



Past Solutions to Present Security Breaches

November 2014

VIR-SEC® is a registered trademark of Vir-Sec, Inc.
U.S. Patent No. 8,074,261; U.S. Patent No. 8,484,701

Prepared by the Cyber Projects Division of Vir-Sec, Inc.

Table of Contents

| | |
|--|----|
| Introduction..... | 5 |
| History of Credit Cards..... | 6 |
| <i>Charge Coins</i> | 6 |
| <i>Charga-Plate</i> | 6 |
| <i>Air Travel Card</i> | 7 |
| <i>Invent of General Purpose Cards</i> | 7 |
| <i>Visa and MasterCard</i> | 7 |
| <i>International Deployment of Credit Cards</i> | 8 |
| Major Breaches of Credit Card Information..... | 9 |
| <i>TRW/Sears</i> | 9 |
| <i>TJX Companies</i> | 9 |
| <i>Heartland Payments Systems</i> | 9 |
| <i>Sony</i> | 9 |
| <i>Adobe Systems Inc</i> | 10 |
| <i>Target Corporation</i> | 10 |
| <i>Neiman Marcus</i> | 10 |
| <i>The Home Depot</i> | 11 |
| <i>JPMorgan Chase & Co</i> | 11 |
| <i>Staples Inc</i> | 11 |
| Retail Cyber-Attacks: Exposure of Critical Infrastructure..... | 12 |
| <i>Credit Card Network Exposed</i> | 12 |
| <i>Consumer Trust</i> | 13 |
| <i>End of the World Scenario</i> | 14 |
| <i>Response to the Breaches</i> | 14 |
| Security Features of Major Credit Cards..... | 15 |
| <i>Visa</i> | 15 |
| <i>MasterCard</i> | 15 |
| <i>American Express</i> | 16 |
| <i>Discover</i> | 16 |

| | |
|---|----|
| Credit Card Fraud Prevention: Failed Industry Solutions..... | 17 |
| <i>PAN Truncation</i> | 17 |
| <i>Request of Additional Information</i> | 18 |
| <i>Falcon Fraud Prevention Software</i> | 18 |
| <i>Card Security Codes (CSCs)</i> | 20 |
| <i>EMV Chip and PIN Credit/Debit Cards</i> | 21 |
| Vir-Sec® SecureAccess™ Solution..... | 25 |
| <i>Multifactor Authentication</i> | 25 |
| ➤ “ <i>Something You Have</i> ” | 27 |
| ➤ “ <i>Something You Know</i> ” | 28 |
| <i>Virtual Environment Application (VEApp)</i> | 29 |
| SecureAccess™: The Next Generation of Credit/Debit Card Security..... | 31 |
| <i>SecureAccess™: Future of Credit/Debit Cards</i> | 31 |
| Conclusion..... | 33 |

Introduction

Credit card fraud has been a rampant problem plaguing the financial industry since the credit card was first introduced to the consumer. While the credit card has enhanced the economic purchasing power of each individual consumer, it has also exposed businesses, individuals, and institutions to fraud and theft.

The financial industry has responded with a multitude of “solutions” to combat fraud and theft, although all of these solutions have been inadequate in solving the overall issue of security. What the industry has sold to consumers as leading innovations have been solutions to past problems and nothing to solve current issues of security breaches.

Financial transactions, data, and accounts have proven difficult to secure for both the consumer and the institution. All technologies deployed have used some type of existing technology and have done little to keep up with the changing cyber landscape. While third party payment systems such as PayPal® have provided some level of security, it has done little to nothing to protect the consumer at the basic level, as the largest consumer hack in U.S. history was of a third-party payment processor.

In addition, financial institutions are also at risk when fraud and theft occur. A banking institution can only have credibility if it can protect the financial information and data of its clients. Recently, financial institutions seem more exposed than usual. With the recent hacking of JPMorgan Chase & Co., one of the largest and most well secure banks, consumers and policy makers are beginning to ask when the other institutions will suffer breaches. While individual accounts may not have been compromised, the personal data of consumers is all that is necessary for bad actors to conduct business on the black market of financial data.

Even worse, banking institutions and retailers have delayed informing the public and account holders that breaches have taken place. Recently, it has taken up to 5 months for a retail institution to disclose to the public that the institution has experienced a breach that could have caused account holders’ financial and personal information to be compromised. In the modern cyber landscape, 5 months can be compared to a lifetime, and by that time it is far too late to be telling consumers their information may be compromised, as the damage has likely already been done.

In the modern age, cybersecurity for consumers and institutions are becoming a market imperative. No longer should institutions deny basic and cost effective security measures that will protect the identities of individuals and the credibility of financial institutions and retail businesses. Technological “solutions” deployed to this point have been highly inadequate, and have left consumers exposed to having their personal and financial information stolen.

History of Credit Cards

The concept of using a “credit card” in order to purchase goods was first described by Edward Bellamy in 1887. In his novel *Looking Backward*, Bellamy used the term “credit card” eleven separate times to describe a citizen using their dividend from the government in order to purchase goods, similar to the current U.S. Social Security system, rather than borrowing money on credit¹. The conception of what would become the modern day credit card began at this time, only at this point, the viewpoint of the credit card is that it would expend dividends on behalf of the government and not the modern day private banking institution.

Charge Coins

Charge coins were in use from the 1800’s up until the 1930’s when the stock market crashed and the Great Depression hit. These “coins” were made with celluloid, copper, or some other material, and also had a small hole enabling the coin to be carried on a key chain. These coins were typically used by department stores, hotels, and other such businesses and were given to those who had large charge accounts at such businesses. The coins typically had the logo of the business on it in addition to a charge account number. The coins, however, did not have the account holder’s name on it, so the security around the coin was virtually non-existent and almost anyone anywhere could use it. In response to the little to no security provided by charge coins, businesses in the 1930’s began using the more popular and reliable Charga-Plate.

Charga-Plate

The Charga-Plate was developed in 1928 and would remain in use in the United States until the 1950’s. The Charga-Plate was a small metal sheet that contained an individual’s name, city, and state and also had a small paper card on the back for the individual’s signature. When a customer would make a purchase, the metal plate containing the customer’s information was laid into a recess in the imprinter with a paper “charge slip” positioned on top of it. The transaction included a copy of the embossed information on the plate, made by the imprinter pressing an inked ribbon against the charge slip. The Charga-Plate was used mostly by very large department stores or merchants, and proved to help speed purchases and reduce errors in those purchases. However, the Charga-Plate wasn’t efficient or secure, and was quickly discarded for a more consumer friendly option.

¹Bellamy, Edward, and John L. Thomas. *Looking Backward, 2000-1887*. Cambridge: Belknap of Harvard UP, 1967. Print.

Air Travel Card

American Airlines and the Air Transport Association created the foundation of what would become the modern credit card. The card used a standardized set of numbers that was attached to issuer's name and the customer's account information. The Air Travel Card allowed passengers to "buy now, and pay later" for their airline tickets and receive a fifteen percent discount at any of the member airlines. All major airlines in the United States offered travel cards by the 1940's, and the Air Travel Card would become the first international charge card to be put into use by the late 1940's. In 1941, Air Travel Card agreements accounted for nearly half of all revenues for domestic airlines².

Invent of General Purpose Cards

Ralph Schneider and Frank McNamara, founders of Diner Club, created the concept of being able to use charge card across multiple retailers and stores. In 1958, American Express created the first worldwide credit card network, although initially used only charge cards, but would lay the foundation for the first universal network of general purpose cards.

Visa and MasterCard

Even with the invention of a general purpose credit card, there was no credit system established by a third party bank that could support a general purpose credit card, as opposed to the merchant system that had been used up until this point. In September of 1958, Bank of America established what would be the first worldwide credit system. "BankAmericard" was the first credit card launched that was supported by a third party bank, and is the first modern credit card. In 1977, BankAmericard changed its name to "Visa" and is now the most recognizable of all major credit cards.

What would become MasterCard was first established by a group of banks in 1966 as Master Charge in order to compete with the BankAmericard. Master Charge, as it was then known, gained significant credibility as a competitor when Citibank merged its "Everything Card" with Master Charge in 1969.

A significant problem had arisen in the late 1960's as a result of the invention of credit cards. Banks began mailing unsolicited cards to virtually everyone who was thought to be good credit risks. These mailings became known as "drops," and were outlawed in 1970 because they had caused financial chaos.

² Layton, Christine. "History Of The Credit Card." Credit Card Processing Space. Credit Card Processing Space, 14 Feb. 2013. Web. 22 Oct. 2014. <<http://www.creditcardprocessingspace.com/history-of-the-credit-card>>.

International Deployment of Credit Cards

In 1966, Barclaycard launched the first credit card outside the U.S in the U.K. In much of the world, however, credit cards are not used as often as is the U.S. and U.K. Most banks and countries in the world are more likely to use some form of debit card rather than credit cards.

Major Breaches of Credit Card Information

Credit card fraud has existed since credit cards themselves were invented. It is difficult to determine the exact numbers of early fraud. However in the new cyber age, identity theft and credit card theft is becoming an all too frequent problem for retailers and banks.

TRW/Sears

In 1984, a thief gained access to the credit histories of 90 million customers of the credit reporting company TRW via a Sears company on the West Coast³. While the organization was eventually tipped off about the thief, the thief had up to a month or more to use the information.

TJX Companies (T.J. Maxx)

From July 2005 to January 2007, a large security breach⁴ of TJX Companies' system led to the theft of 45.6 million credit cards. In October 2007, Court documents show that at least 94 million customers had their data and personal information compromised, twice the original estimate.

Heartland Payment Systems

The breach of Heartland Payment Systems is the largest in history⁵. In 2008, the credit and debit card information of an estimated 130 million users was hacked and accessed. Credits cards of all types were affected, and Heartland eventually paid \$110 million to Visa, MasterCard, and American Express and other card organizations for the breach.

Sony

Between April 17 and April 19 of 2011, Sony experienced a severe hacking of its systems⁶. Sony's PlayStation Network was hit the hardest, in addition to its streaming service Qriosity, with 77 million customers having their personal and credit card information stolen. Sony Online

³ Diamond, Stuart. "CREDIT FILE PASSWORD IS STOLEN." The New York Times. The New York Times, 21 June 1984. Web. 22 Oct. 2014. <<http://www.nytimes.com/1984/06/22/business/credit-file-password-is-stolen.html>>.

⁴ Jewell, Mark. "TJX Breach Could Top 94 Million Accounts." NBCNews.com. Associated Press, 24 Oct. 2007. Web. 22 Oct. 2014. <http://www.nbcnews.com/id/21454847/ns/technology_and_science-security/t/tjx-breach-could-top-million-accounts/>.

⁵ Vijayan, Jaikumar. "Heartland Data Breach Could Be Bigger than TJX's." ComputerWorld. ComputerWorld, 20 Jan. 2009. Web. 22 Oct. 2014. <<http://www.computerworld.com/article/2530582/cybercrime-hacking/heartland-data-breach-could-be-bigger-than-tjx-s.html>>.

⁶ Baker, Liana B., and Jim Finkle. "Sony PlayStation Suffers Massive Data Breach." Reuters. Thomson Reuters, 26 Apr. 2011. Web. 22 Oct. 2014. <<http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426>>.

Entertainment was also breached; however Sony reported that this breach only caused personal information, not credit cards, to be stolen.

Adobe Systems Inc.

In October 2013, Adobe Systems Inc. was breached and nearly 38 million customer accounts, including personal and credit card information, were stolen⁷. When Adobe first reported the breach, the company said that only 3 million customer accounts were hacked. Not only was the hacking more severe, but encrypted passwords to accounts were also stolen off of a separate server.

In November 2013, however, respected security blog Naked Security revealed that in fact 150 million customer accounts were hacked and stolen, and that Adobe had actually failed to encrypt customers' credit and debit cards on their accounts⁸. Adobe stands by the 38 million figure.

Target Corporation

From November 27 to December 15 of 2013, Target experienced a massive security breach that exposed the credit card and personal information of 70 million customers, nearly double the initial report of 40 million customers having their information compromised⁹. Among the information stolen from customers were customers' names, credit and debit card numbers, the expiration date of the cards, and the CVV (card verification value) of the cards.

Neiman Marcus

In January of 2014, Neiman Marcus reported that 1.1 million customers had their credit and debit card information compromised by malware on in-store computers¹⁰. The malware used in this attack was reportedly the same used in the attack against Target. MasterCard, Visa, and Discover reported that at least 2,400 cards were used fraudulently at Neiman Marcus and Last Call stores.

⁷ Finkle, Jim. "Adobe Data Breach More Extensive than Previously Disclosed." Reuters. Thomson Reuters, 29 Oct. 2013. Web. 22 Oct. 2014. <<http://www.reuters.com/article/2013/10/29/us-adobe-cyberattack-idUSBRE99S1DJ20131029>>.

⁸ Ducklin, Paul. "Anatomy of a Password Disaster - Adobe's Giant-sized Cryptographic Blunder." Naked Security. Sophos, 4 Nov. 2013. Web. 22 Oct. 2014. <<http://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/>>.

⁹ McGrath, Maggie. "Target Data Breach Spilled Info On As Many As 70 Million Customers." Forbes. Forbes Magazine, 10 Jan. 2014. Web. 22 Oct. 2014. <<http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/>>.

¹⁰ Harris, Elizabeth A., Nicole Perlroth, and Nathaniel Popper. "Neiman Marcus Data Breach Worse Than First Said." The New York Times. The New York Times, 23 Jan. 2014. Web. 22 Oct. 2014. <<http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html>>.

The Home Depot

In 2014, The Home Depot experienced a five month hack on its systems that compromised the credit card information of 56 million customers¹¹. The attack was malware upon its payment terminals that took five months to completely eliminate from its terminals.

JPMorgan Chase & Co.

In October 2014, JPMorgan Chase & Co. reported a breach of its systems that affected 76 million households and 7 million small businesses¹². Upon investigation, it showed that the personal information of customer accounts were stolen but the specific account information held by customers was not breached.

A report from the New York Times later showed that hackers were able to gain the “highest administrative privilege” on more than 90 servers of the bank. Jeff Williams, CTO of Contrast Security, said that the hackers “could transfer funds, disclose information, close accounts, and basically do whatever they want to the data.” The breach at JPMorgan Chase & Co. is the largest cyber-attack on a U.S. financial institution to date.

Staples, Inc.

Staples, Inc. is currently under investigation of its systems for a possible data breach of customers’ payment and credit card information¹³. Staples has contacted law enforcement officials to assist them in the matter, and have yet to determine if and how many customer accounts may have been affected by the attack.

Several banks, however, have already noticed a pattern of fraud occurring and alerted Staples, which has led to the investigation of a breach. Sources¹⁴ close to the situation told one reporter that several banks had "traced a pattern of fraudulent transactions on a group of cards that had all previously been used at a small number of Staples locations in the Northeast."

¹¹ Sidel, Robin. "Home Depot's 56 Million Card Breach Bigger Than Target's." The Wall Street Journal. Dow Jones & Company, 18 Sept. 2014. Web. 22 Oct. 2014. <<http://online.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571>>.

¹² Weise, Elizabeth. "JP Morgan Reveals Data Breach Affected 76 Million Households." News 10. ABC News, 6 Oct. 2014. Web. 22 Oct. 2014. <<http://www.news10.net/story/news/nation/2014/10/06/jp-morgan-reveals-data-breach-affected-76-million-households/16804947/>>.

¹³ Finkle, Jim, and Supriya Kurane. "Staples Says Probing Possible Payment Card Data Breach." Reuters. Ed. Edwina Gibbs and Gopakumar Warriar. Thomson Reuters, 21 Oct. 2014. Web. 28 Oct. 2014. <<http://www.reuters.com/article/2014/10/21/us-staples-cybersecurity-idUSKCN0IA0AA20141021>>.

¹⁴ Gilbert, David. "Staples Investigating Credit Card Fraud and Customer Data Theft." International Business Times RSS. IBTimes, Co., 21 Oct. 2014. Web. 28 Oct. 2014. <<http://www.ibtimes.co.uk/staples-investigating-credit-card-fraud-customer-data-theft-1471094>>.

Retail Cyber-Attacks: Exposure of Critical Infrastructure

Retail sponsored credit and debit cards are a common and necessary payment medium in the modern economy as they were with the concept of what would become a credit card. However, retail credit and debit cards have also exposed financial institutions and retailers themselves to become victims in the age of cybersecurity.

In a report¹⁵ released by the Deloitte Center for Financial Services on cyber breaches, the firm detailed an increase in the cost of cyber breaches to consumers and the increase in cyber-crime:

“U.S. financial services companies lost on average \$23.6 million from cybersecurity breaches in 2013, which represent the highest average loss across all industries. To underscore the rapid rise in cyber threats, this number is 43.9 percent higher than in 2012, when the industry was ranked third, after the defense and utilities & energy industries. While this trend is not to be ignored, these actual losses are sometimes not meaningful to firms’ income statements. The potentially greater impact from cyber-crime is on customer and investor confidence, reputational risk, and regulatory impact that together add up to substantial risks for financial services companies.”

Therefore bad actors have been using financial companies and retailers to target consumers and steal their personal and financial data. Much of the pain of the attacks is felt by the consumer and not the company that is actually breached. It is no secret that retail is the hardest hit of all cyber-attacks to date. Even payment processors such as Heartland Payments Systems have been exposed to hackers and other bad actors. Retailers have been subject to malware and credit card theft on a rampant basis, with little preventative measures anywhere to protect the consumer and the credit card network in which that consumer operates.

Credit Card Network Exposed

The current credit card network is relatively unsecure and exposes data theft to three separate parties: the bank, the retailer, and the consumer. Breach of one can cause breach of any other part of the network because much of the credential information is the same, without any technological support for increased security. Therefore any amount of data that may be stolen can subject any other part of the network to become a victim of fraud. As a result, retailers are threatened by attack because the data they hold is valuable, and their systems provide relatively no security to their consumer populous.

¹⁵ Transforming Cybersecurity: New Approaches for an Evolving Threat Landscape. Rep. Deloitte Center for Financial Services, 2014. Web. 5 Nov. 2014. <http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/FSI/us_fsi_Transformingcybersecurity_021114.pdf>.

With the recent hacking of JPMorgan Chase & Co., it has become apparent that financial institutions are open to the same type of attack and fraud as retailers. With this development, the credit card network, of which nearly every individual is connected to in some way, is now exposed and consumer data can largely be available to bad actors. Should any financial institution come under a worse attack in the future, the fallout could be worse than account holder information being stolen. If any account within an institution could be compromised, then all accounts are open to the same possible theft and exposure.

While a consumer's sensitive information can be held private at the user, it is a necessity that information be protected and secure within the institutions that the consumer's sensitive information is shared and stored. Data theft usually occurs when information is being transacted or shared between institutions and the user; therefore retailers have become the main target of financial cyber-attacks.

Retailers are not necessarily secure and they have minimum standards they must meet as a business. Retailers are not in the business of providing security but mainly in selling their own products, therefore they have no standard to abide by and thus leave the credit card network exposed unintentionally. By default, the role of retailers within the credit card network ultimately leaves the other two parties, the consumer and the bank, exposed to hacking and data theft.

Consumer Trust

Consumer trust is an underrated pillar of critical infrastructure. Consumers must be able to trust the businesses and institutions they interact and share personal data with. With the string of recent cyber-attacks, retailers and financial institutions have given the consumer little reason to trust that their information is secure.

Consumers, despite recent major cyber-attacks, have come to trust retailers and the other institutions they interact with because much of these institutions, such as JPMorgan Chase & Co., are "too big to fail," meaning that they could never just collapse without a step in from the government or other similar institutions. Such a mentality has allowed retail institutions to take advantage of their customers' trust and place security on the low end of their priorities.

Unfortunately, the consumer has had their information fall victim to bad actors because of the low standards and emphasis on security in the retail industry. Retail should not be blamed itself, but the other two parties of the credit card network, the banks and consumers, should be aware of this flaw in the network and create the standards necessary to provide security. Just because the internet is the medium being used to conduct business does not mean that the consumer forfeits their right to security.

Recent cyber-attacks have already begun to wither away at consumer confidence in the online marketplace, which can be devastating as we head deeper into the cyber age. A loss of confidence could cause all progress made in the cyber age up to this point to seize, especially if consumers drop out of the market place or decide not to use it as frequently due to the threat of breach.

End of the World Scenario

The philosophy of retailers and other institutions that could be the target of cyber-attacks and credit card fraud has been to ignore implementing extra and preventative security measures until the “end of the world” scenario takes place, meaning a major cyber-attack that attacks and disrupts major institutions and critical infrastructure at the same time.

Such an attack was depicted in the popular action film *Live Free or Die Hard*¹⁶, in which a small group of individuals were able to cripple all critical infrastructures of the government and financial institutions. Such a scenario is not impossible in the real world, and without the proper technological improvements to secure the credit card network, the end of the world scenario is inevitable.

Unfortunately, all three parties of the credit card network are guilty of waiting until the end of the world scenario takes place to care about cybersecurity. Cybersecurity for the network has not been a necessity yet, but recent events indicate that cybersecurity will soon be a market imperative. However, many businesses and even consumers will have the mentality that a breach of information won't and can't happen to them until it actually does. As always, at that point in the end of the world scenario, it is too late.

Response to the Breaches

The response to the cyber breaches at retailers and financial institutions have been highly inadequate. The only technological solution put forth is Chip and PIN in credit and debit cards in order to protect against fraud¹⁷, but such a solution will only protect against in-person fraud. Most fraud takes place over the Internet and the theft of hundreds of thousands of credit card data was not to produce fraudulent cards, but to be used on the Internet, and the Chip and PIN solution does nothing to fix that. Current security features in addition to new suggested technologies will only prevent fraud at the point of sale, a point which is diminishing as more fraudulent information is stolen and used over the Internet.

¹⁶ *Live Free or Die Hard*. Dir. Len Wiseman. Prod. Michael Fottrell. By Mark Bombback and David Marconi. Perf. Bruce Willis, Justin Long, and Timothy Olyphant. Twentieth Century-Fox Film Corp., 2007. Film.

¹⁷ Poulsen, Kevin. "Why the Heyday of Credit Card Fraud Is Almost Over | WIRED." *Wired.com*. Conde Nast Digital, 23 Sept. 0014. Web. 31 Oct. 2014. <<http://www.wired.com/2014/09/emv/>>.

Security Features of Major Credit Cards¹⁸

The following section on the security features of individual credit cards is provided entirely by the footnoted source.

Visa

- Account numbers begin with a “4.”
- The four digit number printed below the embossed account number must match the first four digits of the account number.
- A three dimensional dove hologram should reflect light and seem to change as you rotate the card.
- The magnetic stripe on the back of the card should appear smooth and straight with no signs of tampering.
- All Visa cards must be signed before they are valid.

MasterCard

- Account numbers begin with a “5.”
- The preprinted Bank Identification Number (BIN) must match the first four digits of the embossed account number.
- The valid date lists the last day on which the card is valid.
- MasterCard cards have a stylized “MC” security character embossed on the right of the valid dates.
- The back of the card must be signed.
- A three dimensional hologram of interlocking globes should reflect light and seem to change as you rotate the card.
- The magnetic stripe on the back of the card should appear smooth and straight with no signs of tampering.
- The word “MasterCard” is printed repeatedly in multi-colors at an angle on a tamper-evident signature panel.

¹⁸ "What Are the Security Features on a Credit Card?" Pogo Payment. First Data Corporation, n.d. Web. 31 Oct. 2014. <<https://www.pogopayment.com/pogo/www/home/faq/what-are-the-security-features-on-a-credit-card-.html>>.

American Express

- Only the person whose name is embossed on the card is entitled to use it.
- All American Express card numbers begin with “37”.
- The card cannot be accepted for use after its expiration date.
- The portrait of the Centurion is printed with great detail.
- The account number embossed on the front of the card must be exactly the same as the number printed on the back of the card.
- The letters AMEX and phosphorescence in the Centurion portrait are visible when the card is examined under UV light.
- The preprinted CID should always appear above the account number.
- Check to ensure the security panel has not been tampered with.
- All American Express Card types will bear the security features.

Discover

- Under UV light, the word “Discover” will appear on the front of the card.
- All Discover account numbers begin with “6011.”
- The special embossed Security Character appears on the same line as the “Member Since” and “Valid Thru.”
- The “Valid Thru” date indicates the last month in which the card is valid.
- The three-dimensional hologram should reflect light and appear to move as you rotate the card.
- The account number printed on the signature panel and encoded on the magnetic stripe should match the account number embossed on the face of the card.
- The account number on the signature panel appears in reverse indent printing.
- Depending on the date of the card, there might be an overprint pattern on the signature panel.

Credit Card Fraud Prevention: Failed Industry Solutions

The credit card industry and network has yet to provide a secure payment infrastructure that secures the consumer, the retailer, and the bank. The most recent “innovation” for credit cards is to start requiring Chip and PIN protection, which only prevents in-person fraud and does little to stop fraud in the cyber age.

Past solutions have failed to change the dynamic of security for consumers, and the concept of increasing “depth security” has failed to stop bad actors. Depth security never truly provides additional security to the consumer or user. Depth security is like putting another lock on a cabinet, the thief now only has to take extra time to cut the second lock, and does nothing to stop the thief in the first place and protect valuable content.

Beyond each major credit card having its own physical features to provide some security at purchase, there have been other efforts to introduce new technology and verification methods in order to prevent fraud at purchase and over the internet. Each solution that has been offered and put forth on the market has done nothing to stop the recurrence of fraud and cyber-attacks on customers’ personal and financial data.

PAN Truncation

The PAN Truncation is used by merchants as a fraud countermeasure at the point of sale (“PAN” stands for “primary account number”)¹⁹. PAN Truncation countermeasure replaces the account number on receipts with asterisks, except for the last four digits, allowing only the holder of the credit card to be able to identify the specific card used.

The method was initially used on receipts from in purchase sales to avoid fraud from lost or misplaced receipts. The same method has carried into the digital age when sending order confirmations via email or on the web browser. However, Visa suggests merchants only print the PAN Truncation on the receipt at the point of sale and to not store the data. Visa noted that the storage of such data can be harmful to users over the internet.

Visa also acknowledged that there is a better way to store or authenticate PANs without the need for printing the account numbers on a receipt or confirmation. “Acquirers should enhance their systems to provide merchants with substitute transaction identifiers... or software tokens to facilitate retrieval of transaction data stored by the acquirer, in lieu of using the PAN as a reference for individual transactions.”

¹⁹ “Visa Best Practices for Primary Account Number Storage and Truncation.” (n.d.): n. pag. Visa.com. Visa, 14 July 2010. Web. 3 Nov. 2014. <http://usa.visa.com/download/merchants/PAN_truncation_best_practices.pdf>.

Request of Additional Information

The “request for additional information” solution usually requires the card user to authenticate at point of purchase by a request of additional information, usually a pin code, zip code, or challenge question.

Debit cards, for example, typically require the use of pin code at the point of purchase in order to verify the user’s transaction. However, the pin code solution fails when transactions are conducted over the internet because online transactions do not require the use of pin code. In an online transaction, the card holder is typically verified by a billing address or zip code. In this scenario as well, security is not guaranteed because address and zip code information is easy to obtain and is typically the information most often stolen in cyber-attacks (see JPMorgan incident, pg. 11). In addition, the verification information requested typically exists in other parts of the Internet, such as a public Facebook profile or a business profile. With that information readily available, bad actors are more encouraged and able to steal consumers’ personal and financial data via the Internet.

Challenge questions are typically used by banks, such as PNC, in order to sign on into a user’s account online via the web-browser. Challenge questions are even less secure than requiring a user to submit a username and password. The chances of guessing the challenge question, or the information being stolen and used in a fraud incident, are much greater and put the account holder’s personal and financial information at great risk. Due to the lack of technological security barriers, accounts are exposed to essentially any hacker with an internet connection because the login information is not secure and neither is the medium by which to attain that information.

Falcon Fraud Prevention Software

The first fraud prevention software was “Falcon Fraud Manager,” launched by HNC Software in 1992²⁰. Falcon was a software program aimed at preventing fraud for credit card transactions by using specific analytics to detect fraud and halt it. Falcon runs about 15,000 calculations when a credit card is swiped in order to calculate whether or not that purchase is fraudulent. In 1993 the Falcon program was modified to include neural network models, which are designed like the human neural network in order to detect fraud that was not connected through linear equations and also examined purchases for hidden variables and well disguised fraud.

²⁰ Horan, T.J. "Evolution of Fraud Analytics – An Inside Story." KDnuggets Analytics Big Data Data Mining and Data Science. KDnuggets, 14 Mar. 2014. Web. 03 Nov. 2014. <<http://www.kdnuggets.com/2014/03/evolution-fraud-analytics-inside-story.html>>.

In 1999, Falcon introduced e-commerce fraud modeling to respond to the growing need to protect online transactions during the internet boom. The e-commerce fraud modeling was designed to protect merchants from card-not-present fraud, mainly when conducting online transactions.

As e-commerce expanded, Falcon expanded its e-commerce fraud modeling software to include outlier models in 2005, increasing the precision of detecting e-commerce fraud by examining unusual payment incidents and other outlier transactions. In the following year, Falcon expanded its fraud modeling software to also include first-party fraud modeling, which recognizes when people are committing fraud under their own identities. In 2008, Falcon followed up with self-calibrating technology that allows the Falcon anti-fraud software to adapt itself in real-time to detect fraudulent transaction trends. Self-calibration allows for the program to detect fraudulent payments when no historical models of fraudulent transactions may be available.

In 2009, Falcon's software instituted global intelligent profiles identify high risk ATMs, retailers, and regions and apply extra scrutiny when and where fraud is most likely to take place. These profiles provide the prevention software with data of regions which contain the most fraud and allow the program to pinpoint the data necessary for review. Adaptive analytics added to the software in 2010 enables analytic software to adjust models as fraud patterns change within the high risk regions and if there is a shift in high risk regions. As technology develops and bad actors become more sophisticated, these analytics allow for the software to adapt based on hard data and to follow fraud trends to their roots.

Behavioral sorted lists were incorporated in 2013 to improve the ability of the software to identify suspicious transactions by building a more accurate profile of the consumer's likely behavior. The software helps pinpoint a user's likely behavior, such as the websites they visit, purchase goods from, or the location geographically of such purchases.

Falcon has had positive impact by contributing to the reduction of the overall amount of fraud from .18 percent of all payment card purchases in 1992 to .05 percent of all payment card fraud in 2014. However, these numbers only reflect the reduction of overall in person fraud and not fraud conducted over the Internet with payment information or other payment methods.

Falcon can't take credit for this overall reduction in fraud because this number doesn't reflect e-commerce or breach of card information by cyber-attacks. Most fraud in the cyber age is theft of personal and financial data from servers by malware, which essentially counters anything the Falcon software can do to prevent fraud. As seen with the recent cyber-attack on The Home Depot (see The Home Depot incident, pg. 11), malware has the ability to still steal consumer credit card data at point of purchase, regardless of what fraud prevention software is put in place

to keep the servers or terminals safe. In that instance alone, 56 million credit card holders had their information and data compromised.

Falcon doesn't do anything as software to actually prevent fraud; it only detects fraud and halts the continuation of fraud. At this stage, the personal and financial information of the consumer has already been compromised and can't be salvaged. Falcon does nothing as a technology to prevent fraud before it happens and also doesn't provide security to the consumers who interact with the software. As mentioned in the section on recent major cyber-attacks, malware was able to disable any software based defenses the servers or terminals had, and was able to infect terminals for up to five months before being completely eliminated from the terminals. Falcon has no preventative measures to halt in-person fraud or protect the consumer data shared between the networks Falcon is supposed to be protecting.

A software based solution will never provide security to the consumer or the credit card network because all software is subject to attack and infection of malware. In addition, the Falcon software does nothing to protect against cyber-attacks via the web-browser or the Internet in general. In the majority of cyber-attacks, consumer data was not stolen at the point of purchase. Falcon software can't protect against the theft of consumer information, it can only indicate when fraud has already occurred and that's assuming that hackers aren't sophisticated enough to combat the software. The recent string of cyber-attacks proves that the Falcon software, and other similar technologies, are incapable of protecting the consumer and preventing fraud.

Card Security Codes (CSCs)

There are several different types of card security codes utilized by credit card companies to prevent credit card fraud when conducting "card not present" transactions, such as transactions via the Internet:

- Card Security Code (CSC) (debit cards)
- Card Identification Data (CID) (used by Discover and American Express)
- Card Verification Number (CVN)
- Card Verification Value (CVV or CVV2) (used by Visa)
- Card Verification Value Code (CVVC)
- Card Verification Code (CVC or CVC2) (used by MasterCard)
- Verification code (V-code or V code)
- Card Code Verification (CCV)
- Signature Panel Code (SPC)

Each subsequent type of code is in some way similar to the other. Each security number or code is printed on the card which is being used in the transaction. MasterCard was the first major

credit card issuer to use CSCs in 1997. American Express issued CSCs on their cards in 1999 due to the increasing amount of online transactions in the early era of the Internet, and by 2001, Visa was issuing CSCs on their cards for increased security.

The benefit of the CSCs is that it is another piece of information hackers must obtain in order to complete an online transaction. In addition, merchants and online payment systems are prohibited from storing CSCs in online or any other databases.

However, not all merchants require the CSC code to be used in an online transaction. In addition, many third party payment processors store credit or debit card information online to be used in additional transactions to save time for consumers when submitting an order via the Internet. When using a saved payment method, consumers are rarely, if ever, asked to verify the card being used. Therefore, CSCs do not necessarily protect against card-not-present transactions and online transactions.

CSCs do not protect against cyber-attacks and fraudulent incidents over the Internet, where the majority of recent bad actor activity has been conducted. Card security codes also do very little to prevent against in person fraud, for there is no way for the retailer to verify the code on the magnetic strip of a stolen card, and the CSC is already present on the card, leaving no way to verify the card and the user. CSCs cannot be trusted to verify transactions or protect consumer data that is stored or conducted over the internet. There are no technological security measures to protect the consumers' information or prevent fraudulent activities, rendering the credit network no better protected and vastly exposed.

EMV Chip and PIN Credit/Debit Cards

EMV²¹ is an international standard organization that promotes Chip and PIN technology for credit and debit cards. The EMV standard promotes the use of EMV compliant cards with EMV compliant terminals in the world, standardizing credit card security and standardizing Chip and PIN practice in preventing credit card fraud. EMV changes the verification method from a magnetic strip and visual verification of a signed card to EMV chip cards containing embedded microprocessors that provide increased security measures to transactions used at a compliant terminal for maximum security effectiveness.

EMVCo, the organization that manages EMV chip standards, is owned by American Express, Discover, JCB, MasterCard, UnionPay, and Visa, and also includes other organizations from the financial industry that are included as business associates. Financial institutions and card issuers have been pushing for increased use of EMV Chip and PIN cards in addition to compliant

²¹ "EMV Chip Payment Technology: Frequently Asked Questions." SmartCardAlliance.org. Smart Card Alliance, n.d. Web. 04 Nov. 2014. <<http://www.smartcardalliance.org/resources/pdf/EMV-FAQ-update-012814.pdf>>.

terminals in order to shift liability away from the banks and card issuers to merchants and retailers.

Eighty countries globally are in various phases of EMV chip integration into credit/debit card security measures. EMVCo reports that roughly 1.62 billion EMV chip cards have been issued and in use worldwide as Q4 of 2012. As of that same time, 95 percent of terminals in parts of Europe were EMV compliant, in addition to 79 percent of terminals in Canada, Latin America and the Caribbean, 77 percent in Africa and the Middle East, and 51 percent in Asia Pacific were EMV compliant.

The United States is one of the last countries to integrate EMV Chip and PIN protected credit/debit cards. In August 2011, Visa became the first card issuer to begin moving towards EMV Chip and PIN protection in the United States. By June of 2012, MasterCard, Discover, and American Express have announced plans to migrate EMV Chip and PIN credit/debit cards in the United States. Each card issuer has created a timeline by which to implement EMV Chip and PIN protection to credit/debit cards, with each timeline assuming majority migration to the new technology by 2015.

On October 17, 2014, President Obama signed an executive order²² creating the BuySecure Initiative, a program by which the federal government will completely switch over to exclusively using EMV Chip and PIN credit/debit cards by government employees. By 2015, the White House plans to issue over 1 million “more secure” credit/debit cards to government employees, aimed at combating identity theft and fraud in the use of federal dollars. The White House hopes that the initiative will encourage private industry to follow suit and institute EMV Chip and PIN credit/debit cards as the industry standard for cybersecurity and protection against fraud.

The first line of security in an EMV card is a unique microprocessor chip that stores data on the card security protected by PIN and also performs cryptographic processing when a transaction is being made. EMV chips also contain security credentials that are personalized to the chip when the card is initially issued that also verifies the card’s authenticity during a transaction. EMV cards are authenticated by the cardholder by one of four different card verification methods (CVM):

- Online PIN, where the PIN is encrypted and verified online by the card issuer
- Offline PIN, where the PIN is verified offline by the EMV card
- Signature verification, where the cardholder signature on the receipt is compared to the signature on the back of the card

²² United States of America. Executive Office of the President. Office of the Press Secretary. FACT SHEET: Safeguarding Consumers’ Financial Security. The White House, 17 Oct. 2014. Web. 04 Nov. 2014. <<http://www.whitehouse.gov/the-press-office/2014/10/17/fact-sheet-safe-guarding-consumers-financial-security>>.

- No CVM, where none is used (typically for low value transactions or for transactions at unattended POS locations)

The second security feature of EMV chip credit/debit cards is that the chip and terminal analyze dynamic data, whether the purchase is online or offline, and then determines the risk of fraud based of the card issuer's database and determine of risk.

The third security feature is designed to stop fraud in the event of theft of data and information from the chip. If bad actors are able to steal consumer account data from chip transactions, the data from the chip cannot be used to create a fraudulent transaction in an EMV or magnetic stripe environment since every EMV transaction carries dynamic data that must be authenticated with the original chip issued. EMV chip credit/debit cards can also prevent against card-not-present fraud by using individual readers to authenticate transactions made via the Internet.

Countries that have implemented EMV Chip and PIN protected credit/debit cards have reported an overall decrease in credit card fraud. According to the UK Card Association, "Fraud on lost and stolen cards is now at its lowest level for two decades and counterfeit card fraud losses have also fallen and are at their lowest level since 1999. Losses at U.K. retailers have fallen by 67 percent since 2004; lost and stolen card fraud fell by 58 percent between 2004 and 2009; and mail non-receipt fraud has fallen by 91 per cent since 2004."²³

However, the UK Card Association report is also very misleading the success of EMV chip cards in preventing online credit/debit card fraud. The report also details that online fraud increased in 2009 by 14 percent and online fraud is mostly likely to increase in subsequent years, following the same trend as it has. The report attributes the increase in online fraud to bad actors increasing their malicious capabilities and also to malware that infects terminals at the point of purchase. The report was also published previously to most of the major cyber-attacks on retailers, which began primarily after 2010.

EMV Chip and PIN credit/debit cards are not secure and don't provide additional security to consumer, retailers, and banks. The majority of current EMV Chip and PIN credit/debit also have magnetic strips on them in order to allow the cards to be compliant with retail and banking terminals that don't have the ability to read and process EMV chips. Therefore, even if a credit/debit card has an EMV chip on it, it doesn't provide security during transactions unless an EMV compliant terminal is being used to process the transaction. The magnetic strip on the card is essentially a back-door for bad actors to commit fraud using credit/debit cards by replicating the magnetic strip even on EMV cards. The security features of each EMV chip being unique

²³ "New Card and Banking Fraud Figures." TheUKCardAssociation.org.uk. The UK Card Association, 10 Mar. 2010. Web. 4 Nov. 2014. <<http://www.theukcardsassociation.org.uk/news/new-card-banking-fraud-figures.asp>>.

means nothing and provides no security as long as the replicable magnetic strip remains on the credit/debit card.

Researchers at Newcastle University in the United Kingdom have also found that online and offline fraud is actually accomplished easily with EMV chip cards. Martin Emms, lead researcher on the project studying the EMV technology, was able to exploit the EMV Chip and PIN cards without raising awareness of fraudulent activity:

“With just a mobile phone we created a POS terminal that could read a card through a wallet. All the checks are carried out on the card rather than the terminal so at the point of transaction, there is nothing to raise suspicions. By pre-setting the amount you want to transfer, you can bump your mobile against someone’s pocket or swipe your phone over a wallet left on a table and approve a transaction. In our tests, it took less than a second for the transaction to be approved.”²⁴

EMV Chip and PIN cards have essentially enabled bad actors to commit more fraud because mobile card verification methods are easy to complete as long as the bad actor is in the vicinity of an EMV chip credit/debit card. Theft or creation of a fraudulent card isn’t necessary because the bad actor can essentially conduct small amounts of fraud that won’t raise suspicion to the bank or even the consumer. EMVCo has pointed to individual payment processors has an additional security feature that help verify online/offline transactions or transactions conducted over the internet. In contrast to this claim, mobile and individual payment processors are actually security vulnerabilities and expose consumer financial data.

The same researchers found that the EMV Chip and PIN cards couldn’t detect foreign currencies and therefore transactions with foreign currencies don’t require a PIN entry and were not flagged for suspicion. Essentially, the fraudulent transaction is verified due to the EMV Chip and PIN security measures because bad actors need only create a POS terminal by which to charge the card. “All a criminal would need to do is set up somewhere like an airport or the London underground where the use of different currencies would appear legitimate,” said Emms. The card itself is physically present and active at the terminal location, raising no suspicion of a fraudulent transaction under current banking protocol. “It is not clear from reading the payment protocol how banks would deal with the inconsistencies we have found through our research, hence we believe the vulnerability poses a potential threat. The fact that we can by-pass the £20 limit makes this new hack potentially very scalable and lucrative,” said Emms. There is little evidence to support the claim that consumers, banks, and retailers are more secure by using EMV Chip and PIN credit/debit cards.

²⁴ Emms, Martin, Budi Arief, Leo Freitas, Joseph Hannon, and Aad Van Moorsel. "Contactless Cards Fail to Recognise Foreign Currency." Ncl.ac.uk. School of Computer Science, Newcastle University, 1 Nov. 2014. Web. 03 Nov. 2014. <<http://www.ncl.ac.uk/press.office/press.release/item/contactless-cards-fail-to-recognise-foreign-currency>>.

Vir-Sec® SecureAccess™ Solution

Vir-Sec, Inc. is the first company to introduce a dynamic cyber infrastructure that can protect all aspects of the credit card network against fraud, identity theft, and cyber-attacks. Vir-Sec's patented technology is the first of its kind and the future of security and communication in cyberspace.

Vir-Sec's SecureAccess™ solution seeks to accomplish two objectives:

1) Multifactor Authentication

- The goal of multifactor authentication is to virtually eliminate a hacker's ability to pose as the authorized user of the credit/debit card when conducting transactions via the Internet.

2) Security for the User and Application

- The concept of security must be centered on the idea that the interactions and communications of the user must be insulated from outside influences in cyberspace. When a user connects and sends a payment, either at a POS terminal, an offline terminal, or online via the Internet, that data transfer must be kept secure and only visible by the parties which are communicating.

Both objectives provide the basis for Vir-Sec's technology and approach to cybersecurity. In the instance of financial transactions and credit/debit cards, Vir-Sec's technology is the only market available solution that protects all aspects of credit card data.

Multifactor Authentication

Up to this point, a consumer's financial data in an Internet banking environment is only protected by single factor authentication: a username or password, or in some instances, a username and a challenge question. Single factor has been largely disqualified in providing adequate security by industry standards and by government standards. In a report²⁵ on authentication in the Internet banking environment first published in 2001, the Federal Financial Institutions Examination Council (FFIEC) stated that single-factor security does not defend against cyber-attacks and also can't prevent fraud via the Internet or in-person.

“The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Financial institutions offering Internet-based

²⁵ Authentication in an Internet Banking Environment. Report. Federal Financial Institutions Examination Council, n.d. Web. 4 Nov. 2014. <http://www.ffiec.gov/pdf/authentication_guidance.pdf>.

products and services to their customers should use effective methods to authenticate the identity of customers using those products and services. The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.”

Therefore, by financial industry standards, online banking environments are inherently unsecure because each environment is protected only by single factor authentication. Financial institutions will argue their environments have their own layered security to secure the online banking environment, but this “security” does not protect the consumer and it can’t protect against fraud or identity theft once an identity has been stolen.

In addition, there is no way to verify that the user logging into the online banking environment is the owner of the account being accessed. Without a physical presence identifier or any method of verifying that the account user is online while a transaction is being made, consumers are generally exposed to having their information and financial data stolen and used maliciously.

Vir-Sec has incorporated *true* multifactor authentication into its technology and also as a cornerstone of its cyber infrastructure. Vir-Sec’s multifactor authentication process includes “something you have,” a physical presence identifier, and “something you know,” a piece of information known only to the user to authenticate their identity. Vir-Sec’s technology not only incorporates these factors, but enhances their effectiveness with new technologies to support a strong and accurate identification process.

Through these factors and technological innovations, Vir-Sec has created an infrastructure that utilizes multifactor authentication in a consumer friendly aspect while still guaranteeing overall security to the user, financial institution and retailer. The infrastructure, both the physical and virtual aspect, ensure that each time a user logs into their account, their identity and credentials are not only verified but also secure from cyber-attacks while data is being shared between servers.

➤ *“Something You Have”*

Vir-Sec’s technology provides true multifactor authentication in preventing fraud in-person, online, and during card-not-present transactions. Vir-Sec’s technology accomplishes the first factor of authentication, “something you have,” by using a distributable medium, the SecureAccess™ token or “Key”, by which to physically identify the user’s physical presence and status online. The SecureAccess™ token is a custom designed USB device that can be utilized by any USB accepting system or device.



▪ Figure 1

Figure 1 visually represents the Vir-Sec SecureAccess™ token that each consumer would own. Each Vir-Sec SecureAccess™ token is unique, each with its own encryptions and cryptography that can only be accessed by the corresponding user. The tokens, however, are not linked to the user’s personal or financial information and, in the event of a lost or stolen token, can be remotely destroyed rendering it unable to be used. In addition, the individual consumer’s information is not stored on the SecureAccess™ token, meaning that mere possession of the token does not allow a hacker to be able to access any of a consumer’s personal information or data.

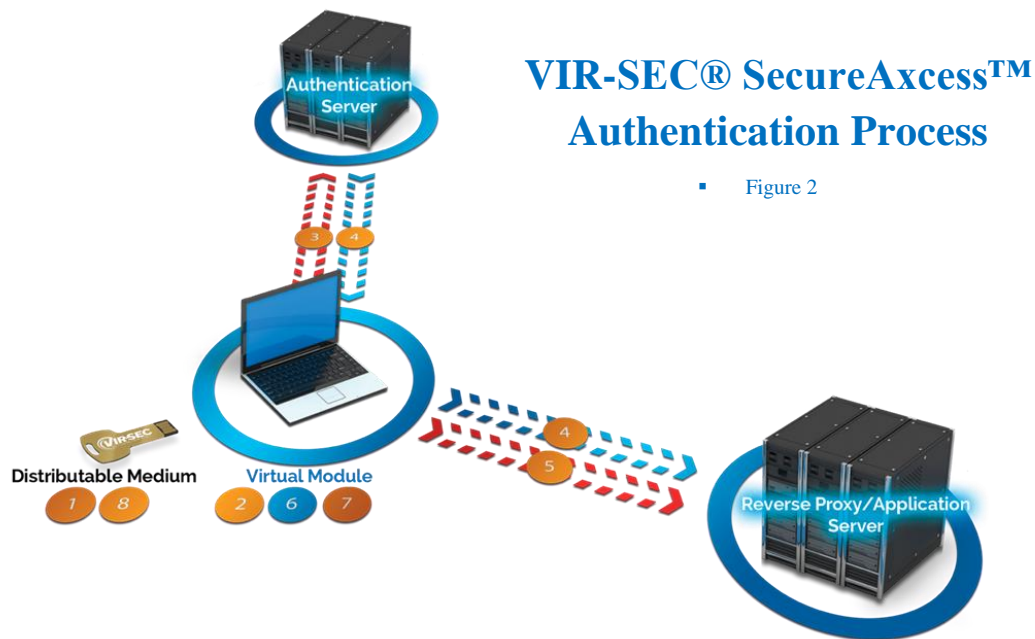
In fact, nothing is ever stored on the Vir-Sec SecureAccess™ token at any time except the hardware needed in order to connect to the internet and necessary applications of the credit card network. Unlike EMV Chip and PIN cards, which contain a consumer’s personal and financial information, Vir-Sec’s SecureAccess™ token contains only the technology necessary to safely and securely conduct transactions via the internet. The possible theft of the physical object, in this case the SecureAccess™ token, instead of a credit/debit card, would not expose the consumer to identity theft or fraud, as possession of the device means absolutely nothing without the other steps to authenticate.

The SecureAccess™ token is essentially a distributable medium by which to connect and authenticate to the requested applications. The device does not contain any specific information except its unique serial key and unique cryptography, which would mean nothing to any bad actor should the token be lost or stolen. In addition, no information regarding any virtual session the user constructs exist on the SecureAccess™ token. No one and no program can decipher how many times the token has been used or even who it belongs to because that information is not available on the token.

➤ “Something You Know”

Vir-Sec incorporates the most common way for authentication into its multifactor authentication structure. The “something you know” factor is the second step in authenticating for the consumer, both physically and virtually. Figure 2 details the entire process of authentication of the SecureAccess™ token, the user, and the application.

- 1) The SecureAccess™ token is inserted into the virtual module (laptop, desktop, POS terminal, etc.), by the user.
- 2) An Open SSL connection is established by the token to Vir-Sec’s authentication server that is off-site and maintained by Vir-Sec. Vir-Sec’s Virtual Environment Application (VEApp) then constructs a unique virtual session from RAM on the SecureAccess™ token. The authentication server verifies the SecureAccess™ token’s unique serial key and unique coding, verifying that the key is physically connected to a USB connecting device and that the SecureAccess™ token is online.



- 3) The SecureAccess™ token then sends a challenge request to Vir-Sec’s off-site authentication server.
- 4) The authentication server verifies the challenge request, encrypts the request, and then sends the request to the requested application server (online banking environment, etc).
- 5) The user then authenticates to the requested application, such as an online banking environment.
- 6) The user authenticates with their credentials to the application. The requested application is then constructed within SecureAccess™, with Vir-Sec’s authentication server sending constant “keep alive” messages between the SecureAccess™ token, application server,

and the authentication server. The user is then allowed to conduct transactions, make purchases, and any other activity that the application permits.

- If at any time during the VEApp session any part of the authentication network is disrupted (SecureAccess™ token removed, application server compromised, etc.), the VEApp closes and the session is completely destroyed, leaving no foot print anywhere.
- 7) When the user is finished, the SecureAccess™ token is removed from the virtual module and the session collapses, leaving no trace of existence on the virtual module or the SecureAccess™ token.

The full authentication process ensures security of the user's identity, individual online transactions, and security of web applications. Vir-Sec's cyber infrastructure is dependent upon each pillar of authentication: the token, the user, the VEApp, the authentication server, and the web application server. If any one of these pillars is interrupted or removed, the entire session collapses and is rendered unusable and inaccessible. In doing so, the consumer can trust that their personal and financial information is secure at all times, because without each pillar engaged, active, and verified at the same time, none of the consumer's information is open to attack or theft.

Virtual Environment Application (VEApp)

While some companies have instituted some sort of tokenization or form of multifactor authentication, Vir-Sec's SecureAccess™ solution is the only solution available that uses technological innovations to make multifactor authentication secure. Vir-Sec's patented Virtual Environment Application (VEApp) is a patented technology that, simply, is a container that contains nothing and can be remotely destroyed leaving no trace. It is the only application that is purely virtual and non-existent on hardware.

Figure 2 illustrates the construction of the VEApp and its important role in the process of authentication and security when online. When the user inserts the SecureAccess™ token into the virtual module, the VEApp constructs and once the authentication server verifies the SecureAccess™ token is online, the user authenticates and is then connected to the web application within the VEApp. VEApp therefore provides a completely secure environment for the user to communicate and operate within.

SecureAccess™ is a complete revolutionary technology that does not require a web-browser or software to use web applications. The VEApp allows users to connect to any application server and use that application normally within an entirely virtual session. By doing so, Vir-Sec has removed the two main points of cyber-attacks: the web-browser and software applications. The VEApp is an impenetrable silo that protects the user when communicating with applications

online. Because each VEApp virtual session is completely unique and does not exist until constructed in RAM once the SecureAxxcess™ token is inserted into the virtual module, bad actors cannot use the VEApp as a medium to conduct a cyber-attack on a server or terminal to steal a consumer’s personal and financial information.

Vir-Sec Virtual Environment

- 1 Browser-less connection
- 2 Multi factor authentication
- 3 Virtual application session in RAM, with no disc operation
- 4 Session ends immediately with no trace on local computer or path to server

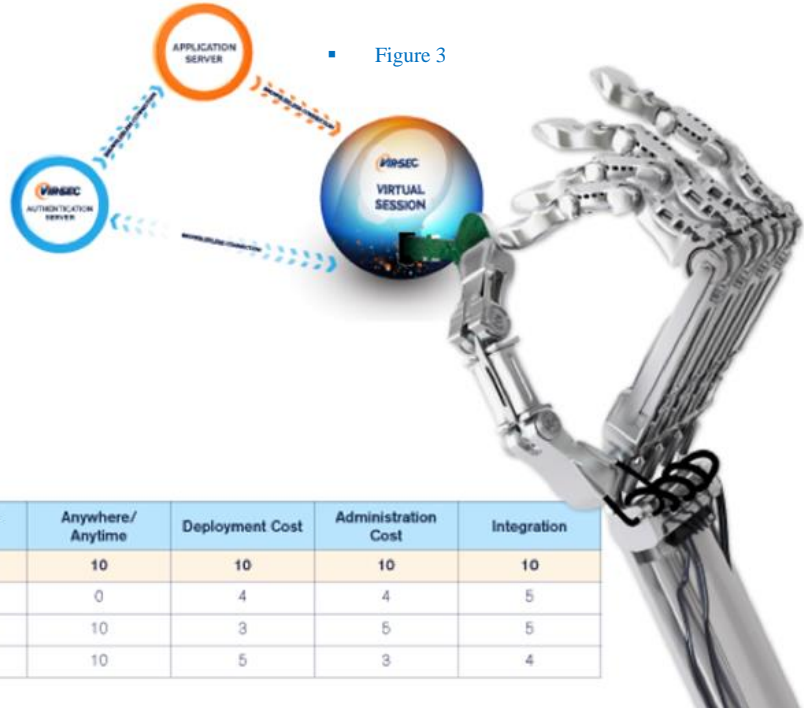


Figure 3

Multi-Factor Security Technology Comparison (10=Best)

| Technology | Strength | Browseless Internet | Anywhere/ Anytime | Deployment Cost | Administration Cost | Integration |
|---------------------------|----------|---------------------|-------------------|-----------------|---------------------|-------------|
| Key + Virtual Environment | 10 | 10 | 10 | 10 | 10 | 10 |
| Embedded Hardware | 8 | 0 | 0 | 4 | 4 | 5 |
| Hardware Token | 8 | 7 | 10 | 3 | 5 | 5 |
| Software Token | 8 | 0 | 10 | 5 | 3 | 4 |

Unlike web-browser applications or software based terminals, which basically allow anyone with an internet connection to access a web application’s server containing millions, if not billions, of consumers’ data and personal information, the VEApp is never constantly engaged on a device, and only the user authenticated on the virtual module can view the virtual session being used. Any other user authenticated and online at the same time is operating within their own unique virtual session, and therefore is secure from other users’ activity and secure from cyber-attacks by bad actors.

Since the VEApp requires that the user first authenticate to Vir-Sec’s authentication server, bad actors are prevented from using the VEApp without first authenticating the specific SecureAxxcess™ token and the account information connected with it. Each pillar of authentication makes in-person fraud near impossible and makes fraud and identity via the Internet next to impossible. The VEApp allows users to conduct safe transactions of data via the internet without exposing it to anyone but the user and web application the user is connected to.

SecureAccess™: The Next Generation of Credit/Debit Card Security

Vir-Sec's patented SecureAccess™ technology is the future of credit and debit card security. Major card issuers, such as Visa²⁶, have already instituted programs to offer token services to provide security for credit/debit cards. While these programs are moving the industry in the right direction, the technology of these tokenization programs cannot match the level of security of the SecureAccess™ solution. The technological innovation Vir-Sec has created is completely revolutionary. Vir-Sec holds the patent on all Virtual Environments, therefore Vir-Sec can verify that the only solution offered that utilizes complete virtual security in cyberspace is SecureAccess™.

Vir-Sec's SecureAccess™ can be deployed to the current market and provide consumers with complete security when conducting transactions online and connecting to online banking environments. SecureAccess™ does not require a complete overhaul of current technology to operate and can innovate technological cybersecurity simply by deploying SecureAccess™ to consumers and providing them the proper environment to operate within.

SecureAccess™: Future of Credit/Debit Cards

As the technological timeline advances, card issuers are realizing that tokenization is inevitable and are instituting their own programs to offer such services. Vir-Sec is already ahead of that timeline and offering the market a solution that is far beyond simple token verification.

SecureAccess™ is a complete cyber infrastructure that secures every aspect of the credit card network at every possible point. SecureAccess™ is the only solution available that offers both physical and virtual security, protecting the consumer, the retailer, the bank, and transactions at all possible vulnerabilities.

In addition, retailers need only have terminals that have a USB port in order to migrate their systems to accept SecureAccess™ tokens as credit cards. The POS terminal does not need any software on it to process the payments because that transaction would be conducted within the VEApp and communicated between the remote authentication and web application servers that process the payments between the retailer and customer's bank. Since no software or hardware is needed on the POS terminals for the user to authenticate and conduct a transaction, cyber-attacks by malware are impossible. In addition, the terminals are no longer a medium by which to steal consumer data and information because each time a USB credit/debit card is inserted into the terminal, a completely unique virtual session is constructed, protecting the user from bad actors.

²⁶ "Visa Launches Innovative Token Service." Visa.com. Visa, Inc., 09 Sept. 2014. Web. 05 Nov. 2014. <<http://investor.visa.com/news/news-details/2014/Visa-Launches-Innovative-Token-Service/default.aspx>>.

Card issuers need only adopt Vir-Sec's SecureAcess™ tokens in order to implement the solution for their credit/debit cards. All consumer and account information is store remotely on the application server; therefore, card issuers need only assign consumers a Vir-Sec SecureAcess™ token and create a username and password for the token. Beyond that, SecureAcess™ can incorporate every application needed to process a transaction between a retailer and a bank in-person and online.

With Vir-Sec, banks can now provide secure connections to their online banking environments without fear of cyber-attacks via malware or the web-browser. Both avenues of attack are eliminated and banks can assure their customers that their information is private and secure.

Conclusion

Vir-Sec has concluded that current industry solutions are inadequate in providing security to the credit card network. Under current industry standards, the consumer, retailer, and financial institutions are exposed to fraud and cyber-attacks on a constant basis. Other proposed solutions have been invalidated as providing security in the cyber age. Following the history of credit cards, their technological improvements, and recent history of cyber-attacks writes its own narrative of failed solutions that don't solve fraud and identity theft problems, but rather shift liability from one party to another. The deployment of EMV Chip and PIN in conjunction with SecureAcess™ can provide security to consumer in person and online.

Vir-Sec's SecureAcess™ solution is the first proposed solution that provides a virtual cyber infrastructure for the credit card network by which to verify consumer identities in cyberspace and verify the authenticity of financial transactions. The SecureAcess™ solution has already reached the destination of the innovative technological timeline through tokenization, multifactor authentication, and completely virtual technology. Vir-Sec has created the industry standard cyber infrastructure for a secure credit/debit card network that aims at stopping in-person and online fraud and identity theft *before* it happens.

SecureAcess™ is the future of credit and debit card security in the cyber age.