CREDIT CARD FRAUD AND SOCIAL ENGINEERING: MITIGATION OF IDENTITY THEFT RELATED LOSSES REQUIRES MORE THAN TECHNOLOGY

by

Glenn A. Hall

A Capstone Project Submitted to the Faculty of

Utica College

December 2012

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Economic Crime Management

ABSTRACT

Credit card fraud is a billion dollar a year industry (Nilson, 2011). Financial institutions invest heavily in detection and prevention technology in an effort to mitigate their losses due to fraud. Bank technology spending is estimated to grow approximately 30 percent to $7.2 billion by 2015 in anti-fraud technology for mobile banking alone (Computerworld, 2012). According to the Federal Trade Commission, the total number of complaints submitted to the Consumer Sentinel database in 2005 totaled 686,683, an increase of 21 percent from 2003 (Identity Theft Data, 2005). Identity theft complaints represented 255,565, or 37 percent of the total complaints, and the most common type of identity theft was credit card fraud. In an effort to stem the tide of identity theft related fraud losses, the credit card industry have traditionally taken the approach of investing more money and resources into enhancing their authentication technology. However, technology alone has not, and will not, effectively address the problem. The millions of dollars and thousands of man-hours invested in the development of new authentication technology is undermined by the financial institutions' front-line employees and the credit card banking customers themselves due to the cunning and, often times impressive, social engineering and technical subterfuge tactics perpetrated by the fraudsters.

Acknowledgements

The author wishes to thank Raymond Philo and Sue Ross for their support, insight, and willingness to help.

TABLE OF CONTENTS

LIST OF ILLUSTRATIVE MATERIALS

Introduction

The evolving target population

Consumer confidence in financial institutions ability to provide safe, secure, and convenient credit services has become a key driver in determining direction and investment in technology and resources. It used to be that interest rates and acceptance were amongst the most important considerations for consumers when choosing their credit card company. Then, driven by the expanding economy and the competition of new issuers, credit card companies developed rewards programs, affiliations, and other incentives that soon became very popular features for consumers as well. Consumers were suddenly faced with numerous and creative options from which to choose for their credit card products. It was no longer about owning one or two credit cards with wide acceptance and lower interest rates. Instead, credit card ownership became a matter of style, statement of one's status in society, and a means of immediate gratification without regard to longer term consequences. Credit card companies soon recognized the target rich environment that had developed and the tremendous growth opportunities it presented to them. Credit card companies realized that if they could capture younger college students early in their credit lifecycle, they could develop a special long term relationship with the young consumer and earn a loyalty that would develop into a longer term and more profitable relationship when that college consumer matured into a successful professional. Beginning in the 1980's and even still today, college campuses were and are flooded with credit card application campaigns. Credit card companies set up elaborate and enticing solicitation booths at sporting and concert events with "free" gifts, send pre-approved application mailers directly to the students, and conduct telephone solicitation campaigns in an attempt to gain market share of this desirable young consumer demographic. The U.S. Public Interest research Group's student

debt program director , Christine Lindstrom, cited a 2008 survey by the U.S. Public Interest Research Group which found that 80 percent of students said they received direct mail from credit card companies and 22 percent received approximately four phone calls a month from credit card companies (CNN Money, 2008). Of course, this is not to suggest that college students are the only demographic population targeted for solicitation by the credit card companies. Rather, they are just one example population used to demonstrate the environment which helped set the stage for increased risk of identity theft, identity fraud, and social engineering.

Identity Theft and Identity Fraud

In general terms, and for the purposes of this paper, identity theft and identity fraud are typically used interchangeably and at times incorrectly by the media and even the Government but indeed have different meanings that need to be clearly distinguished and understood. According to the Federal Trade Commission, Identity Theft occurs when someone uses your personally identifiable information, like your name, social security number, or credit card number, without your permission, to commit fraud or other crimes (Federal Trade Commission, 2004). This interpretation is not entirely accurate. Identity theft is when someone's personally identifiable information is taken by another individual without explicit permission. Personally identifiable information (PII) includes items such as social security number, bank or card account numbers, date of birth, PINs, calling card numbers, name, and address. Criminals can obtain personally identifiable information in several ways:

- **Dumpster diving.** Rummaging through a person's trash for financial statements, pre-approved credit card applications, utility bills, documents with person's social security number.

- **Shoulder surfing.** Overhearing someone provide their personally identifiable information over the phone or looking over their shoulder while they provide information or at an ATM when they input their PIN.
- **Skimming.** Attaching a data storage device to an ATM or retail point of sale checkout terminal that reads and stores the credit card information and/or PIN as the card is swiped.
- **Mail theft.** Stealing pre-approved credit card applications, financial statements, utility bills, tax statements, etc from mailboxes
- **Phishing.** Fraudulent emails that appear to be from legitimate sources are sent to unsuspecting victims requesting they provide sensitive information or click on links taking them to fraudulent websites.
- **Vishing.** Phishing over the telephone. Unsuspecting victims are contacted via telephone and asked to provide sensitive information. Often, voice over IP (VoIP) is leveraged to complete the ruse by manipulating the caller ID information that consumers have come to trust.
- **Technical subterfuge.** Malicious software (Malware) is surreptitiously downloaded onto the victim's device. The malware captures sensitive information, passwords, user id's, keystrokes, etc. and then transmits them to the perpetrator.

On the other hand, Identity Fraud occurs when the stolen personally identifiable information is misused for nefarious and illicit purposes or financial gain. Criminals use the stolen PII to both open new accounts (new account fraud) and take-over existing financial accounts (account takeover). Identity fraud can occur numerous ways: unauthorized transfer of funds, unauthorized

payments, and unauthorized purchases to name but a few. Millions of people every year fall victim to identity theft in one form or another. According to the Federal Trade Commission's 2006 Identity Theft Survey Report, approximately 8.3 million U.S. adults over the age of 18 were victims of some form of identity theft in 2005 (Federal Trade Commission, 2006).

Table 1: Prevalence of ID Theft in 2005, by Category of Misuse

	Percent of Adult Population[1]	**Number of Persons (millions)[2]**
New Accounts & Other Fraud	0.8 % (0.5 % - 1.2%)	1.8 (1.2 – 2.8)
Misuse of Existing Non-Credit Card Account or Account Number	1.5 % (1.1% - 2.1%)	3.3 (2.4 – 4.6)
Misuse of Existing Credit Card or Credit Card Number	1.4 % (1.0 % - 2.1%)	3.2 (2.1 – 4.6)
Total Victims in 2005	3.7 % (3.0% - 4.6%)	8.3 (6.6 – 10.3)

[1] Figures in parentheses are 95% confidence intervals.

[2] Based on U.S. population age 18 and over of 222.94 million as of July 1, 2005. (http://www.census.gov/popest/states/asrh/tables/SC-EST2005-01Res.xls (visited August 15, 2006)).

The act of Identity Theft has been around for decades. In the late 1500s, impersonating royalty or someone of wealth and power was en-vogue. In 1578, the King of Portugal was killed while on his second expedition to Morocco; many Portuguese people refused to accept his death and called King Sebastian "the hidden king" believing that he would soon someday return to rule. To seize upon the opportunity to instantly become wealthy and powerful, four individuals attempted to impersonate the deceased king and in doing so committed identity theft. Two were uneducated and of peasant origin and were quickly captured. Two other impersonators were more educated and did better at impersonating King Sebastian. However, in the end, both were

eventually captured and executed. Then there was Frank Abignale whose adventures in identity theft and check fraud were glamorized in the 2002 Stephen Spielberg film "Catch Me If You Can" starring Leonard DiCaprio as Frank Abignale. Mr. Abignale began his Identity Theft exploits in the 1960s at the age of 16 and proceeded to impersonate an airline pilot, a doctor, a lawyer, and an instructor all before the age of 23 (Identity Theft Manifesto, 2009). However, as it relates more to the credit card industry, it was in the early 1980's that the term "Identity Theft" became popular and began to be utilized by the financial industry and federal and local law enforcement agencies. In the early 1980's, personally identifiable information (PII) was used to submit fraudulent applications for credit cards. Nigerian nationals were especially talented at perpetrating application fraud and quickly became enemy number one in the eyes of the financial industry and law enforcement. Nigerian tactics included obtaining employment positions with commercial cleaning services that were contracted by businesses and other institutions with Human Resource departments. Commercial cleaning services typically work at night after business hours when only the physical security guard services are on premises. This provided for uninterrupted access to the employee files that were typically stored in filing cabinets in the Human Resources departments. Back in the early 1980's, computerized filing systems were not yet utilized by companies. They would make copies of the files and place them back in the cabinets so as not to alert anyone that a crime has happened and allow their identity theft exploit to continue for a longer run time. Employee files contained everything they needed to complete an application for a credit card. They would simply place the victim's current address as the previous address and provide another address under their control as the current address. Nigerians were well educated in the ways of American banking and credit bureau reporting and new that the credit bureaus would validate the victim's address even though it was listed on the

application as a previous address. Additionally, there are no birth records maintained in Nigeria so when they come to America to perpetrate their identity theft exploits they can easily assume a new identity for purposes of obtaining employment with a commercial cleaning company. Furthermore, when they did get arrested, they were typically just sent back to Nigeria verses imprisoned in America for any long period of time. This was beneficial in that they could simply return to America with new identity documents. The risk of getting caught was exceedingly outweighed by the potential rewards from just a few successful fraudulent applications. They were further incented due to the extremely depressed economy and poor quality of life back in Nigeria.

Nigerians were not only one of the founding fathers of present day Identity Theft; they have remained very active and continue to evolve with the times. In May of 2012, Simi Valley, CA detectives completed a six-week investigation into a Nigerian fraud ring and arrested four Nigerians for possession of stolen credit information and credit card fraud. They were responsible for over $2 million in credit losses (Ventura County News, 2012).

Definition of 18 U.S.C. §1028

Identity theft continued to grow and evolve throughout the 1980's and 1990's to become a serious issue for both consumers and financial institutions. Consumers were becoming victimized, sustaining significant financial and mental hardship, and losing trust in the financial services industry. Much of the blame was being placed on the financial services industry due to their inability to detect and prevent identity theft related fraud. Both consumers and the financial services industry began to pressure their local representatives and law enforcement to something about it. At this time, Identity Theft was not, in and of itself, an actual crime. Law enforcement

had to rely upon a few federal statutes to protect the information necessary to commit identity theft and upon general anti-fraud provisions to punish and redress any injury. It wasn't until incidents and losses attributed to identity theft dramatically increased in the 1990's did Congress finally decided to take direct action. Federal law 18 U.S.C. §1028 - The Identity Theft and Assumption Deterrence Act of 1998 criminalized the act of Identity theft namely:

> Knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law (Federal Trade Commission, 2000).

The Act was the first law to criminalize identity theft at the federal level. In addition, the law expands the definition of identity theft to include the misuse of any identifying information linked to an individual, as a violation of federal or state law. The definition covers misuse of existing as well as creation of new accounts.

Identity and Privacy Protection Related Legislation

In addition to The Identity Theft and Assumption Deterrence Act, state and federal governments have enacted laws protecting personal privacy and information:

- **The Identity Theft Penalty Enhancement Act.** Signed into law on July 15th, 2004, the Act adds two years to the prison sentence of criminals convicted of crimes involving stolen credit card information and other personal information. N additional five years are added to the sentence of those who used the stolen information for purposes of terrorism.

- **The Children's Online Privacy Protection Act (COPPA).** Enacted in 1998, gives parents control of their child's information that is collected over the Internet. Parents also control how the collected information will be used. The Act requires the commercial websites to notify the children prior to obtaining the information and to post their privacy policy.
- **Notification of Risk to Personal Data Act.** Introduce in 2006, this Act requires businesses or government to notify individuals that their personal information (e.g., social security number, driver's license number, credit card or bank account number) has been compromised due to a database breach. The Act carries with it fines of $5000.00 per violation or up to $25,000.00 per day while the violation persists.
- **California SB 168, Identity Theft Prevention Bill.** Enacted in 2004, protects individuals by prohibiting businesses from posting or disseminating social security numbers and requires insurers and health care providers to apply safeguards to protect social security numbers they keep on file.

(Preventing Identity Theft, 2006)

Identity Theft and Identity Fraud Trends

The incidents of identity theft and identity fraud reported to agencies increases fairly consistently year over year. There are many different ways to measure the impacts of identity theft and identity fraud. Javelin Strategy and Research has developed a comprehensive identity fraud survey that has been in existence since 2003. According the 2010 Identity Fraud Survey

Report, more consumers reported identity fraud in 2009, but the mean consumer expense and resolution time hours decreased.

More Consumers Experience Fraud, but Mean Consumer Costs and Resolution Hours Drop

Overall Measures of Impact

		Survey Report						
	Trend	2009	2008	2007	2006	2005	2004	2003
US adult victims of identity fraud **	↑	11.1 M	9.9 M	8.1 M	8.4 M	8.9 M	9.3 M	10.1 M
Fraud victims as % of US population	↑	4.8%	4.3%	3.6%	3.7%	4.0%	4.3%	4.7%
Total one year fraud amount *	↑	$54 B	$48 B	$45 B	$50 B	$57 B	$60 B	$58 B
Mean fraud amount per fraud victim ***	=	$4,841	$4,858	$5,509	$5,955	$6,436	$6,507	$5,736
Median fraud amount per fraud victim	=	$750	$750	$750	$750	$750	$750	$750
Mean consumer cost	↑	$373	$498	$720	$574	$467	$746	$606
Median consumer cost	=	$0	$0	$0	$0	$0	$0	$0
Mean resolution time (hours)	↑	21	30	26	25	40	28	33
Median resolution time (hours)	=	5	5	5	5	5	5	5

*Past years dollars figures have been adjusted for inflation using the Consumer Price Index (CPI-U) issued by the Bureau of Labor Statistics, ftp://ftp.bls.gov/pub/special.requests/cpi/cpiai.txt accessed 12/14/2009.

**Based on US population estimates (age 18 and over), http://www.census.gov/popest/estimates.php accessed January 01/11/10

***2006, 2007, 2008, and 2009 dollar cost estimates have been smoothed using three-year averaging—refer to Methodology Section for details.

Key survey findings:

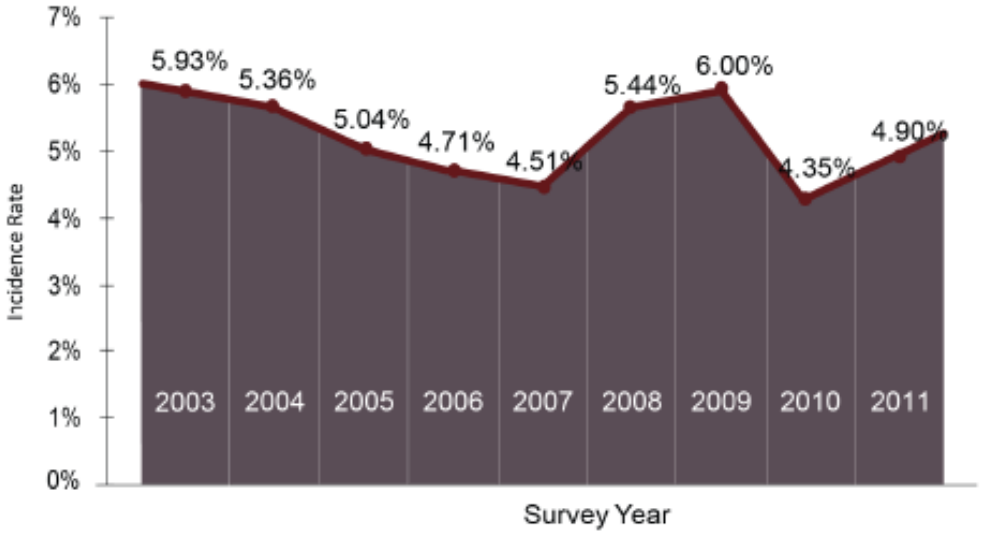
- The number of adult victims of identity fraud increased 12 percent from 2008 to reach 11.1 million, its highest number since the survey started in 2003. Potential contributor was the slower economy. Historically, fraud increases during economic downturns.
- Fraud victims as a percentage of the U.S population also increased to rich an all time high of 4.8 percent

- Total one year fraud amount increased 12 percent from 2008 to reach $54 billion, the highest since 2005.
- Although the incidents and fraud amounts have increased, the average cost and amount of time to resolve an incident of identity fraud decreased from 2008. This is most likely attributed to increased consumer awareness and increased assistance from financial institutions, consumer support agencies, and law enforcement.
- The number of fraudulent new accounts opened with stolen information in 2009 increased 33 percent from 2008. The number of new on-line accounts opened fraudulently more than doubled over that of 2008.
- Data breaches of health insurance information increased 4 percent over 2008 (Javelin Strategy & research, 2010)

The Javelin 2012 Identity Fraud Report reveals more interesting findings regarding trending and the prevalence of personally identifiable information found on targeted social networking websites. After a short-lived decrease in the incidence rate of identity fraud victims from 6 percent in 2009 to 4.35 percent in 2010, we see an increase of 12.6 percent from 2010 to 4.9 percent in 2011. In addition, the total number of identity fraud victims increased to 11.6 million in 2011, the highest since the survey began in 2003. However, despite an increase in the incidence and incidence rate, the overall fraud amount decreased from $54 billion in 2009 to an all time low of $18 billion. This is thought to be attributed to an increase in the traditionally less severe type of existing card account fraud verses the more severe new account fraud.

4.9% of U.S. Adults Were Victims of Fraud in 2011

Figure 1: Fraud Incidence Rate, 2003-2011

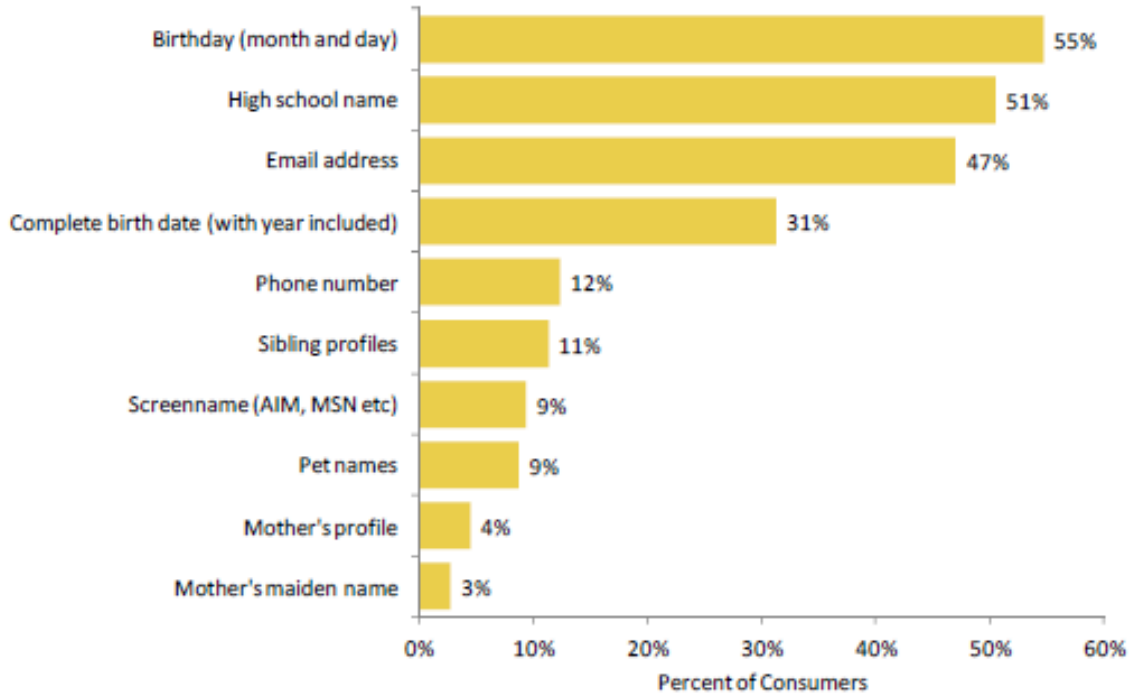


October 2011
n= approx. 5,000 per survey year
Base: All consumers.

The 2012 Identity Fraud Survey also included, for the first time, reporting on the types of information consumers post to the social networking sites. Identity thieves fully understand the value of this data. Many financial institutions use this information not only for processing applications but for customer authentication as well. With the growth in popularity for the social networking sites, more and more individuals of all ages are blindly jumping in and not fully comprehending the consequences of their actions.

Social Networking Sites Offer a Treasure Trove of Personal Information

Figure 2: Information Revealed on Social Networking Sites



Q45B: Which of the following have you currently provided on your social networking sites as part of your profile?

October 2011, n= 3,126
Base: All consumers who have accessed a social networking site.
©2012 Javelin Strategy & Research

The personal information identified in figure 2 above are commonly used by credit card companies and other financial services companies as a means to authenticate the customer via their customer service phone agents, Interactive Voice Response (IVR), and the on-line banking channels. Identity authentication challenge questions are often used to authenticate high-risk on-line banking and credit card transactions involving movement of funds, changes to user's online credentials, and changes to customer contact and demographic information (e.g., residential address, email address, home and mobile phone numbers). According to the Javelin survey, there is a higher rate of identity fraud among social media users than non users (Javelin Strategy & Research, 2012). This is not surprising when you consider the willingness of individuals to

share their personal information without regard to safety and security. Social media sites like Facebook and the professional networking site LinkedIn often request this type of information but do not necessarily require it in order to use their site. However, users often don't take the time to read the details and fail to adjust the settings that would reduce the risk of exposure. Additionally, many consumers use the same user name and password for both their social media and their on-line banking registrations. Identity thieves recognize and take advantage of this unsafe habit by using phishing and malware attacks, as well as, hacking the less secure social media sites for potential un-encrypted sensitive data. In June of 2012, LinkedIn was hacked and an estimated 6.5 million passwords were compromised and later published on a Russian hacker website (CBS News Money Watch, 2012). In June 2006, Google's social networking site "Orkut" was attacked with a worm seeking financial information and passwords. In the same month, My Space was targeted by an instant messenger phishing attack that attempted to steal account information from users (Social Networks a hacker's paradise, 2006). Both cases demonstrate the desire of ability of the identity thieves to access the vast amount of information that people willingly leave on the social networking sites. One of the techniques employed by the hackers is to compromise the victim's email address book and generate emails appearing to be from the victim to their unsuspecting friends and asking them to provide their information or click on links and download information which then compromises their computers.

Technical Subterfuge; Advancement of Malware

As mentioned in the previous passage, identity thieves adapted to the times and to technology and began to use the victims very own computers against them by way of malware. Deceiving users into clicking on links in emails appearing to be from people they know and infecting their machines with malware. Many times, the hacker would use the victim's machine

as a robot or "BOT" terminal. Sophisticated hackers would then create "BOTNETS" consisting of hundreds and sometimes thousands of compromised robot terminals under their command. The sole purpose of these attacks is to obtain personal and financial information to be used in more identity fraud. Typically, the victims are not even aware their computers have been compromised for months. Over the years, the types and purposes of malwares evolved and adapted to the anti-malware solutions that were developed to combat them. More sophisticated malware was developed that would be undetectable by typical anti-virus software. Certain malwares would remain dormant until which time the user would perform certain commands on their infected computer that would "awaken" the malware to perform its intended purpose. For instance, many malwares would only target on-line banking websites and would only activate when the user entered a banking institution URL. There are also more customized versions of the malware that would target a specific banking institution and only activate for that specific bank's URL. The perpetrators involved in these attacks research the banking institutions and identify all the countermeasures and customer authentication protocols required to perform the types of transactions they desire to compromise. Login credentials, challenge questions, and tokens are just some of the on-line banking anti-fraud controls that they target in their malware. The activated malware typically runs transparent to the victim while they perform their legitimate banking transaction(s). Some forms of the malware compromise the user credentials and account information entered by the victim and then use them later. Other more advanced malware known as "Man in the Middle" and "Man in the Browser" intercept the victim's on-line banking session and insert themselves into the session real-time. In these particular exploits, unbeknownst to the victim, the fraud transactions are occurring simultaneously with the legitimate transactions.

Social Engineering

According to Merriam Webster's dictionary (2012), social engineering is the "management of human beings in accordance with their place and function in society: applied social science." In other words, social engineering is essentially using human relationships to attain a goal. Social engineering is used in identity theft and identity fraud exploits in many different ways. In order to get someone to click on a link in an email that will infect their computer with malware, social engineering is used to trick the user by making them believe it was sent by a friend or legitimate company. The perpetrator is counting on the established relationship between the victim and the owner of the email address they have compromised and is leveraging that relationship to complete their ruse by making the victim take certain actions or provide certain sensitive or financial information. However, social engineering does not always require vast technical knowledge. Instead, social engineering can rely heavily on social skills. Calling a financial institution's customer service department and pretending to be an IT help desk technician or someone of similar position within the organization can also result in obtaining the necessary information to complete the identity theft or identity fraud exploit. Social engineering involves establishing trust, invoking sympathy, instilling fear, and any other human emotion that will result in taking the next step towards obtaining the perpetrator's goal.

Literature Review

Identity theft and identity fraud have been plaguing the financial and credit card services for decades. There has been sufficient research completed on the different types and techniques of identity theft, the relationship of identity theft, identity fraud, and social engineering, and ways for consumers to prevent identity theft. There has also been and continues to be consistent identity theft and identity fraud consumer victim reporting tracking the key metrics and trends year over year. However, there appears to be a lack of research on the financial services investment specifically dedicated towards combating identity theft and social engineering.

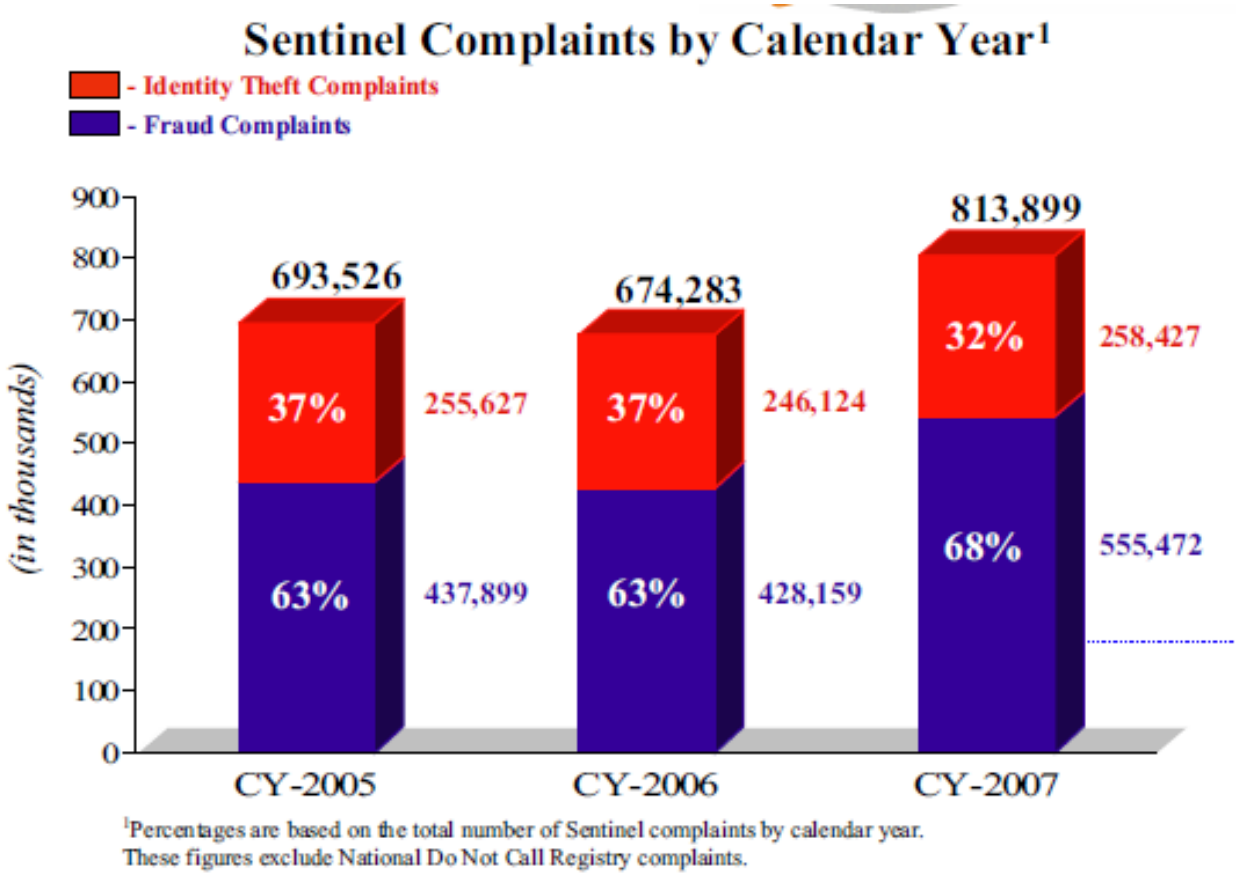
Identity Theft Reporting

There are numerous studies and research conducted on the scope and scale of identity theft and identity fraud. It's important to have different organizations conducting the various studies and research in order to gain some different and interesting insights into the impacts of identity theft and identity fraud.

Government reporting. As in most cases, the government always takes somewhat of a lead role in researching and reporting on crimes impacting American consumers.

Federal Trade Commission. The Federal Trade Commission has taken the lead in this respect and is responsible for housing the consumer identity theft and identity fraud data. The FTC also maintains the Consumer Sentinel Network, an on-line investigative database housing millions of consumer complaints utilized solely by law enforcement. In 2007, the Sentinel database contained over 4.3 million in identity theft complaints. According to the Federal Trade Commission's Consumer Sentinel Database (2008), the Federal Trade Commission received over 800,000 complaints during the 2007 calendar year, 32 percent of which were identity theft

complaints. The Sentinel graph below illustrates both the increase in overall complaints, as well as, increase in identity theft specific complaints year over year.



To further illustrate the prevalence of identity theft, the table below reveals the other types of fraud complaints that are also included in the complaint survey.

Sentinel Top Complaint Categories[1]

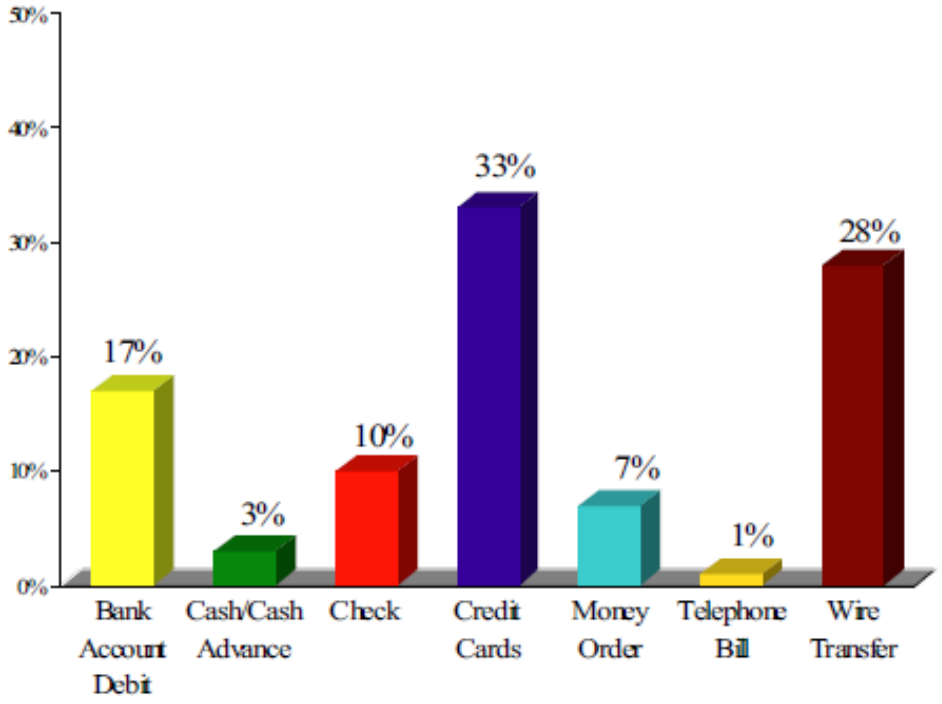
January 1 – December 31, 2007

Rank	Top Categories	Complaints	Percentage[1]
1	Identity Theft	258,427	32%
2	Shop-at-Home/Catalog Sales	62,811	8%
3	Internet Services[2]	42,266	5%
4	Foreign Money Offers	32,868	4%
5	Prizes/Sweepstakes and Lotteries	32,162	4%
6	Computer Equipment and Software[2]	27,036	3%
7	Internet Auctions	24,376	3%
8	Health Care	16,097	2%
9	Travel, Vacations and Timeshare	14,903	2%
10	Advance-Fee Loans and Credit Protection/Repair	14,342	2%
11	Investments	13,705	2%
12	Magazines and Buyers Clubs	12,970	2%
13	Business Opps and Work-at-Home Plans	11,362	1%
14	Real Estate (Not Timeshares)	9,475	1%
15	Office Supplies and Services	9,211	1%
16	Telephone Services	8,155	1%
17	Employ Agencies/Job Counsel/Overseas Work	5,932	1%
18	Debt Management/Credit Counseling	3,442	<1%
19	Multi-Level Mktg/Pyramids/Chain Letters	3,092	<1%
20	Charitable Solicitations	1,843	<1%

In keeping with the more specific research related to identity theft and credit card fraud, the Sentinel database also provides additional analysis that breaks down the method of payment by the consumer within the identity theft category. This represents how the consumer was eventually impacted by the identity fraud.

Methods of Payment Reported by Consumers[1]

January 1 - December 31, 2007



Methods of Payment Reported by Consumers

Calendar Years 2005 through 2007

	CY - 2005			*CY - 2006*			*CY - 2007*		
Payment Method	**Complaints**	**Percentages[1]**	**Amount Paid**	**Complaints**	**Percentages[1]**	**Amount Paid**	**Complaints**	**Percentages[1]**	**Amount Paid**
Bank Account Debit	14,802	23%	$ 26,448,169	13,156	20%	$ 37,712,964	11,726	17%	$ 29,371,619
Cash/Cash Advance	2,383	4%	$ 17,210,216	2,444	4%	$ 13,245,360	2,334	3%	$ 18,187,539
Check	10,440	16%	$ 75,252,950	8,628	13%	$ 96,464,400	6,757	10%	$ 80,035,706
Credit Cards	19,371	30%	$ 36,735,021	20,475	30%	$ 40,677,855	22,324	33%	$ 49,770,123
Money Order	7,200	11%	$ 12,538,520	5,913	9%	$ 20,357,643	4,596	7%	$ 31,071,393
Telephone Bill	1,175	2%	$ 491,499	1,267	2%	$ 418,295	974	1%	$ 295,724
Wire Transfer	9,485	15%	$ 86,558,141	15,460	23%	$ 149,640,338	18,484	28%	$ 130,958,802
Total Reporting Payment Method	*64,856*			*67,343*			*67,195*		

[1]Percentages are based on the total number of fraud complaints for each calendar year where consumers reported the method of payment: CY-2005 = 64,856; CY-2006 = 67,343; and CY-2007 = 67,195. 12% of the consumers reported this information during CY-2007, 15% and 16% for CY-2005 and CY-2006, respectively.

Credit card fraud, as a method of payment related to identity theft, consistently represents approximately 30 percent of the population and has increased year over year from 2005 through

2007. Further analysis reveals that, within the credit card fraud population, New Accounts fraud consistently averages over 14 percent with Existing Account fraud decreasing to 9.4 percent into 2007 from 10.7 percent in 2006.

The Federal Trade Commission also publishes the Identity Theft Survey Report (2006) commissioned and produced by Synovate. The specific objectives of the survey were to:

- Estimate the prevalence of ID theft victimization
- Measure the impacts of ID theft on the victims
- Identify actions taken by victims
- Explore measures that may help victims of future cases of ID theft

The following results were pulled directly from the 2006 Identity Theft Survey Report:

For the calendar year 2005:

- 1.4 percent of survey participants, representing 3.2 million American adults, reported that the misuse of their information was limited to the misuse of one or more of their existing credit card accounts in 2005. These victims were placed in the "Existing Credit Cards Only" category because they did not report any more serious form of identity theft.
- 1.5 percent of participants, representing 3.3 million American adults, reported discovering in 2005 the misuse of one or more of their existing accounts other than credit cards—for example, checking or savings accounts or telephone accounts—but not experiencing the most serious form of identity theft. These victims were placed in the "Existing Non-Credit Card Accounts" category.
- 0.8 percent of survey participants, representing 1.8 million American adults, reported that in 2005 they had discovered that their personal information had been misused to open new accounts or to engage in types of fraud other than the misuse of existing or new

financial accounts in the victim's name. These victims were placed in the "New Accounts & Other Fraud" category, whether or not they also experienced another type of identity theft.

Financial Value Obtained by Thief

- The median value of goods and services obtained by the identity thieves for all categories of ID theft was $500. Ten percent of victims reported that the thief obtained $6,000 or more, while 5 percent reported that the thief obtained at least $13,000 in goods and services.
- Where the identity thieves opened new accounts or committed other frauds (the "New Accounts & Other Frauds" category), the median value of goods and services obtained by the thieves was $1,350. Ten percent of these victims reported that the thief obtained $15,000 or more in goods and services; in the top 5 percent, the thief obtained at least $30,000 in goods and services. Victims in the New Accounts & Other Frauds category were three times as likely to report that the thieves obtained more than $5,000 as victims in the other two categories of ID theft (23percent vs. 7percent).
- Where the ID theft was limited to the misuse of existing accounts – either credit card or noncredit card – the median value of goods and services obtained was less than $500. However, much higher amounts were obtained in some cases. Ten percent of victims in the "Existing Credit Card Only" category reported that the thief obtained $4,000 or more in goods and services. In the "Existing Non-Credit Card Accounts" category, the comparable figure was $3,800.

The Costs of ID Theft to Victims

- In more than 50 percent of ID thefts, victims incurred no out-of-pocket expenses. (Out-of pocket expenses include any lost wages, legal fees, any payment of fraudulent debts, and miscellaneous expenses such as notarization, copying, and postage.) In the New Accounts & Other Frauds category, the median value of out-of-pocket expenses was $40.
- However, some victims do incur substantial out-of-pocket expenses. Ten percent of all victims reported out-of-pocket expenses of $1,200 or more. For the New Accounts & other Frauds category, the top 10 percent of the victims incurred expenses of at least $3,000, and the top 5 percent incurred expenses of at least $5,000. One-quarter of victims in the New Accounts & Other Frauds category reported paying out-of-pocket expenses of at least $1,000.
- Victims of all types of ID theft spent hours of their time resolving the various problems that result from ID theft. The median value for the number of hours spent resolving problems by all victims was 4. However, 10 percent of all victims spent at least 55 hours resolving their problems. The top 5 percent of victims spent at least 130 hours.
- Victims in the New Accounts & Other Frauds category spent the greatest amount of time resolving problems. In the top 10 percent in this category, victims reported spending 100 hours or more resolving problems. The top 5 percent reported spending at least 1,200 hours.
- Almost one-quarter of all victims were able to resolve any problems experienced as a result of ID theft within one day of discovering that their personal information had been misused. This refers to the amount of time that passed from when they discovered the

crime to when their problems where resolved, not to the number of hours spent resolving their problems.

- Thirty-seven percent of victims reported experiencing problems other than out-of-pocket expenses or the expenditure of time resolving issues as a result of having their personal information misused. The problems victims reported include, among other things, being harassed by collections agents, being denied new credit, being unable to use existing credit cards, being unable to obtain loans, having their utilities cut off, being subject to a criminal investigation or civil suit, being arrested, and having difficulties obtaining or accessing bank accounts.
- Victims of New Accounts & Other Frauds were more than twice as likely to report having one or more of these other types of problems (68 percent) than were victims in the Existing Non-Credit Card Accounts category (32 percent,) and four times as likely as victims in the Existing Credit Cards Only category (17 percent).

The Identity Theft Survey Report contains many more interesting metrics breaking down identity theft consumer complaint data but neither the report nor the Federal Trade Commission Identity Theft website contain any reporting on the financial services and credit card industry's challenges and expenses attributed to identity theft and social engineering detection and prevention.

Department of Justice. The Department of Justice commissioned a project in 2005 that also provided a great deal of identity theft related research and statistics, often referencing the Federal Trade Commission research and data clearinghouse. In the *Identity Theft Literature Review* (Newman & McNally, 2005) conducted by the United States Department of Justice, the researchers do identify some identity theft related costs to the credit card industry. With the

passage of the Fair and Accurate Credit Transactions Act of 2003, liability for the resolution of disputed credit report data was placed on the provider of the data. In addition, the three main credit bureaus, Equifax, Trans Union, and Experian all announced increased rates to their commercial clients. Whereas the total dollar loss of such costs cannot be estimated, one of the anticipated "soft costs" will be incurred through increasing staff levels in order to investigate complaints. Such increases, however, are accepted in the industry as "their cost of doing business". The researchers go on to state that other prevention costs are not directly reported and may be included in estimates of management costs related to commercial fraud departments. However, the American Bankers Association did provide an estimate by the General Accounting Office in 2002 suggesting that the total loss avoidance costs assumed by banks alone in 1999 totaled $1.5 billion dollars (Newman & McNally, 2005).

Non-profit organization reporting. Because of the tremendous negative financial and mental impacts identity theft and identity fraud have on the consumer, non-profit consumer advocacy groups and organizations also take an active role in research and reporting. The Identity Theft Resource Center (ITRC) is one such organization. The ITRC conducts research and reporting on behalf of the consumer and provides an interesting and different consumer lens on Identity Theft. One study from the ITRC reports on the concerns of the consumer in regards to the security and safety of their credit card information in regards to data breaches and transacting on the Internet. In the *Consumer Internet Transaction Concerns* survey (2010) consumers are increasingly concerned about the security of their personal and financial information when transacting on-line. Eighty seven percent express significant concern about their credit card information stolen or compromised via a merchant data breach. The survey goes on to provide the following:

- 81 percent of respondents cited phishing emails as a significant concern;
- 80 percent of respondents expressed significant concern over having their passwords stolen;
- 78 percent of respondents indicated they were significantly concerned over having usernames stolen;
- 77 percent of respondents were concerned about receiving SPAM emails (2010).

The survey also illustrates that consumers are becoming more aware and starting to take extra measures and caution to protect them when conducting credit card transactions or banking transactions in the on-line environment. Consumers immediately establish the link between on-line shopping and banking and identity theft. They also realize they cannot rely solely on the financial services and credit card industries to invest more in human and systemic resources to protect them and that they need to take matters in their own hands by exercising more due diligence. The survey reports the following in this regard:

- 58 percent of respondents always check the URL of links they receive in email before clicking;
- 41 percent refuse to use payment methods that allow access to their bank accounts;
- 35 percent regularly change passwords;
- 23 percent use low limit credit cards when conducting transactions on the Internet;
- 21 percent use a service that makes their identity anonymous when transacting online;

- 18 percent use a service that provides replacement credit cards that they're not liable for (2010).

Data breaches are also identified as a growing concern of consumers as well.

- If a breach occurred at a shopping website, 73 percent of respondents would stop making purchases at that website;
- If a breach occurred at a bill pay site, 68 percent would stop paying bills at that website;
- If a breach occurred at a bank site, 66 percent of respondents would stop online banking at that website and 46 percent would stop all banking at that institution;
- 68 percent would be likely to tell their friends about the breach at the offending website;
- 11 percent would not change anything despite losing personal or financial information.

The ITRC survey demonstrate the level of concern expressed by consumers in regards to the safety and security of their personal and financial information when transacting on-line and that they understand the link between the theft of their information and its potential use for identity fraud. The other key learning from the survey is that while consumers may want their financial institutions to take a more active role to protect their information, they are going to exercise greater due diligence when it comes to protecting their personal information.

Private research organization reporting. There are several well known and respected organizations consistently called upon to publish meaningful research pertaining to the financial services industry. However, the *Faces of Fraud, Complying with the FFIEC Guidance (2012)* report published by Information Security Media Group comes closest to identifying company investment and expenditures on resources dedicated to mitigating losses attributed fraud. According to the survey, for the first time since 2008, financial institutions expect an increase in their funds and personnel dedicated to fighting fraud. However, with the increase in on-line and mobile banking, there will also be increased fraud attacks and evolving and more sophisticated malware exploits as well. The survey reveals four main topics:

1. The Faces of Fraud - What are the most common fraud threats institutions face, and which threats are they best prepared to face? We also explore the factors that increase institutions' exposure to fraud, as well as the toll fraud incidents takes – hard costs and non-financial losses, too.

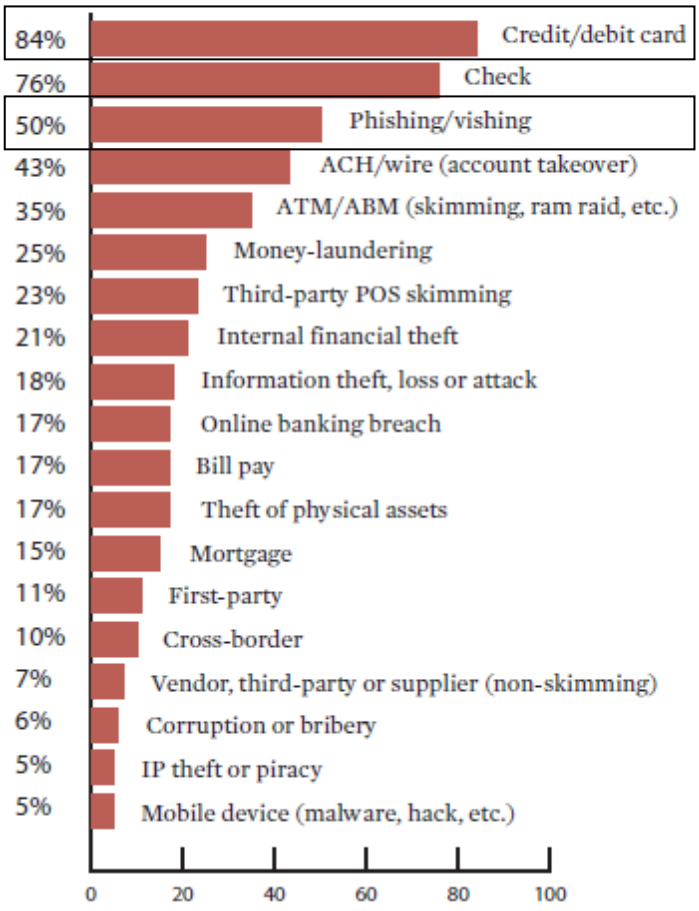
2. Conforming to the FFIEC Guidance - Why are financial institutions so unprepared to meet the expectations of the guidance, and when do they expect to achieve conformance? We show which recommended steps institutions have taken, and we share their overwhelming response to the question, "What's missing from the guidance?"

3. Anti-Fraud Investments - Some 58 percent of respondents expect increased anti-fraud resources in 2012, so where are they investing the money and personnel? We show a prioritized list of institutions' planned technology investments, then look at their stance on some emerging solutions.

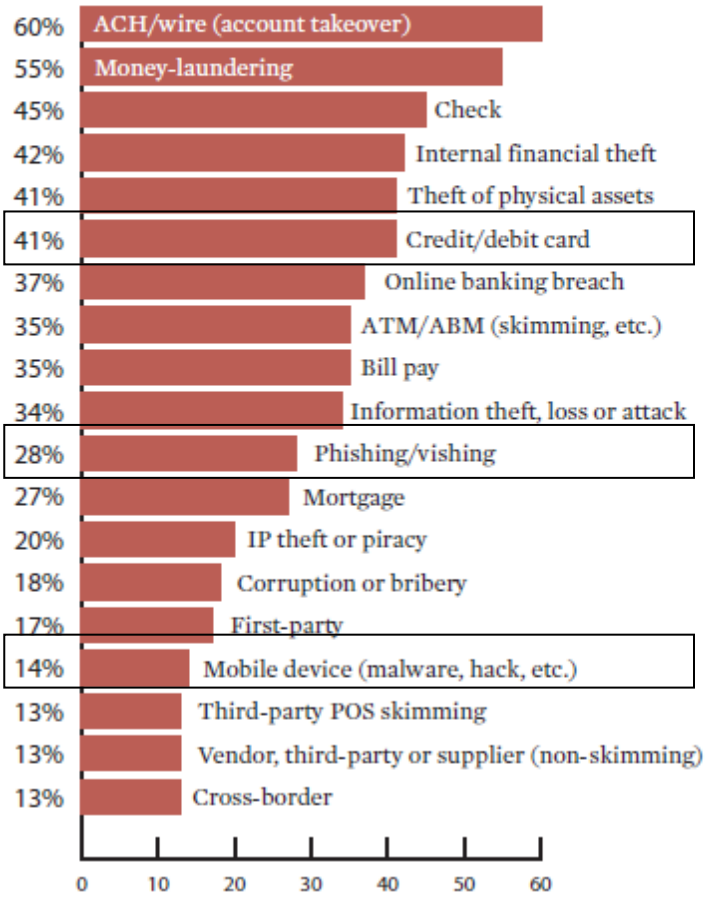
4. The Agenda - 2013 will be all about more - more fraud threats, more threat vectors, more anti-fraud solutions, perhaps even more regulation. How should banking institutions shape their fraud-fighting strategies? We share the tips gleaned from our survey results and expert analysis.

Financial services companies are trying to get better at detecting and preventing fraud by leveraging bigger and better data analytics to become smarter and more efficient. They also rank the types of fraud that they currently face and what types they feel their company is best positioned to manage. The charts below illustrate their responses.

Which types of fraud has your organization experienced in the past year?



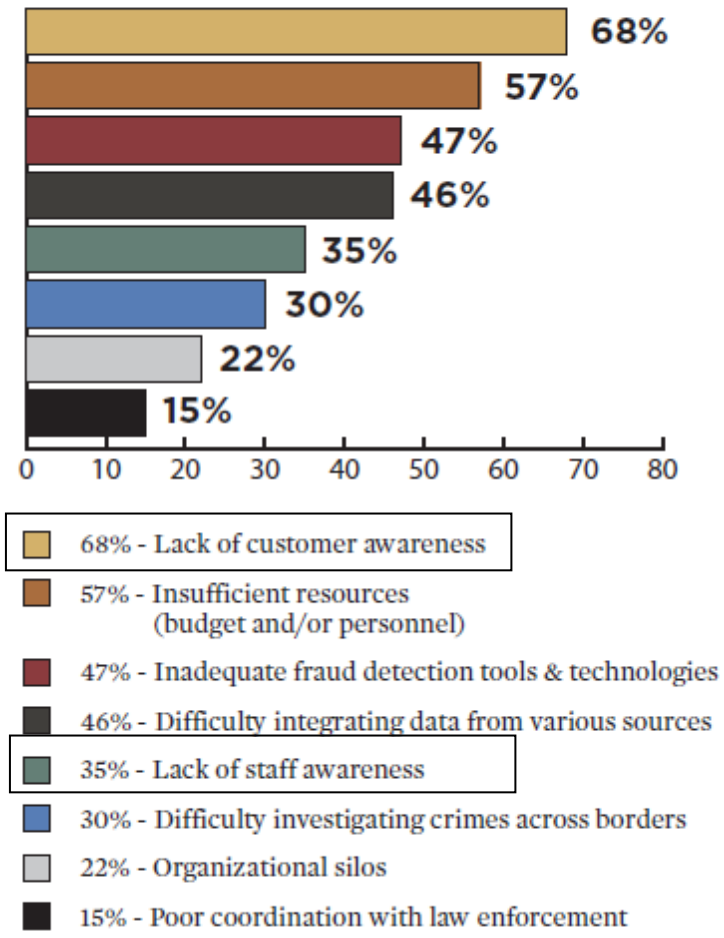
Which types of fraud do you feel your organization is currently best prepared to prevent and detect?



The interesting and also frightening finding of this particular survey is that the institutions rank identity theft related frauds as a current challenge yet don't feel they are prepared to deal with them in the future. In regards specifically to Phishing/Vishing, once a fraudster implants malware through a phishing e-mail or talks a banking customer (or employee) into surrendering an account number, this is the start of account takeover, which can lead to huge fraud losses – particularly for commercial customers. Identity thieves are getting better at mimicking corporate communications. They are also doing so cross-channel – through e-mails, telephone calls and text messages. So institutions must focus on educating staff and customers alike about the risks

of socially-engineered schemes. Organizations say their biggest challenge to fraud prevention is a lack of customer awareness.

What are your organization's biggest challenges to fraud prevention?



A key take away from this survey question is that institutions recognize that social engineering of both customers and staff is a major issue. Social engineering renders most authentication controls useless. In 2011, approximately 1 in 300 emails contained elements pointing to phishing. According to RSA, phishing emails increased 37 percent in 2011 with 50 percent of

the attacks targeting financial institutions (Information Security Media Group, 2012). In addition to the increased social engineering attacks via phishing, malware continues to evolve and become more sophisticated. The malware are intelligent enough to detect and bypass policies and security control layers, hijack the account and compromise the victim's credentials. Again, social engineering is involved in both phishing emails and deployment of malware. The Federal Financial Institutions Examination Council (FFIEC) has finally picked up on the social engineering problem and how it causes havoc on the traditional authentication mechanisms that their very own guidance recommended using back in 2005. FFIEC has required layered security controls in their updated guidance issued in 2011.

General Supervisory Expectations

> "The concept of customer authentication, as described in the 2005 Guidance, is broad. It includes more than the initial authentication of the customer when he/she connects to the financial institution at login. Since virtually every authentication technique can be compromised, financial institutions should not rely solely on any single control for authorizing high risk transactions, but rather institute a system of layered security, as described herein. " (FFIEC, 2011)

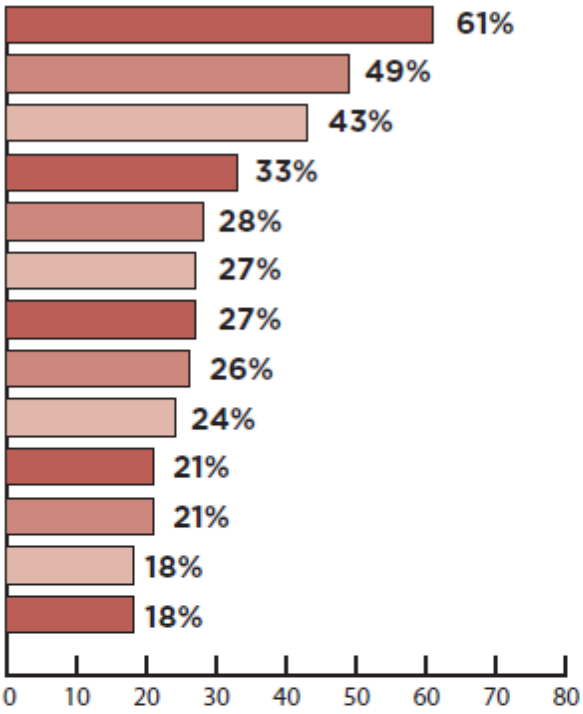
When it comes to layered controls, the FFIEC has two main requirements: The ability to detect and respond to suspicious activity; enhanced controls of administrative functions for business accounts. They also outlined some potential controls that could be used as part of the institution's layered security program. Majority of institutions favor customer education and fraud detection and monitoring systems. When asked which of the recommended controls the financial institutions planned to invest in, overwhelmingly they selected customer education and detection systems. While government regulation is a driver for spending and investment, so too

is the increased technology-based fraud threat coupled with the consumer's lack of awareness of them. Today's technology moves so fast that by the time a new phishing, malware, or social engineering attack is identified and communicated to the public, they have already fallen prey to it and given up their personal and financial information. In addition, companies have to re-educate their employees as to the many nuances of social engineering tactics.

The *Faces of Fraud*: *Complying with the FFIEC Guidance* survey has established that the financial services industry will increase their spending on anti-fraud resources in 2012 due largely to the FFIEC guidance update but also to the rapid advancement of technology-based fraud. The survey also identified where they will invest their increased resources.

- Technology - 41 percent;
- Personnel - 12 percent;
- External services - 9 percent;
- All of the above - 20 percent.

Which of the following anti-fraud controls and measures does your organization plan to invest in over the next 12 months? (Top 12 answers)



61% - Fraud detection and monitoring systems

49% - Staff training

43% - Enhanced customer education

33% - Out-of-band verification for a) authentication and b) transactions

28% - Enhanced controls over account activities

27% - Vendor management

27% - Internal or external audit

26% - Anti-money laundering tools

24% - Dual customer authorization through different access devices

21% - Case management or investigation management systems

21% - Enhanced tracking of high-risk customers

18% - "Positive pay," debit blocks, and other limits on transactional use

18% - Anti-phishing related technologies and services

Methodology

Research Information

The information that was located and used for this project was retrieved from government and private agencies. The information is then made available to the public, allowing the media to report any increase or decrease of crimes. The media makes it easier for the general public to access this information, and makes it a lot easier for the general public to understand.

The information contained in this report was mostly gathered from media outlets reporting on trends and activity in identity theft and identity fraud crimes. The statistics included in this report were gathered from a variety of media outlets including resources such as news reporting agencies. Utilizing information and data from news reporting agencies can benefit the researcher in different ways than utilizing information from the government or research organizations. Information and data collected from the media may not be as reliable but can still be used as qualified data for research.

This report also utilized information and data gathered from scholarly papers. This information was found through a search of scholarly articles related to the research question and directed to provide information to provide evidence throughout the paper. The ability to facilitate information from a scholarly article allows the researcher to add research from the past, giving the researcher a better idea of activity that was occurring in previous years. This concept works particularly well because it will identify trends that occur in the past, allowing the researcher to compare the trends of identity theft or identity fraud in the present, and how these crimes have evolved.

When using results and statistics from resources other than your own studies, there is always the potential for issues regarding validity. When the researcher is using someone else's

statistics, one is not sure that the findings in the research are relevant, and it may not be 100percent accurate. If the researcher does not perform their own research, the validity of the statistics is unknown. Other validity issues regarding the use of outside resources include the time that the study was conducted and the location.

There were some disparities in the time-frames of the data used in the research due to the length of time that had passed from when the research had begun and when it ended. The researcher had to take multiple leaves of absence from the project due to some personal hardships creating a gap of time of several years from when some of the original research had been pulled compared to the later research pulled closer to the completion of the project.

The desired information available while writing this paper was very limited. When trying to locate previous statistics and research on trends related to the financial services and credit card industries' identity theft detection and prevention related expenses, none were published.

Findings

The concepts of identity theft and social engineering have been in existence for long time. In the earlier times, people of lesser means would impersonate other people of power and wealth. This impersonation involved the use of another person's personal information and thus is considered to be a form of identity theft. As time passed and technology advanced, the evolution of identity theft continued and began to have a more pronounced impact on consumers and the financial services industry beginning in the early 1980's with the new account fraud application attacks championed by the Nigerians. The American financial services industry was under attack by the Nigerians who were educated and trained in their homeland Nigeria with explicit purpose to defraud the American financial system for their personal financial gain.

Later in the 1990's the development and eventual rapid growth of the Internet became the new frontier for the financial services and credit card industries for which to conduct business. Unfortunately, it also came with its share of vulnerabilities to be exploited by identity thieves and fraudsters. It was a race for first to market and all the major credit card companies and financial services institutions were throwing caution to the wind in an effort to be the first ones there. Consumers jumped at the opportunity to use this new technology and opened the door for increased rate of identity theft and identity fraud. The internet was extremely attractive for fraudsters as well because of the speed and efficiency, as well as, the faceless anonymity it provided. Identity thieves risk-reward equation favored reward more so with internet banking and e-commerce than it ever had before.

As technology advanced so too did computing power and scale. It became more and more popular to bank and shop online and consumer demand for increased functionality on the web grew. Tech-savvy hackers began to develop code that would be used to social engineer someone into performing a certain action or to make them willingly give up their personal or financial credentials to what they mistakenly believed to be a legitimate source. These phishing emails, as they were so aptly named flourished and wreaked havoc on the financial services industry. Consumers could not possibly differentiate valid from phishing emails and suffered great financial loss and hardship as a result. The pressure was on the federal government to enact new legislation making it a crime to commit identity theft and begin to empower and equip law enforcement with the right tools for the job to crack down on identity theft and identity fraud related activities.

Financial services and credit card industries also started to take notice of the consumers' lack of faith in the system and began investing in anti-fraud technologies specifically targeting

the types of actions related to identity theft. Although it is assumed that both industries invest heavily in the anti-fraud technologies, no research could be located that quantified the expense.

Conclusion and Recommendations

The purpose of this research project was to describe the evolution of identity theft, identity fraud, and social engineering and their impacts on the credit card and financial services industries. Although, there is plenty of research available on the trends of identity theft and identity fraud complaints and costs to consumers, there is no research that shows the industries' level of investment over the years in the systems and resources it dedicates towards to mitigating financial losses to fraud and compliance, financial loss due to operational expense, and even losses resulting from brand damage. However, the research and findings found in the *Faces of Fraud, Complying with the FFIEC Guidance (2012)* study reveals very enlightening and valuable findings with which the author of this research project in concurrence. The technological solutions that financial institutions invested in to reduce the losses attributed to identity theft can be both costly and a cause of increased negative client experience. The authentication protocols that have been placed in front of the credit card and banking transactions over the years have become the financial industry's primary weapons in the battle against identity theft. Yet, they have not proven to be sustainable due to the impacts of social engineering. The human element continues to be the weak link. Whether it's the unsuspecting consumer who unwittingly responds to a phishing email or the financial institution's customer service employee who unwittingly falls prey to the criminal's ruse, it's the human factor that will remain the key vulnerability that nullifies the effectiveness of the identity theft controls.

The FFIEC recognized the challenges and deficiencies of the authentication recommendations outlined in their original guidance and compensated for them in the 2011

update by requiring layered controls and increased customer awareness and education. The *Faces of Fraud, Complying with the FFIEC Guidance (2012)* study also recognizes the importance of education and awareness. The author feels that increased consumer awareness and employee education and training are critical components of an effective anti-fraud, identity theft prevention program. Technology will always have a place in a fraud prevention program; however, it must be accompanied by a robust awareness and education program in order to fully effective and sustainable.

REFERENCES

Computerworld (2012). Retrieved June 1st, 2012, from the computer world Web site: http://www.computerworld.com/s/article/9204760/Bank_tech_spending_to_hit_132B_in_2015_analyst_say

Nilson Report (2011). Retrieved August 20th, 2012, from the Nilson Report Web site: http://www.nilsonreport.com/pdf/news/112111.pdf

Identity Theft Data Clearinghouse (2005) Retrieved April 14th, 2006, from Federal Trade Commission Web site: www.consumer.gov/idtheft/pdf/clearinghouse_2005.pdf

Credit card debt on campus (2008). Retrieved October 8th, 2012, from CNN Money Web site: http://money.cnn.com/2008/07/10/pf/credit_cards_college/index.htm

About Identity Theft - Deter, Detect, Defend (2012). Retrieved September 8th, 2012, from Federal Trade Commission web site: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html

2006 Identity Theft Consumer Survey (2006). Retrieved September 12th, 2012, from Federal Trade Commission web site: http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

Identity Theft Manifesto (2009). Retrieved July 12th, 2012, from the Identity Theft Manifesto web site: http://www.identitytheftmanifesto.com/video-the-history-of-identity-theft/

Ventura County News (2012). Retrieved September 24th, 2012, from the KABC TV Los Angeles, CA web site: http://abclocal.go.com/kabc/story?section=news/local/ventura_county&id=8682473&pt=print

Federal Trade Commission (2000). Retrieved September 12th, 2012, from the Federal Trade Commission web site: http://www.ftc.gov/os/2000/03/identitytheft.htm

Preventing Identity Theft (2006.) Retrieved November 3rd, 2006, from the Utica ProQuest web site: http://proquest.umi.com.ezproxy.utica.edu/pqdweb?did=709638791&sid=14&Fmt=4&clientId=47962&RQT=309&VName=PQD

Javelin Strategy & Research (2010). Retrieved September 8th, 2012, from the Javelin Strategy web site: https://www.javelinstrategy.com/news/831/92/Javelin-Study-Finds-Identity-Fraud-Reached-New-High-in-2009-but-Consumers-are-Fighting-Back/d,pressRoomDetail

Javelin Strategy & Research (2012). Retrieved September 8th, 2012, from the Javelin Strategy web site: https://www.javelinstrategy.com/brochure/240#DownloadReport

CBS News Money Watch (2012). Retrieved October 8th, 2012, from the CBSnews.com web site: http://www.cbsnews.com/8301-505124_162-57450077/linkedin-hacked-how-to-protect-yourself-online/

Social Networks a hacker's paradise, (2006). Retrieved November 11th, 2006, from the ProQuest web site: http://proquest.umi.com.exproxy.utica.edu/pqdweb?did=1064594871&sid=12&fmt=3&clientid=47962&rqt=309&vname=pqd

Merriam Webster (2012). Retrieved October 1st, 2012, from the Merriam-Webster web site: http://www.merriam-webster.com/dictionary/social%20engineering

Federal trade Commission (2007). Retrieved June 1st, 2012, from the Federal Trade Commission web site: http://www.ftc.gov/sentinel/reports.shtml

Federal Trade Commission (2006). Retrieved June 1st, 2012, from the Federal Trade Commission web site: http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

Department of Justice/Office of Justice Programs (2011). Retrieved September 21st, 2012, from the Department of Justice/Office of Justice Program's web site: https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf

ITRC Consumer Internet Transaction Concerns Survey (2010). Retrieved September 25th, 2012, from the Identity Theft Resource Center web site: http://www.idtheftcenter.org/artman2/publish/m_press/2010_Consumer_Survey.shtml

Faces of Fraud, Complying with the FFIEC Guidance (2012). Retrieved August 25th, 2012, from the Information Security Media Group web site: http://docs.ismgcorp.com/files/handbooks/Fraud-Survey-2012/Fraud_survey_report_2012.pdf

Supplement to Authentication in an Internet Banking Environment (2011). Retrieved May 25th, 2012, from the Federal Financial Institution Examination Council web site: http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf