

Source: Gemalto, 2017, p. 11

The Identity Theft Resource Center (ITRC) found that Social Security numbers were exposed in 52% of data breach incidents, an 8% increase over 2015, and four data breaches alone were responsible for exposing over 120 million Social Security numbers in 2016 (Identity Theft Resource Center, 2017). This can be problematic for any institution that continues to use Social Security numbers as a form of authentication since consumers are unable to easily change their Social Security number once these numbers have been exposed. According to Javelin's 2014 Identity Fraud study found that 80% of the top 25 banks and 96% of the top credit card issuers allowed their customers to authenticate using their Social Security number (Javelin Strategy & Research, 2014).

### SOCIAL ENGINEERING

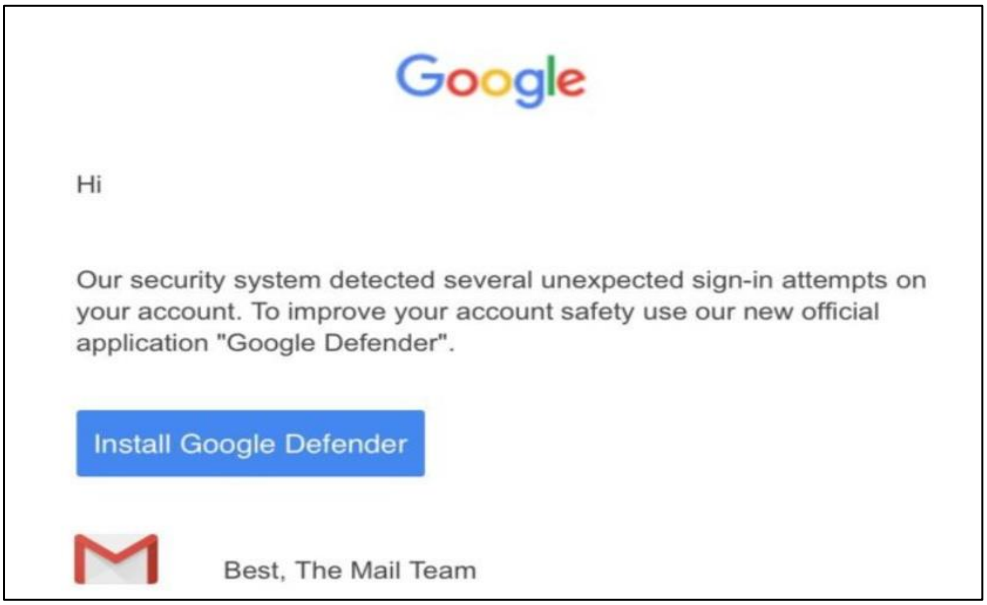
Social engineering consists of tactics used to gain access to systems, data, or money by manipulating human psychology. Some common social engineering tactics are known as phishing, SMSishing or vishing. Phishing, SMSishing, and vishing are social engineering scams that come in the form of emails, mobile text messages, or phone calls. Another form of social engineering known as angler phishing targets consumers on social media.

Phishing is a type of social engineering tactic which consists of fraudulent emails constructed to steal sensitive information by disguising as a trustworthy entity. Phishing emails may include files or links that will infect computers with malware once opened by the recipient. The malware enables cybercriminals to remotely access the infected computers to obtain sensitive information. Phishing emails may also consist of a message

that incorporates a sense of urgency or threat to manipulate individuals into releasing login credentials or PII such as names, dates of birth, and Social Security numbers.

For example, in 2017 a Russian hacking group, known as Fancy Bear or Pawn Storm, sent phishing emails pretending to be from Google informing email users of unexpected sign-in attempts into their email account (Kan, 2017). The phishing email manipulated Google users into installing a security application to further protect their email account (see Figure 1). Once installed the phishing victims unknowingly authorized the hacking group to view and manage their email by circumventing Google's 2-step verification process. Google's 2-step verification consists of providing a password and a temporary security code received through a SMS message when accessing an email account. This can be problematic for financial institutions, or any other organization, that send temporary security codes or passwords and security alerts through email to their customers.

Figure 1: Fancy Bear Phishing Email Example

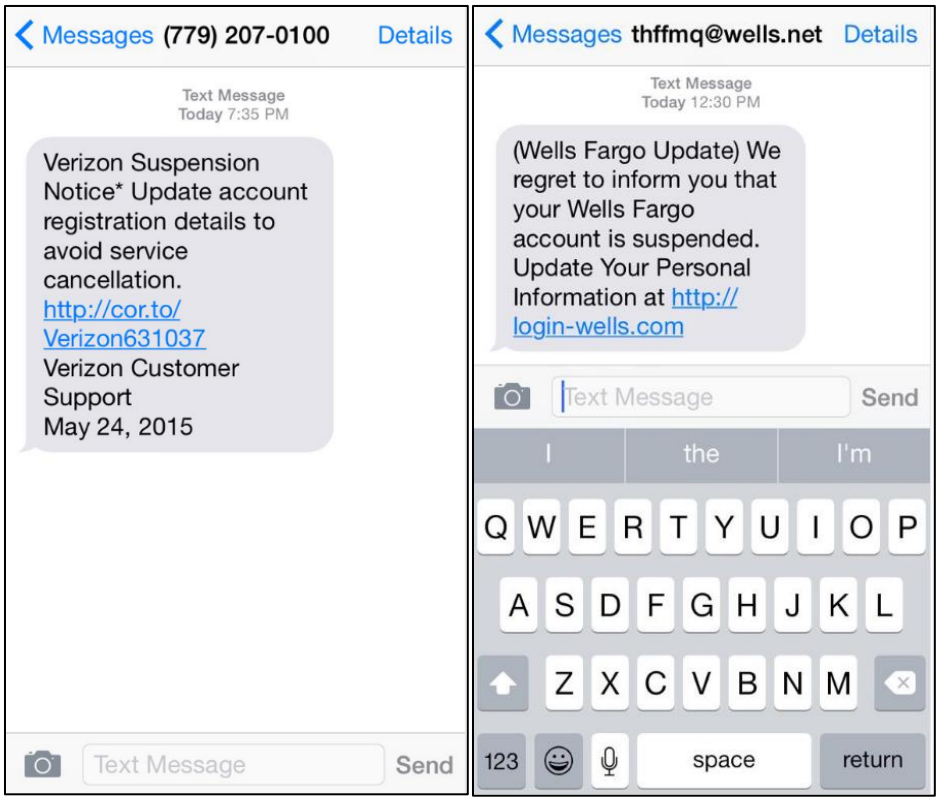



Source: Kan, 2017

SMSishing is a type of social engineering tactic which consists of mobile phone text messages constructed to steal sensitive information. Identity thieves send mobile text messages to manipulate individuals into selecting links to malicious websites, downloading mobile malware, or calling a fraudulent phone number. Like phishing emails, SMS messages consist of a message that incorporates a sense of urgency such as “account suspension” or “fraudulent activity detected” to manipulate individuals into releasing account information, login credentials, and other personal information (see Figure 2). Identity thieves can take over a mobile phone account by redirecting one-time security codes and security alert SMS messages to a device in their possession once victims release PII or account information. Identity thieves can also walk into mobile phone store pretending to be a customer who is requesting to upgrade their mobile phone. Once

upgraded, the identity thief walks out with a new phone device assigned to the true customer's mobile phone number. With this tactic, the true customer immediately stops receiving phone calls and SMS messages due to the newly activated phone device that is in the possession of the identity thief. Other tactics may consist of contacting the mobile network provider pretending to be the true customer who is needing to report a lost phone and needs assistance activating a new phone or requesting to forward all calls and text messages to a different number.

Figure 2: SMSishing Examples




Source: Weekly Summary 5/4-5/17, n.d.

Another form of social engineering may occur through impersonation to build a false sense of trust in the form of a phone call, also known as vishing. For example, an identity thief may manipulate an individual into believing they are a representative from their financial institution or some type of legal authority, such as the Internal Revenue Service (IRS), to obtain PII. The United States Government consistently warns consumers about identity thieves that pose as the IRS to manipulate individuals into releasing personal information or money (Internal Revenue Service, 2013). These calls typically involve an immediate actionable request that consists of providing PII and bank account details.

Vishing attacks may also consist of exploiting a financial institution's call center to manipulate customer service representatives into believing that the caller is the true customer. Call centers can be the weakest link for authentication since customer service representatives focus on delivering excellent customer service. Identity thieves may pose as a forgetful customer or a customer in distress to gain access to a victim's account. For example, an identity thief may convince a customer service representative to expedite a wire request or a credit card to an alternate address due to theft event occurring while traveling. At this point, the identity thief provides enough of the victim's PII to manipulate the customer service representative into believing that the caller is the true customer.

Identity thieves also use social media as an attack vector by creating fraudulent social media accounts to social engineer for PII, also known as angler phishing. Angler phishing continues to emerge as a significant threat as social media accounts increased 100% from the third to fourth quarter of 2016 (Proofpoint, 2017, p. 9). The creation of fraudulent social media accounts often coincides with highly publicized events, holidays,

major brands or corporations, or popular topics that are trending. For example, an individual may post on their own social media account about their frustrations with not being able to access their financial accounts (see Figure 3). Unknowingly, the individual may receive a response from an identity thief who has created a fraudulent social media account that directs the individual to a fraudulent website that looks exactly like their financial institution. The fraudulent website prompts the individual to provide personal information such as login and account information.

Figure 3: Angler Phishing Example


Source: Roberts, 2016

## SOCIAL NETWORKS AND THE INTERNET

Social networks sites have the greatest potential for abuse since the intent of these sites is to provide "friends" with deeper insights into people's lives, families and friends, hobbies, and interests. In addition to the shared information, social network sites also

collect personal information such as full name, date of birth, place of residence, relationship status, education, employment, and any other affiliations. Social network sites use this personal information to increase social networking opportunities with other online users with similar backgrounds and interests. However, identity thieves can use PII obtained from these sites and the Internet to commit account takeover fraud by passing knowledge based authentication (KBA) questions. KBA questions consist of referencing previously selected and answered security questions during a recovery flow for user id and password credentials. KBA may also consist of questions based on an individual's past credit or public records and provides multiple-choice answers.

For example, I observed that without having to sign into a Pinterest account, I could access the personal information about users that posted reviews using the Pinterest Save button. Pinterest users that post reviews often have their username link to another social media account such as Facebook or Google+. One individual's username hyperlinked to their Google+ page which made their personal information publicly available because their privacy settings were set to public instead of private. The individual's Google+ page provided the following personal information: current place of residence, current and previous employment history dating back ten years, information about the individual's family (3 children, plus 6 additional children acquired through marriage, and 9 grandchildren), pet information, and education information to include dates of attendance (see Figure 4). In addition, the individual's Instagram account could be easily located and confirmed through posts and pictures that were accessible from public views on both the Google+ page and Instagram account (see Figure 5). The Instagram account provided

additional personal information such as photos of the individual and their spouse on a 9-day vacation at Hollywood Studios in December of 2016.

Figure 4: Google+ Page Example

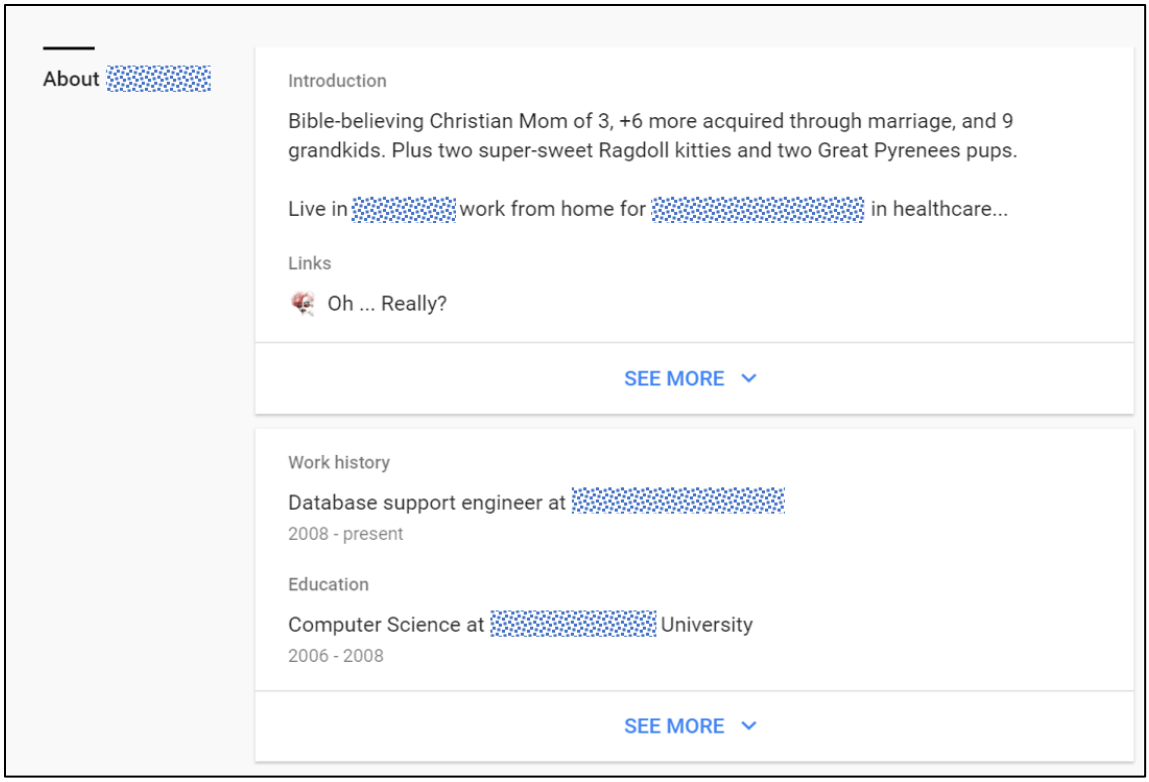
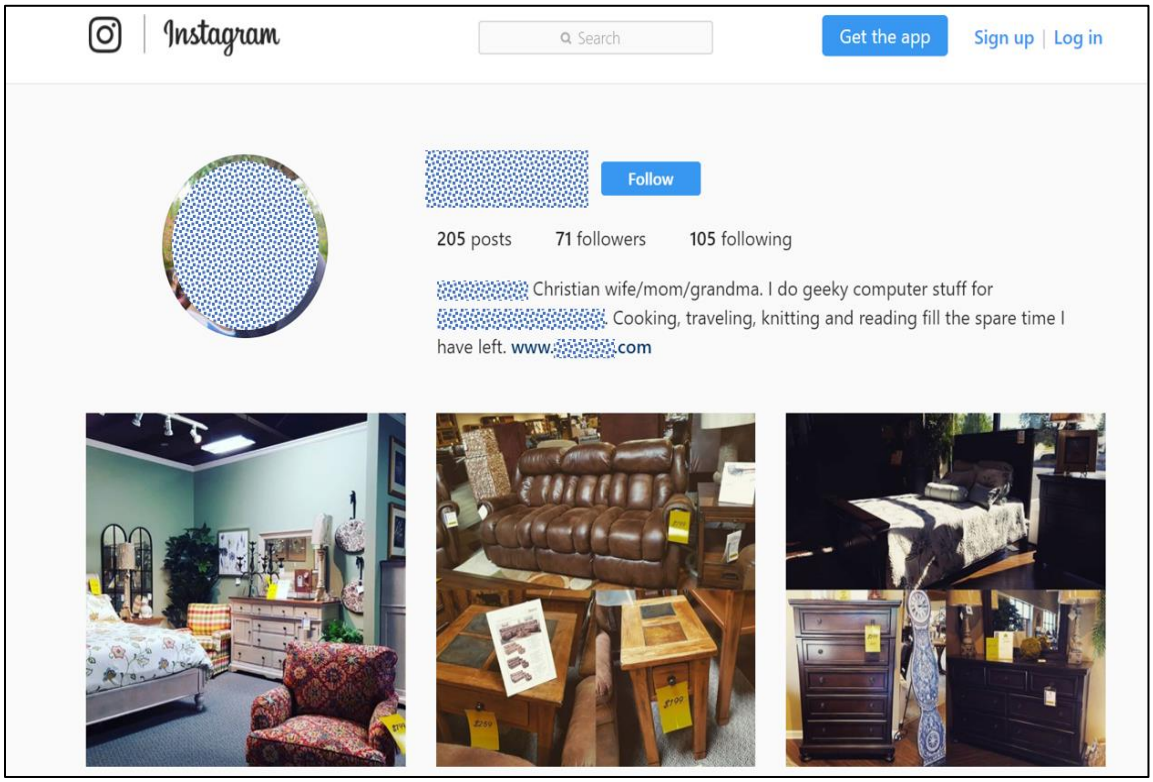


Figure 5: Instagram Page Example

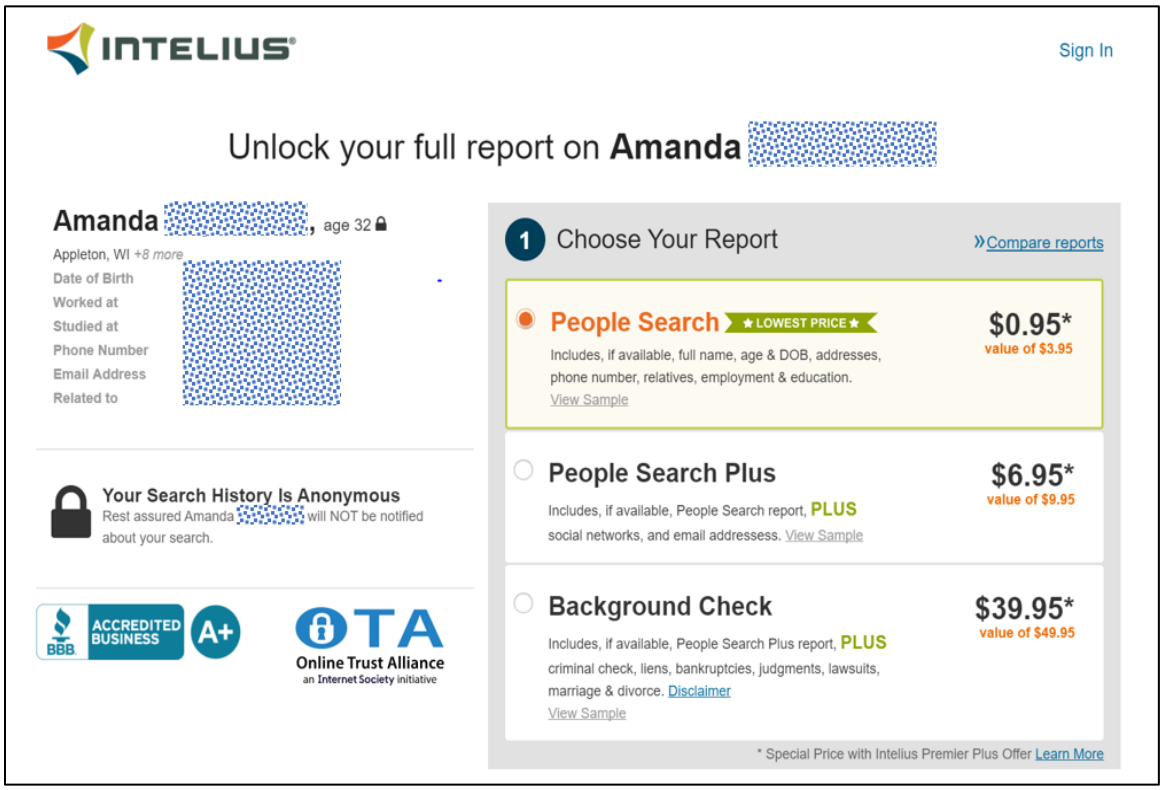



Identity thieves may utilize the acquired PII to obtain additional information from information-gathering websites such as Spokeo or Intelius. Information-gathering websites utilize web crawlers to aggregate data about people from billions of public records. The aggregate data may include information such as income, religion, relatives, current and former places of residences, employment history, estimated income, and estimated credit. These websites advertise the ease with which people searches can be initiated using an individual's name, address, phone number, or email address.

For example, another individual's Pinterest username used their first and last name and included a picture of the individual. A Google search conducted on the individual's name provided matches to LinkedIn, Instagram, and Intelius pages. The LinkedIn page

provided additional personal information such as current and previous places of residences, employment, and education history. The Intelius site provided additional personal information that included the individual's age range, different states of residences, current employment information, and information on immediate family members. The Intelius site advertised that additional personal information was available for a fee that ranged from $0.95 to $39.95 (see Figure 6).

Figure 6: Intelius Site Example




Personal information may also be accessible from non-social network sites such as Wikipedia. Wikipedia pages can provide identity thieves the PII needed to proceed with account takeover or any other type of identity fraud. Examples of PII obtained from

Wikipedia pages may include an individual's: full name, date and place of birth, education history, spouse's name and date of birth, children's names and dates of births, family relationships to include parents and siblings' full names, employment information, and military service information. This type of information enables an identity thief to easily deceive a customer service representative to gain access to an individual's account.

In summary, this section provides an overview of how identity thieves obtain unauthorized access to PII to commit account takeover fraud. The success rate of these cybercrimes continued to make headlines across multiple industries impacting millions of Americans in 2017. For example, Equifax, one of the three largest aggregators of personal and financial data, announced that malicious outsiders gained unauthorized access to the PII of 145 million consumers in 2017 (Cybersecurity Incident & Important Consumer Information, 2017). The compromised data consisted of names, Social Security numbers, birth dates, addresses, driver's license numbers, and credit card numbers. Less than a month after the Equifax announcement, Yahoo announced a revision to the number of impacted accounts reported for the data breach that occurred in August of 2013 (Larson, 2017). The revised number increased from 1 billion to 3 billion accounts impacted, which is every single customer account that existed at that time, exposing names, email addresses, and passwords as part of the data breach. The magnitude of these breaches should be of concern to both consumers and financial institutions since it creates the perfect toolkit to execute account takeover fraud. This volume of exposure and the value of the information to fraudsters leads to the need to research mitigating tactics to combat and recover from account takeover incidents.

## Mitigating and Resolving Account Takeover Fraud

Account takeover mitigation and resolution tactics are important to financial institutions since victims expect financial institutions to protect their accounts regardless of how an identity thief obtained their PII. For example, CBS News reported a story about an account takeover victim who believed identity thieves used his PII that was stolen as part of the Office of Personnel Management data breach in 2015 (News, 2017). Even though he knew he had been a victim of a data breach external to his financial institution, the account takeover victim still felt violated by his bank for not preventing the account takeover incident. Since consumers are repeatedly exposed to social engineering tactics and are victims to multiple data breaches, it is difficult for a consumer or a financial institution to identify exactly how a victim's PII was obtained. In addition, predicting the unauthorized use of exposed PII is even more difficult since it can have value for many years. Financial institutions can minimize both the consumer and business impact by implementing a business model that focuses on preventing, detecting, and resolving account takeover incidents. However, combating account takeover needs to be a shared responsibility between the financial institution and their customers. The best mitigation tactic to combat account takeover is for both the financial institution and their customers to be vigilant.

### PREVENTING ACCOUNT TAKEOVER INCIDENTS

Financial institutions can implement multiple strategies to help combat account takeover incidents. Strategies may consist of automatically enabling the strongest security settings on all customer contact channels to proactively provide education versus relying

on their customers to seek out information on their security centers. Educating customers on the risks of oversharing personal information on social media along with the risks of utilizing poor security settings can help mitigate account takeover fraud. In addition, financial institutions need to anticipate the risk that external data breaches can bring since exposed PII can have value for many years, if not the lifetime of the victim.

**Automatically Enable the Strongest Security Settings**

Financial institutions should automatically enable new customer accounts using the strongest security settings to help mitigate account takeover incidents. This may seem like a simple strategy, but defaults are powerful since the majority of consumers never change the default settings on most online websites, computers, and smart phone devices. Consumers tend to just trust that the developer or designer has enabled the best and most secure settings available for them. The default settings may consist of security methods such as multifactor authentication. Multifactor authentication creates a layered defense since it requires a combination of two or more credentials as part of the authentication process. Credentials may consist of a combination of what the customer has (one-time security code), plus something a customer knows (a password), and something the customer is (a biometric credential). In addition, financial institutions should offer multiple biometric capabilities such as fingerprint, face recognition, or voice print and multiple ways to utilize a one-time security code to accommodate their customer needs during the authentication process.

Financial institutions should also develop a customer centric strategy to enroll existing customers that are capable of successfully completing these stronger security

methods, and to help minimize the amount of frustration and cost to implement stronger security for customers that may not be capable or prepared.

One customer focused strategy may include identifying customers who have already established or utilized some type of multifactor authentication method. For example, customers that have enabled a biometric capability, such as fingerprint verification, to access the financial institution's mobile app or have utilized a temporary one-time security code to recover login credentials for the online website. A second strategy may consist of conducting data analysis to identify customers that have the capability to provide the credentials needed to pass multifactor authentication based on available information within their customer profile. For example, if a customer has a mobile phone on file then he or she should be capable of receiving a text message with a one-time security code. Financial institutions can, in conjunction with a clear communication strategy and outreach program, automatically enroll these identified customers into multifactor authentication methods when accessing their accounts online, through a mobile app, or when speaking to a customer service representative.

**Educate Customers to be Vigilant**

Consumers will typically seek fraud prevention or resolution guidance once they become concerned with or have become a victim of identity theft or account takeover fraud. Therefore, financial institutions should proactively communicate to educate customers on the need to be vigilant in protecting their account, along with how to be vigilant. Creating a connection to the audience by using easy to understand terms and real-life scenarios to

articulate what the risk is, why it is a risk, and how to avoid the risk will help the message be more effective.

Communication should consist of educating their customers on the latest social engineering tactics and should be followed by prevention tips. For example, educating customers about the dangers and consequences of using social media since these sites encourage users to provide and share personal information. Articulating how the Internet can provide a false sense of anonymity which may lead users to overshare their personal information to an invisible and unknown audience. Providing simple reminders to avoid oversharing personal information online and to never post personal information that an identity thief could use to gain access to an email and/or financial accounts can help mitigate account takeover incidents. Providing guidance to enable and customize privacy settings can also help control who has access to the personal information customers choose to share online. In addition, advising their customers to also be selective when they respond to friend or follow requests since the Internet makes it easy for people to misrepresent their identities.

Financial institutions should humanize their communication by articulating how identity thieves can continually leverage exposed PII that is extremely difficult to update. For example, reminding customers that updating account information and login credentials is easy, but obtaining a new Social Security number is extremely difficult to obtain. In addition, compromised PII can sell for less than a dollar in the underground of the Internet, also known as the Dark Web.

Using prevention tips to communicate with customers about security can also help enable customers to be vigilant. One prevention tip may consist of enabling the strongest security settings available on smart devices, email, and financial accounts. A second prevention tip may consist of providing guidance on how to be creative when establishing a strong password along with the importance of using a separate password on each account to help minimize the risk of an identity thief having the password to multiple accounts if compromised. It is always helpful to include an example on how to create a stronger password such as using the first letter of each word from a verse of a favorite song and substituting numbers or special characters for some letters. Another prevention tip may consist of educating customers on how to identify suspicious emails by providing common red flags and some examples of phishing emails that customers have received. Some financial institutions inform their customers to look for red flags that consist of typos, grammatical errors, and to be cautious of any links or attachments requesting personal information. In addition, the financial institution's website should also include examples of phishing emails that their customers have received pretending to be from the financial institution along with an email address that customers can forward suspicious emails to for investigation.

**Allow Customers to Customize Account Alerts**

Financial institutions should provide customers the capability to easily customize account alerts that accommodate their own financial habits. These capabilities will help reduce false-positive results and maintain the level of customer participation needed to quickly review and respond to unauthorized activity. Customers should also have the

capability to easily customize their notification preferences with options to receive account alerts through email, text message, or push notifications. Customizable alerts may consist of receiving notifications for:

- An account balance that is above or below a predetermined amount.
- A withdrawal or deposit to an account.
- An ATM withdrawal or debit card transaction that exceeds a predetermined amount.
- Credit card transaction activity.

**Be Proactive on External Data Breaches**

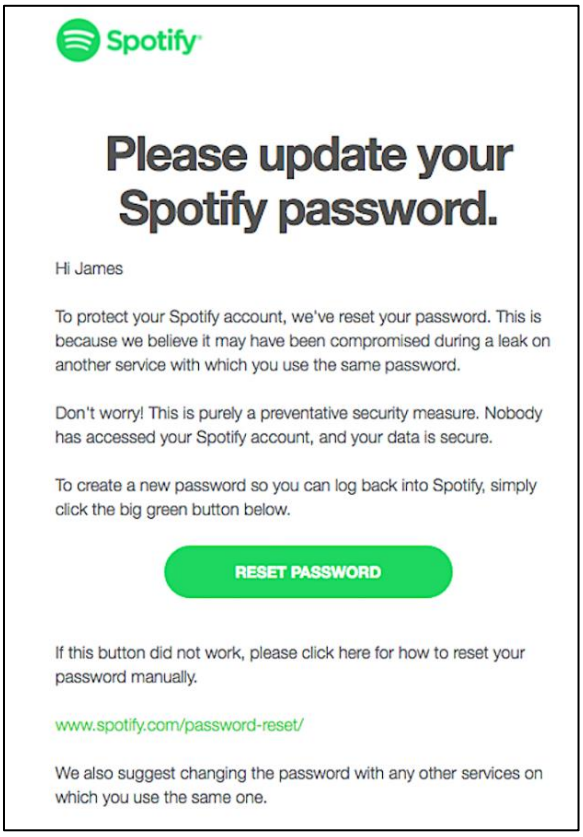
Account takeover incidents can occur due to the reuse of the same usernames and passwords across multiple websites and services. When one of those third-party websites or services becomes a victim of a data breach, financial institutions should anticipate that identity thieves can use the exposed PII to commit account takeover fraud. Financial institutions should proactively review sites for leaked user credentials that identity thieves can use to access their customers' accounts. Once identified, controls should be implemented to prohibit the use of any known passwords that are commonly used and any compromised passwords that have been identified in previous data breaches as recommended by NIST (NIST, 2017, p. 14).

Financial institutions should also implement controls to monitor for credential stuffing attacks which is becoming a large source of account takeover fraud. Credential stuffing consists of using scripted software to rapidly test compromised usernames and passwords to identify credential reuse across multiple websites. Shape Network observed

that the testing of stolen credentials makes up more than 90% of login traffic on some of the largest websites and mobile applications in 2016 (Shape Security, 2017, p. 2). In addition, the success rate was as high as 2% for credential stuffing attacks.

Financial institutions can also require their impacted customers to update their login credentials to help prevent account takeover incidents. As an example, Spotify, a music streaming service, proactively sent an email to some customers informing that an automatic password reset occurred to protect their account (see Figure 7). The email further explained the password reset was due to the risk that their current password may have been compromised during a data breach with another service that the same password is used (Price, 2016).

Figure 7: Spotify Email Example




Source: Price, 2016

**Reduce the Chances of Customers being Phished**

Financial institutions should strive to have a consistent look and feel on customer communication to help reduce the chances of their customers falling victim to a phishing attack. Consistency helps customers identify red flags typically associated to phishing emails. For example, always including a personalized greeting that includes the customer's first and last name versus a generic greeting of "Dear Customer" and a concise subject line that states exactly what the email is about. Communication that is in the form of an outbound phone call or email should never request for customers to provide any personal

or account information. In addition, reminding customers that the financial institution will never request this type of sensitive information in an outbound phone call or email. Customer communication should also direct customers to visit the financial institution's website to link to any specialized webpages versus including any attachments or links.

Helping customers identify red flags within phishing attacks can only help stop some attacks. Therefore, financial institutions should also monitor the web for unauthorized uses of their logo or to see if their name is associated with fraudulently registered domains. Proactive monitoring can enable financial institutions to shut down an identified fraudulent site prior to the launch of an impending phishing campaign. In addition, the implementation of a Domain-based Message Authentication, Reporting and Conformance (DMARC) policy can also help reduce phishing attacks against customers. DMARC is an email-validation system designed to detect and block fraudulent emails that appear to come from a financial institution's domain. DMARC enables financial institutions to have email providers either quarantine (move to the Spam folder) or prevent the delivery of fraudulent emails. As a final mitigation tactic, financial institutions should also provide customers and noncustomers the capability to report received phishing attacks to a dedicated email address such as abuse@domainname.com or phish@domainname.com. Enabling customers to report phishing attacks provides financial institutions the opportunity to conduct cyber threat analysis on the reported phishing emails.

## DETECTING AND RESPONDING TO ACCOUNT TAKEOVER INCIDENTS

Financial institutions will not have the capability or capacity to prevent every account takeover incident therefore rapid detection of account takeover incidents is critical. The implementation of fraud detection systems and processes to detect new and existing types of fraud may consist of techniques that are automated or require a manual review. For example, data analytics enables financial institutions to approach fraud differently by implementing a proactive fraud monitoring program that detects anomalies. The capability to identify fraud quickly enables financial institutions to send security and fraud notifications to their customers. The combination of these approaches combined can help mitigate the monetary impact for both the financial institution and the account takeover victim.

### Implement Analytical Technologies and Strategies

Financial institutions should implement capabilities to continually monitor customer behavioral patterns to detect, in real time, transaction patterns consistent with fraudulent activity. Using real-time data analytics enables financial institutions to leverage customer data to gain an understanding of fraudulent activities to identify trends, derive patterns, and locate anomalies in data. Some identifying key factors may consist of:

- how often a customer typically accesses their account from a mobile device, online website, or customer service channel.
- the average time it takes a customer to type in their login credentials.
- the geographic locations that a customer typically accesses their accounts from.

- understanding the average length and number of calls a customer may make in a specified timeframe.

Data analytics can help monitor these scenarios to identify account takeover incidents. For example, understanding the average length and number of calls a customer may make enables a financial institution to develop strategies to identify potential social engineering attempts that may be occurring against their customer service representatives. Some additional strategies may include identifying whether an IP address that is inconsistent with the customer's behavior or location tries to access the customer account, or whether multiple IP addresses from different cities try accessing a customer's account within a brief time gap. Data analysis also enhances a financial institution's ability to review and monitor multiple contact channels and banking platforms to detect cross-channel anomalies consistent with account takeover fraud. Financial institutions can also link previous fraud events between people, events, locations, and times to become more effective in identifying new fraud trends and patterns.

**Default on Security and Fraud Notifications**

Financial institutions should immediately notify customers of any suspicious activity detected and of any updates to a customer's account information to help mitigate any fraudulent activity that may be occurring. Security and fraud notifications can consist of two types of responsive alerts. One type of responsive alert consists of the financial institution holding a transaction until receiving a response from the customer. A second type of responsive alert consists of the financial institution allowing a transaction to process

followed by notifying the customer. Once notified, the customer will review and respond indicating if the processed transaction is authorized or unauthorized.

Security and fraud notifications could consist of notifying customers of login events from suspicious devices, locations, or suspicious in-account activity. In-account activity consists of money movement transactions such as a request to expedite a debit or credit card to alternate address or multiple requests to move bank account funds externally. Notifications should alert customers of any updates to contact information such as address, phone number, and email addresses. Financial institutions should send these types of security notifications to both the previously listed contact information and the new contact information on the customer's profile. Security notifications should also consist of notifying customers of any changes to security settings to include the enabling or disabling of authentication methods or requests to recover login credentials.

Financial institutions should default to providing the customer with security and fraud notifications versus relying on customers to enable them on their own. Customers should also have the capability to receive security and fraud notifications in many different ways such as a push notification within the financial institution's mobile app, a text message, an email, or an automated outbound phone call to the primary and secondary phone numbers on the customer's profile. Notifications should provide enough information regarding the detected activity to enable customers to easily review and determine whether the activity is authorized. The financial institution should also include clear instructions about how the customer should respond, enabling customers to respond easily and quickly to the detected activity.

## Resolving Account Takeover Incidents

The customer experience involving the resolution of account takeover incidents is crucial since it can be the key difference between the incident being a minor inconvenience or major disruptive event for victims. A positive account takeover resolution experience can help retain existing customers and strengthen customer loyalty. Financial institutions should provide their customers multiple channels to report fraudulent activity to help minimize customer frustration. These channels may consist of reporting fraudulent activity using the financial institution's website, mobile app, by contacting a customer service representative, or in person at a branch. Prompting customers to provide as much information as possible when utilizing the financial institution's website or mobile app will help mitigate any additional fraudulent activity.

### Assign a Dedicated Resolution Specialist

Financial institutions should strive to provide a consistent customer service experience by assigning a dedicated point of contact that specializes in assisting with the resolution process from beginning to end. A single point of contact can help minimize miscommunication between different representatives and notify the victim as early as possible if any additional information is necessary will result in a streamlined and expedited resolution process. A dedicated resolution specialist can also assist with guiding the victim through the tools and resources provided by the financial institution to recover from the account takeover incident. Since account takeover incidents can be complex and time consuming, measuring dedicated resolution specialists on customer satisfaction rates versus number of accounts serviced will allow for a better customer experience.

**Expedite the Reimbursement of Funds and Cards**

Financial institutions should expedite the reimbursement of funds and cards to help minimize the monetary impact for victims of account takeover. Immediately applying a temporary provisional credit to the victim's account will help maintain, or even gain, a customer's confidence in their financial institution. The provisional credit should include enough funds to cover any expected transactions, such as reoccurring payments, to avoid the victim from incurring any external non-sufficient fund fees. In addition, providing replacement cards within two to three business days and offering next day card replacement when necessary can minimize the unintentional impact of preventing the victim from utilizing impacted debit or credit cards.

**Require Stronger Security Settings**

Financial institutions should require victims of account takeover to enable the strongest security settings available to help mitigate the risk of repeat account takeover incidents. The dedicated resolution specialist responsibilities should consist of educating customers on the need for stronger security, assisting with enabling the stronger security settings, and articulating the experience going forward when using these stronger settings. Responsibilities should also consist of advising customers to immediately review and update all passwords, security settings, and credential recovery options external to the financial institution. Establishing stronger security settings with email and mobile phone providers will help mitigate account takeover incidents from occurring through intercepted email or SMS messages.

**Provide Identity Theft Resolution Guidance**

Financial institutions should provide an identity theft resolution toolkit that guides their customers through recommended actions that can help identify and resolve any additional identity fraud that may be external to the reported account takeover incident. The dedicated resolution specialist should assist with highlighting the importance of the recommended actions listed within the provided identity theft resolution toolkit. The toolkit should be accessible to customers through multiple channels such as the financial institution's website, mobile app, email, or paper. Some best practices consist of providing an interactive capability that will enable customers to mark recommended action items complete, identify specific action items as high priority, enable reminders, and the capability to capture any notes related to each recommended action item.

One recommendation should consist of advising the account takeover victim to request a free copy of their credit report from each of the major credit reporting agencies or by visiting AnnualCreditReport.com. The AnnualCreditReport.com website is a single site that provides consumers the ability to obtain a free credit report from the 3 major credit reporting agencies. Once the customer attains the credit report, the account takeover victim can review their credit reports thoroughly to identify and report any unauthorized inquires or accounts that may be external to the account takeover incident. A second recommendation should consist of advising the account takeover victim to place an initial fraud alert on their credit report that is valid for 90 days to help mitigate any additional identity fraud from occurring. An initial fraud alert notifies potential creditors or lenders that the consumer has concerns about identity theft and must take reasonable steps to verify

identity prior to extending a line of credit. When adding an initial fraud alert with any of the three major credit reporting agencies, the first agency contacted will notify the remaining two reporting agencies of the need to add an initial fraud alert on the consumer's credit report.

A third recommendation should consist of advising the account takeover victim to complete an Identity Theft Report with the Federal Trade Commission (FTC). The Identity Theft Report serves as official documentation and evidence of the identity theft event since the FTC is a federal law enforcement agency (Gressin, 2017). An identity theft report helps consumers dispute unauthorized activity by proving that their identity was stolen. The Fair Credit Reporting Act (FCRA) requires credit reporting agencies to inform appropriate creditors of the identity theft event and remove all fraudulent information and accounts from the consumer's credit report. In addition, the Fair Debt Collection Practices Act (FDCPA) prohibits creditors from submitting fraudulent debts to debt collectors. The Identity Theft Report also enables consumers to place an extended fraud alert or security freeze on their credit file for free which will notify potential creditors or lenders that the customer is a victim of identity theft. An extended fraud alert is valid for seven years and requires creditors to contact the consumer by telephone to verify requests for credit. A security freeze prevents creditors from accessing the consumer's credit file unless the consumer provides permission. The consumer will utilize an identification number that will temporarily lift the security freeze allowing access to their credit file. The security freeze remains on the credit file until the consumer decides to remove it.

A fourth recommendation should consist of advising the account takeover victim to enroll in an identity theft protection service as such as a credit monitoring or an identity monitoring service as described by the FTC (Federal Trade Commission, 2016). Credit monitoring services alert consumers of updates identified on their credit report. Updates may consist of a creditor conducting a credit check, the establishment of a new line of credit, or updates to personal information such as name, address, or phone number. These alerts help consumers quickly identify unauthorized activity related to their credit report, so actions may be taken to mitigate an identity theft event. An identity monitoring service will scan the Internet, such as public records and websites, to identify and detect a consumer's PII in other places that would not show up on their credit report. In addition to monitoring, identity theft protection services can also provide helpful resolution tools and help reduce out of pocket expenses.

A fifth recommendation should consist of advising the account takeover victim to protect all other external accounts and services by enabling the strongest security options available. Updating all accounts to have a unique and complex password will help minimize the risk of an identity thief having the password to multiple accounts if one of these accounts is compromised. Updating the security settings on mobile and email accounts is also critical since security alerts, one-time security codes, and recovery options for login credentials are capable of being received through these channels.

# Conclusion and Future Work

## Research Summary

This research articulated how account takeover fraud is a damaging and personally intrusive type of fraud. The first section defined what account takeover fraud is and the distinct phases of an account takeover incident. This section also described how account takeover fraud continued to be a serious fraud threat impacting millions of consumers and resulting in billions in fraud losses. The second section investigated how account takeover fraud can occur due to numerous data breaches across multiple industries, sophisticated social engineering schemes, and the oversharing of PII on social network sites and the Internet. The third section recommended a three-step approach that financial institutions can use to combat account takeover fraud and help their customers recover from account takeover incidents in the form of a prevent, detect, and resolve business model.

Throughout this research I identified that financial institutions should find opportunities to collaborate with other industries that understand the importance of security and share the same commitment in the fight against cybercrimes. For example, the four largest mobile carriers in the United States (AT&T, Verizon, T-Mobile, and Sprint) announced that they are collaborating to improve the security of mobile authentication (Knight, 2017). This type of collaboration will help mitigate risks related to identity thieves intercepting one-time security codes and security alerts delivered via SMS messages. Google also introduced an anti-phishing feature for their Gmail app for Android and Apple devices that informs users of suspicious links within Gmail messages (G Suite Updates, 2017). This type of enhancement will help prevent consumers from harmful phishing

attacks designed to steal PII. Collaborating across multiple industries will prove to be invaluable as identity thieves continuously seek out vulnerabilities in financial institutions and their customers.

## FUTURE WORK

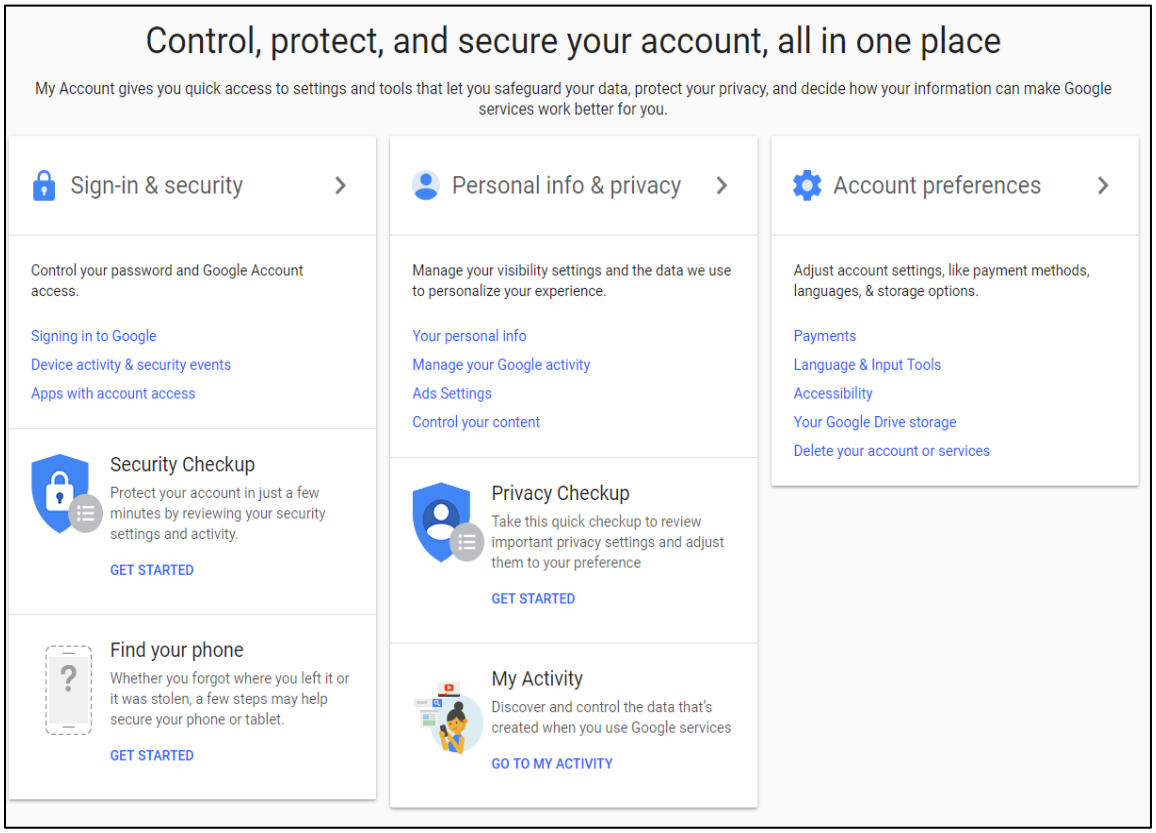
Financial institutions should anticipate that account takeover incidents will occur and should focus on implementing a frictionless resolution process for their customers. One question not examined here is what determines a best in class customer experience. This question offers the opportunity to explore best practices both within and outside of the financial industry. For example, insurance companies consistently focus on improving customer satisfaction associated with the filing of a property claim. With unforeseeable natural disasters, this process is critical since it can be a determining factor in customer loyalty when someone has just experienced some type of loss.

A second research opportunity is to explore strategies to strengthen the processes associated with both the issuing and the recovery of credentials. These strategies are critical to mitigate account takeover fraud since a financial institution's authentication processes are only as strong as the credential recovery processes. This research opportunity should also include strategies to strengthen the authentication associated with the customer service representative channel to help minimize the effect of social engineering tactics against customer service representatives.

A final research opportunity is to explore strategies to develop a user-friendly security center that presents available security tools and explains the benefits these tools provide. This is another opportunity to explore best practices not only within the financial industry

but outside the financial industry. For example, Google has developed a security center that enables their users to quickly access security settings and tools to protect their information and privacy (see Figure 8).

Figure 8: Google's Security Page Example



# References


*Cybersecurity Incident & Important Consumer Information*. (2017, September). Retrieved from Equifax: https://www.equifaxsecurity2017.com/

Federal Trade Commission. (2016, March). *Identity Theft Protection Services*. Retrieved from Consumer Information: https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services

G Suite Updates. (2017, August 10). *Anti-phishing security checks in the Gmail app for iOS*. Retrieved from G Suite Updates: https://gsuiteupdates.googleblog.com/2017/08/anti-phishing-security-checks-in-gmail.html

Gemalto. (2017). *Breach Level Index Report 2016.* Retrieved from http://breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf

Gressin, S. (2017, April 27). *Most ID theft victims don't need a police report*. Retrieved from Consumer Information: https://www.consumer.ftc.gov/blog/2017/04/most-id-theft-victims-dont-need-police-report

Identity Theft Resource Center. (2017, January 19). *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout*. Retrieved from Identity Theft Resource Center: http://www.idtheftcenter.org/2016databreaches.html

Internal Revenue Service. (2013, October 31). *IRS Warns of Pervasive Telephone Scam*. Retrieved from Internal Revenue Service: https://www.irs.gov/newsroom/irs-warns-of-pervasive-telephone-scam

Javelin Strategy & Research. (2014, February 5). *A New Identity Fraud Victim Every Two Seconds in 2013 According to Latest Javelin Strategy & Research Study*. Retrieved from Javelin Strategy: https://www.javelinstrategy.com/press-release/new-identity-fraud-victim-every-two-seconds-2013-according-latest-javelin-strategy

Javelin Strategy & Research. (2017). *2017 Data Breach Fraud Impact Report: Going Undercover and Recovering Data.*

Javelin Strategy & Research. (2017). *2017 Identity Fraud: Securing the Connected Life.*

Javelin Strategy & Research. (2017). *Account Safety in Banking Scorecard.*

Kan, M. (2017, April 25). *Russian hackers use OAuth, fake Google apps to phish users*. Retrieved from PC World: http://www.pcworld.com/article/3192484/security/russian-hackers-use-oauth-fake-google-apps-to-phish-users.html

Knight, S. (2017, September 8). *AT&T, Sprint, T-Mobile and Verizon join forces to develop secure two-factor system*. Retrieved from TechSpot: https://www.techspot.com/news/70918-att-sprint-t-mobile-verizon-join-forces-develop.html

Larson, S. (2017, October 4). *Every single Yahoo account was hacked - 3 billion in all*. Retrieved from CNN:

http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html
News, C. (2017, 6 February). *How con artists are changing tactics to steal identities*. Retrieved from CBS News: http://www.cbsnews.com/news/combating-the-rise-in-identity-theft/
NIST. (2010). *Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).* Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf
NIST. (2017). *Special Publication 800-63B, Digital Identity Guidelines Authentication and Lifecycle Management.* Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
Palermo, E., & Wagenseil, P. (2017, October 17). *The Worst Data Breaches of All Time*. Retrieved from Tom's Guide: https://www.tomsguide.com/us/pictures-story/872-worst-data-breaches.html
Price, R. (2016, September 1). *Spotify is making users change their passwords because other companies keep getting hacked*. Retrieved from Business Insider: http://www.businessinsider.com/spotify-users-password-reset-not-hacked-other-companies-data-breaches-reuse-account-logins-2016-9
Proofpoint. (2017). *Q4 2016 & Year in Review Threat Summary.* Retrieved from Proofpoint: https://www.proofpoint.com/sites/default/files/proofpoint_q4_threat_report-final.pdf
Roberts, J. J. (2016, November). *Meet the Latest Scary Form of Social Media Fraud*. Retrieved from Fortune: http://fortune.com/2016/11/11/social-media-cyber-scam/
Shape Security. (2017). *2017 Credential Spill Report.* Retrieved from http://info.shapesecurity.com/rs/935-ZAM-778/images/Shape-2017-Credential-Spill-Report.pdf
*Weekly Summary 5/4-5/17*. (n.d.). Retrieved from SMSishing & Vishing News: https://numbercop.tumblr.com/post/119761088780/weekly-summary-54-517

# Vita

Misty Heaven Vasquez was born in Corpus Christi, Texas. After graduating from Business Careers High School, San Antonio, Texas in 1998, she attended the University of the Incarnate Word in San Antonio, Texas. She received the degree of Bachelor of Business Administration with a discipline in Information Systems from the University of the Incarnate Word in December 2002. She entered the graduate program at the University of the Incarnate Word in August 2004 and received the degree of Master of Business Administration in May 2007. She was awarded the professional credential of Certified Fraud Examiner from the Association of Certified Fraud Examiners (ACFE), the world's largest anti-fraud organization, in December 2012. In January 2016, she entered the Master of Science in Identity Management and Security degree program offered by the School of Information at the University of Texas at Austin.

Permanent email: mistyvasquez@utexas.edu

This report was typed by the author.