National White Collar Crime Center

CONTACT:
Research Section
5000 NASA Blvd. Suite 2400
Fairmont, WV 26554
Ph: 877-628-7674
Fax: 304-366-9095
Web: www.nw3c.org

Credit Card Fraud (2017)

Credit card (or debit card) fraud is a form of identity theft that involves an unauthorized taking of another's credit card information for the purpose of charging purchases to the account or removing funds from it.[1] This unauthorized 'taking' can occur through a number of methods.

How It Happens

Credit card fraud can occur in-person or via the Internet. Most consumer action groups, police departments, retail stores, and agencies such as Better Business Bureaus (BBB) and the Federal Trade Commission (FTC), routinely release consumers' information on how to avoid credit card fraud and identity theft. Nevertheless, there are numerous forms of credit card fraud that are committed by enterprising thieves, organized crime rings, business owners and even otherwise legitimate cardholders.

Lost or Stolen: One method of obtaining account information or even an actual credit card is through postal theft which involves a thief searching your mail box to steal credit card company statements which may contain personal account access data. They may even obtain a renewed card ready for activation. The thief can use the account information to make Internet purchases, order additional cards or make cash withdrawals with "checks" often included as promotional programs.

Card Not Present Purchases: Mail, including internet based transactions as well as traditional postal services) and telephone order frauds are regarded as the simplest and safest method for fraudsters to avoid detection. The illegally obtained information allows the perpetrator to make purchases anonymously as the authorized user. This method is reported as one of the most common methods of credit card fraud, amounting to almost three quarters of all reported fraud cases.[2]

Account Takeover: Also known as counterfeiting cards occurs when a perpetrator obtains sufficient personal information in order to report the card lost or stolen. The perpetrator requests a change of billing address and a new card is issued to an alternate address. Personal information can also be obtained by fooling victims with credit card or application verifier telephone scams, dumpster diving in search of discarded bills in the trash, or utilizing on-line directories in hacker forums, of information stolen by hackers and posted for sale in bulk. In some situations, perpetrators are able to purchase lists of stolen account information on the Internet through hacker web sites and blogs These bulk list can contain several hundred or even thousands of users' account information that were stolen expressly for their resale value.

Skimming: This fraud involves an electronic attachment that appears valid such as a self-service credit card swipe at a gas pump, or ATM. The fraudulent device reads and stores card information for the perpetrator.

Account information can also be obtained with low-tech strategies such as a retailer collecting credit card data (name, number, expiration date, and security code when the card is taken out of sight. Dinner purchases are a prime example. The perpetrator can use a smartphone adapter for credit card reading to obtain the information from the magnetic strip, or simply photograph both sides of the card. Once the victim information is obtained, there is little to prevent the determined thief from using that information to take over the victims account and run the card to the maximum credit limit.

A desktop computer system with peripheral equipment makes it relatively each for a counterfeiter to transform stolen data into a fraudulent debit or credit card.[3] As crime-fighting technology has improved, counterfeiting has become a multi-step process involving lamination, holograms and encoded magnetic strips. Most of the supplies used to manufacture counterfeited cards, including the plastic cards and Visa/MasterCard holograms (the Visa dove and the MasterCard interlocking globes) are smuggled into the United States from the Far East.[4]

Costs and Statistics

- The 2017 Identity Fraud Study released today by Javelin Strategy & Research revealed that the identity fraud incidence rate increased by sixteen percent, a record high since Javelin Strategy & Research began tracking identity fraud in 2003. The study found that despite the efforts of the industry, fraudsters successfully adapted to net two million more victims this year with the amount fraudsters took rising by nearly one billion dollars to $16 billion.[5]
- General purpose credit card spending has risen as a proportion of gross domestic product, rising from 10 percent of GDP in 2000 to 15 percent in 2014[6]
- Nearly half of all the credit card fraud around the world occurs in the US, even though America accounts for only about a quarter of the global card volume.[7]
- Multiple studies say about 7 in 10 Americans have at least one credit card. Federal Reserve data released in 2015, for example, found 70 percent of consumers had at least one credit card.[8]
- Using the Census Bureau estimate of 248 million adults in the U.S.,[9] reveals there are about 174 million Americans adults with at least one credit card.
- The FTC reports that from 2014 to 2016, the number of credit card fraud complaints increased by 29.09%, (36,230 to 46,771) and the costs of credit card fraud increased from $76,260,623 in 2014 to $96,444,198 in 2016, representing a 26.46% rise.[10]

Examples/Case Studies

- March 2016, in Kent County, MI - Sheriff's deputies arrested a Detroit man who used stolen credit card information to buy $100,000 in merchandise, $40,000 of which he spent at Kent County businesses. The arrest of Deandre Calhoun, age 27, is one of several by Kent County sheriff's deputies investigating numerous identity-theft and credit card fraud cases. Police say the suspects, from the Detroit area, used stolen credit card information to buy gift cards, iPads, electronic games and other products. Sheriff's deputies and Detroit police searched two Detroit homes and found property such as a sofa, television and collectible coins bought with stolen account numbers. Police also found hundreds of credit cards, credit-card numbers, Social Security numbers, personal information and equipment to encode magnetic strips on credit cards with stolen account information.[11]

- December , 2016, New York City: *Law enforcement officials say credit card fraud appears to be the latest frontier for violent gangs eager to make a quick buck.* "The Hoodstarz are a notorious gang that has terrorized parts of Brooklyn for years," said NYPD Assistant Chief James Essig. "That's what gangs usually do with guns, violence and drugs." However, the NYPD and Brooklyn DA's office say several gangs in the Brownsville area were also heavy into credit card fraud. Investigators say alleged gang members printed thousands of illegal credit cards using real and fake names. They bought the card numbers from hackers who sell stolen identification and financial data over encrypted websites, what's known as the "dark web." The members of Hoodstarz and other crews such as Folk Nation and 823 Crips then used the bogus cards to rent expensive cars, and buy everything from concert tickets to food. In all, 35 people were arrested.[12]
- Miami, September, 2016: Police raided the home at 3621 SW, 149th Place overnight. In addition to the phony cards police found skimmers, scanning machines, encoding equipment, a money counter and about 13 grams of crystal meth. Luis Perez-Luis and his son Jose Perez – father and son – lived in the home. They were led away in handcuffs in the early morning hours and charged with more than 400 counts each of various credit card fraud offenses. Court documents indicated that the number of charges could reach into the thousands after police had an opportunity to count all the seized credit and gift cards that were estimated to be worth a minimum, of $50,000. The thousands of phony credit cards contained information gathered by skimmers that were installed on ATMs, gas station pumps and store counters. Stolen gift cards from stores like Macy's and Kohl's would have their magnetic strip scanned then discretely returned to the store inventory. Later when a scanned card was purchased by an unsuspecting victim, the two criminals would encode an identical fake card, thereby loading it with legitimate funds. The duplicate could then be used or sold. A Miami judge set each man's bail at more than a half million dollars. In order to post bond, they had to prove the money was "clean," and not derived from illegal operations. If bonded, they would be kept under house arrest.[13]
- April, 2016. Two New York City men were arraigned in federal court Friday on charges for fraudulently purchasing gift cards to buy hundreds of thousands of dollars' worth of electronics and other goods. Nikolay Krechet, 45, of Queens and James Olla, 24, of Brooklyn, were each charged with one count of conspiracy to commit wire fraud and four counts of wire fraud. According to criminal complaints, Krechet, Olla and others procured stolen credit card information. Since the credit card thefts are generally detected quickly, they used the credit cards to purchase gift cards which were less detectable, and maximized usability. In one example, a cooperating witness allegedly sold Krechet $28,700 in gift cards for $22,452. Krechet paid for it with $14,300 in cash and 44 iPads. In another example, Krechet in part traded more than $60,000 in fraudulently purchased gift cards with 58 iPhones. From December 2014 through April 2015, the informant allegedly sold Krechet fraudulently purchased gift cards worth more than $2 million. Olla also

purchased gift cards, noting that phone records show he called Target about the balance on 117 gift cards before using them -- allegedly a sign of fraudulent purchases. The informant sold Olla more than $400,000 in gift cards in 2014.[14]

- January, 2016. Tahir Lodhi led one of the largest credit card fraud schemes ever charged by the U.S. Department of Justice (DOJ). The Hicksville, New York man was sentenced to more than six years in prison after pleading guilty to one count of conspiracy to commit bank fraud. According to court records, Lodhi directed the gang to fabricate more than 7,000 false identities to obtain tens of thousands of credit cards. The group used the cards and initially paid the bills, boosting their supposed creditworthiness, according to the U.S. Attorney's office. They then borrowed or spent the maximum allowed for the account, which they did not repay. Besides the phony credit card accounts, the gang set up more than 1,800 drop addresses, which were used as mailing addresses for the false identities. Those addresses also were used to obtain credit card terminals to submit charges on the fraudulent cards. The sham companies were set up at the drop addresses, and provided false credit histories on fake company employees. The U.S. Attorney's office also said that several jewelry stores in Jersey City cooperated in the scam, using multiple credit card processing accounts to accept numerous transactions, with the proceeds being split amongst the gang. In addition, $4 million in gold was seized from a number of jewelry stores.[15]
- Elton Lee Flenaugh and Deje D. Silas have been sentenced to federal prison for credit card fraud and identity theft crimes. Flenaugh and Silas had a romantic relationship dating back several years. On February 9, 2013, Flenaugh and Silas were scheduled to fly from Atlanta to Los Angeles. During the pre-flight security screening process in Atlanta, alert TSA security officers noticed a suspicious package in Flenaugh’s carry-on bag, and upon further inspection, found nearly 100 fraudulent credit cards secreted inside a double-sealed manila envelope. The cards had been, hidden inside a foil-lined Lay’s potato chip bag. Thirty-three of the cards were embossed in Silas’ name, 28 were embossed in three different aliases used by Flenaugh, and 21 were blank and had not yet been embossed. Subsequent searches by the Atlanta Police Department revealed fraudulent driver’s licenses inside the protective case attached to Silas’ cell phone and underneath the removable insole of one of Flenaugh’s shoes in the carry-on bag. Additional investigation revealed fraudulent credit cards, licenses and stolen credit card accounts and identity information of hundreds of people. These items were found in personal belongings seized during searches, and found under Google e-mail accounts (controlled by Flenaugh and Silas) in an Apple iPad seized from them at the airport, and a 2007 BMW M6 automobile registered to one of Flenaugh’s aliases. The scheme involved obtaining credit and debit card account information from hundreds of people, which were then used to manufacture fraudulent credit cards. The cards were made to appear as if they had been issued by major financial institutions such as Chase Bank, U.S. Bank, and Capital One. The defendants also obtained personal identifying information (including Social Security numbers, dates of birth, and credit information) from dozens of people, which were used to create fraudulent driver’s licenses to verify use of the fraudulent credit cards.[16]

The Response / Current Efforts

The security weaknesses of credit cards start with their embossed 16 digit number. The number identifies the specific account that holds funds to withdraw during card presentation. Anyone equipped with this information has the ability to make a copy of the card, or conduct a transaction over the phone.

There have been several methods in the past to secure cards. Imprinted receipts were originally implemented to help assure that the person making the financial transaction was in possession of the embossed card. Embossing machines in the hands of counterfeiters negated the effectiveness of this method of security. Credit cards also utilized signature panels on the back of the cards that allowed the merchant to compare the signature with another form of identification. The signature panel was designed to make it obvious if erased or otherwise manipulated. Merchants could refuse card acceptance if a signature was not present. The magnetic strip on the back of the card effectively did away with the need for imprinting. Later, small inexpensive palm held readers thwarted the security measure. Beginning in 1981, a Hologram was added to the front of the cards as another type of security. The intent was to make it more difficult to counterfeit the cards, but even holograms were duplicated and sold to identity thieves. It didn't take long for large-scale hologram counterfeiting operations to develop in Taiwan, Hong Kong, and China which sell for between $5 and $15, depending on the quality of the hologram.[17] In 1994, the Canadian Combined Forces Special Enforcement Unit and the Combined Forces Asian Investigation Unit arrested members of a Chinese syndicate that produced approximately 300,000 counterfeit holograms. They had distributed 250,000 holograms. Based on the quantity delivered and using an estimate of $3,000 lost per card, Visa and MasterCard valued this crime caused combined losses of $750 million.[18]

The credit card security weaknesses of all the methods discussed thus far, is that once the data is compromised, the card could be duplicated and illicit transactions could be made without the owners' knowledge or consent.

Beginning in the early 90's, the EMV, also referred to as chip and PIN or smart cards, were created by the consortium of Europay, MasterCard and Visa (EMV).[19] The EMV chip creates a flow of information between the card and the issuing financial institution to verify the card's legitimacy and creates a unique set of financial data for that specific transaction. The chip is much more difficult to duplicate and has reportedly led to reduction in credit card fraud from "point of sale" transactions (i.e. where the card must be physically presented to the vendor). Initial findings showed impressive reductions in credit card fraud, 80% reduction in France and 67% in the UK. EMV conversion in the U.S. was scheduled to be complete as of October 2015. As of the end of September 2016, it is estimated that 81% of all U.S. credit cards issued are equipped with the EMV chips.

Regardless of the measures taken to prevent credit card fraud, it appears that this fraud is still on the rise, and a major reason for stealing someone's identity is to commit credit card fraud. According to Javelin research, the trend in 2016 is that incidents of credit card fraud are still on the rise.

> In all, 15.4 million victims were affected, 2 million more than in 2015, representing 6.15% of all consumers. The study did not look exclusively at credit card, but Javelin said the vast majority of identity theft fraud is linked to credit cards.[20]

The general feeling is that individual security measures are relatively ineffective as long as cyberintrusions and data breaches compromise the security of personally identifiable information. As cards became harder and harder to duplicate, point of sale frauds declined, but the thieves shifted their strategies and moved to on-line purchases that can't take advantage of the new security technology.

Banks, credit card companies and retailers must remain vigilant in order to control these frauds. Last year, online retail sales totaled $22 trillion and are expected to top $27.7 trillion in 2020.[21] Fraudsters are willing to adapt to changing security measures, and no matter how many new safeguards are created, there will always be vulnerability to exploit.[22]

Additionally, many major credit card companies have banded together to help ensure safety by issuing what is known as the Payment Card Industry Data Security Standard (PCI DSS). This standard requires all merchants to follow the same guidelines of data security. It is unknown how many retailers are PCI compliant, but Visa estimates that upwards of two-thirds of its large and medium-sized merchants meet requirements. In order to assist business owners to navigate the intricate technology regulations, card companies and payment processors are supplying tutorials and webinars..[23]

Now available nationwide is an initiative to battle credit card fraud and identity theft on a federal level. The Fair Credit Reporting Act requires consumer reporting companies, upon consumer request, to provide a free copy of the consumer's credit report (including information on where you live, how you pay your bills, and whether you've been sued, arrested, or filed for bankruptcy).[24] This allows consumers the ability to closely monitor their own credit histories without paying charges to reporting agencies.

Credit Card Fraud Prevention Tips

In an attempt to secure our credit score and finances, it is important to remember to use caution when taking advantage of credit card convenience. As described above, new innovative credit card security designed to foil credit card fraud has proven fallible. Regardless of the latest invulnerable security, the responsibility ultimately rests with the credit card owner. A number of agencies provide lists of pro-active common sense measures that every credit card owner can take to minimize exposure and the threat of becoming a victim of fraud.[25]

- **Stay secure on-line**: Beware of using public Wi-Fi to conduct online financial transactions of any kind. If forced to use a public computer, always be sure to clear log-in information such as username and password at the end of every transaction. Periodically change usernames and passwords to secure from prying eyes.

- **VPN Technology**: A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. To ensure safety, data travels through secure tunnels and VPN users must use authentication methods -- including passwords, tokens and other unique identification methods -- to gain access to the VPN. The benefit of using a secure VPN is it ensures the appropriate level of security to the connected systems when the underlying network infrastructure alone cannot provide it.[26]

- **Demand a new credit or debit card if you think your information may have been compromised**: Retailers, financial institutions, educational systems, law enforcement, governments and anyone with information to be stolen can be the victim of cyber intrusions/data breaches which compromises personally identifiable information. Many times, when these high profile incidents happen, customers are notified and replacement credit or debit cards are issued immediately. If your personally identifiable information/personal health information (PII/PHI), data is involved in such an incident, and have not been offered a replacement card, call and request a new issuance.

- **Become aware and stay abreast of "phishing" attacks:** These attacks are designed to trick you into divulging your confidential access information. These are particularly prevalent after a high profile breach that makes the news. If you receive an email supposedly from a financial institution, do not respond via email, do not click links and do not enter information that could give a hacker access to your financial information. Find a phone number and call the bank referenced in the email to make sure the message was legitimate. Do not use a phone number that comes within the email message. Independently search for the institution's phone number.

- **If you feel your information has been compromised, lock down your credit report with a security freeze:** This shuts off access to your credit history by new would-be lenders. If a hacker applies for a loan in your name, the creditor is less likely to approve it if he or she can't see your credit file. If you have bene the victim of identity theft, the freeze may be free through your credit card agency

- **Use a Credit Card rather than a Debit Card:** Debit cards do not offer the same protections against fraud as the credit card. In either case, the bank will likely see that you get your money back from fraud. The minor difference noticed when choosing "credit" over "debit" when you're using a debit card: Since they go through the credit card network, transactions processed as "credit" may take a few days to clear. Transactions processed as "debit" hit your checking account immediately.[27]

- **Review all of your credit card transactions online**: It's not necessary to wait for the monthly statement to monitor questionable transactions on your card. Use the online log-in capabilities to check your transactions regularly to identify questionable activity, before too much damage.

- **Get as many as 18 free credit reports per year:** This helps you actively monitor your accounts and locate fraudulent new accounts. You can get three free credit reports (one from each credit bureau) from annualcreditreport.com. You're also entitled to a free credit report from each bureau (Transunion, Experian or Equifax) after you file a 90-day fraud alert, which you should do every 90 days if you've been a victim of data breach or have a good-faith suspicion that you're about to become a victim of identity fraud.[28]

- **Use the same credit card for all online transactions**: It's a good idea to keep one credit card for nothing else but online transactions. This helps limit the damage that can be done if someone has obtained your information and is attempting to take over the account.

- **Be sure to log off after each online transaction**: Many retailers and banks will have a feature that will automatically log the user off after a pre-determined period of inactivity, but it's always best to train yourself to log off after every online transaction.

- **Be sure to shred all documents and statements that may contain personally identifiable information**: Monthly statements in regular mail may seem convenient for keeping abreast of payments and due dates, but thieves are also aware of their existence and may search trash. Shredding all such documents is a good habit.

- **Be aware of your surroundings when making purchases over the phone:** Verbally providing someone your account number, expiration date and three digit verification code over the phone may seem harmless enough; however, it's always best to be sure that no one is within hearing range to copy information for use at a later time.

- **Never provide the card number or other identifying information to an unverified caller:** In the event someone calls and claims to represent the company, a vendor or they provide some other reason for asking for the credit card information over the phone, simply decline to provide the information. Ask for verification and look up the company to determine the correct contact information. Call and verify that someone from that agency legitimately contacted you and needed the information before providing it.

- **Avoid emailing the card number and other info needed to conduct the transaction**: Any time you write or type your credit card number and give it to someone in an unsecured, unencrypted manner (including on a piece of paper), you increase the chance that the card number will be exposed.

"For More Information" Links

- Federal Bureau of Investigation – www.fbi.gov
- Federal Trade Commission – www.ftc.gov
- Better Business Bureau – https://www.bbb.org/
- Credit Card Insider - https://www.creditcardinsider.com/
- Credit Cards . com - http://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264.php
- Multi-State Information Sharing and analysis Center (MS_ISAC) - https://msisac.cisecurity.org/
- FBI's Internet Crime complaint Center - https://www.ic3.gov/default.aspx

Maintenance and Revisions: NW3C Research Department

Bureau of Justice Assistance
U.S. Department of Justice

This project was supported by Grant No. 2015-BE-BX-0011 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Smart Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Endnotes

[1] Definitiion obtained from FindLaw.com web site at http://criminal.findlaw.com/criminal-charges/credit-debit-card-fraud.html

[2] MasterCard Newsroom, October 28, 2014, retrieved from https://newsroom.mastercard.com/asia-pacific/2014/10/28/8-different-types-card-fraud/

[3] Slotter, K. Plastic payments: Trends in credit card fraud. FBI Law Enforcement Bulletin, Retrieved, from http://www.debtsmart.com/pages/article_trends_in_credit_fraud_020731241.html

[4] Slotter, K. Plastic payments: Trends in credit card fraud. FBI Law Enforcement Bulletin, located at; http://www.debtsmart.com/pages/article_trends_in_credit_fraud_020731241.html

[5] Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study, Javelin Research, located at; https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

[6] The Consumer Credit Market Report, published by U.S. Consumer Finance Protection Bureau, December 2015, located at; http://files.consumerfinance.gov/f/201512_cfpb_report-the-consumer-credit-card-market.pdf

[7] Americans are By Far the Hackers Favorite Credit Card Fraud Target, located at; https://qz.com/411000/americans-are-by-far-hackers-favorite-credit-card-fraud-targets/

[8] The Federal Reserve Bank of Boston's 2013 Surveys of Consumer Payment Choice, released July 27, 2015 located at; https://www.bostonfed.org/publications/survey-of-consumer-payment-choice.aspx

[9] U.S. Census bureau, July 2015 estimate of U.S. population (minus under-18s) located at; https://factfinder.census.gov/faces/nav/jsf/pages/index.xhtml

[10] Federal Trade commissions' Consumer Sentinel Network Data Book for January – December 2016, located at; https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf

[11] Agar, J. Man Spent $100,000.00 with Stolen Credic Cards, Fraud Cases Cracked, published in Mlive. com, March 8, 2016, located at http://www.mlive.com/news/grand-rapids/index.ssf/2016/03/man_spent_100k_with_stolen_cre.html

[12] Meminger, D. "Brooklyn Gang Bust Uncovers Credit Card Fraud, ID Theft Ring" published in NY1, March 3, 2017, located at; http://www.ny1.com/nyc/all-boroughs/news/2016/12/13/brooklyn-gang-bust-arrests-.html

[13] Father, Son Arrested in $50K Gift Card Fraud Raid. Nelson, G. published 9/1/16 in the Miami Herald, located at; http://miami.cbslocal.com/2016/09/01/counterfeit-credit-card-operation-busted-in-sw-dade/

[14] "2 NY Men Charged in Credit Card Fraud Scheme Using Gift Cards" by Darragh, T. published in NJ.com on 4/15/16, located at; http://www.nj.com/news/index.ssf/2016/04/two_nyc_men_charged_in_credit_card_fraud_scheme_us.html

[15] "Leader of $200M Credit Card Fraud Scheme Sentenced" by Darragh T. published by NJ.com 1/7/16, located at; http://www.nj.com/hudson/index.ssf/2016/01/leader_of_massive_credit_card_fraud_scheme_sentenc.html

[16] "California Couple Sentenced to Federal Prison for Credit Card Fraud and Identity Theft Crimes." Posted in the U.S. DOJ web site, under U.S. Attorney's Office Northern District of Georgia, Feb. 28, 2014, located at; https://www.justice.gov/usao-ndga/pr/california-couple-sentenced-federal-prison-credit-card-fraud-and-identity-theft-crimes

[17] Slotter, K. (1997, June). Plastic payments: Trends in credit card fraud. http://www.debtsmart.com/pages/article_trends_in_credit_fraud_020731241.html

[18] Slotter, K. (1997, June). Plastic payments: Trends in credit card fraud. FBI Law Enforcement Bulletin. Retrieved, from http://www.debtsmart.com/pages/article_trends_in_credit_fraud_020731241.html

[19] "The Past, Present and Future of Credit Card Security", retrieved on March 31, 2017 from; http://www.theonebrief.com/the-past-present-and-future-of-credit-card-security/

[20] 2016 Identity Fraud: Fraud Hits an Inflection Point, by Pascual, A.,Marchini, K., and Miller, S. published 2/2/16 by Javelin Research, located at; https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point

[21] "About 10 Million More Americans Shopped Online than in Stores Over Black Friday Weekend" by Wahba, P. in Fortune Magazine, November27, 2016. Located at; http://fortune.com/2016/11/27/black-friday-nrf-shopping/

[22] "That Chip on Your Credit Card Isn't Stopping Fraud At All" by Bukhari, J. published Feb. 1, 2017, in Fortune Magazine,   located at; http://fortune.com/2017/02/01/credit-card-chips-fraud/

[23]Huggins, R. (2015, August). *Holding Client Credit Card Info On File: Why and How To Do It, How Not To Do It*. Retrieved January 21, 2016, from https://personcenteredtech.com/2014/01/08/holding-client-credit-card-info-on-file/

[24] Federal Trade Commission. (2012). *Facts for consumers: Your access to free credit reports.* https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf

[25] Keeping Your Credit Cards Secure by Harkness, B. 2/21/17, located at; https://www.creditcardinsider.com/learn/keeping-your-credit-cards-secure/

[26] Definition of VPN from TechTarget.com, located at; http://searchenterprisewan.techtarget.com/definition/virtual-private-network

[27] Debit Cards Vs. Credit Cards by Credit Card Insider, located at; https://www.creditcardinsider.com/learn/debit-cards-vs-credit-cards/

[28] "Security breaches such as the one at Home Depot aren't going away anytime soon. It's time to put your personal information on lockdown." Published in Consumer Reports, September 2014, located at; http://www.consumerreports.org/cro/news/2014/09/protect-against-credit-card-fraud-now/index.htm