Payment Security Systems:

Response to Debit Card Interchange Fees and Routing: Proposed Rule

Portions of this Paper were first developed in 2009 to help explain to various Government Officials where security problems exist, and remain unaddressed, in the U.S. Payments Industry. The recommendations from 2009 have been revised since the Dodd-Frank Act has changed the way solutions will be developed, but major issues remain with regard to Payment Security and recommendations to address these issues are now presented in response to the Federal Reserve's request for comments in Docket No. R-1404

12 CFR Part 235
Debit Card Interchange Fees and Routing; Proposed Rule

Robert R. Dykes
Senior Vice President
Office: +1 408 646 5080

VeriFone Inc.
2099 Gateway Place
Suite 600
San Jose, CA 95110

Content

Executive Summary

The payment card industry is an integral part of the U.S. financial infrastructure, relied upon by consumers for a wide variety of transactions. Consumers making a purchase with a payment card expect the transaction to be secure and not expose them to fraudulent transactions in the future.

Today, there are significant weaknesses in Payment Security Standards and equally important what Standards exist are enforced in an inconsistent and ineffective manner. This ineffectiveness enables stolen card data to be used in fraudulent transactions, exposing consumers to financial losses and significant inconvenience. These weaknesses are further outlined in the attached paper.

VeriFone recommends that the Federal Reserve take some specific actions as part of its responsibility under the Dodd-Frank Wall Street Reform and Consumer Protection Act, to require card issuers to take effective steps to reduce the occurrence of, and costs from fraud in relation to electronic debit transactions through the development and implementation of cost-effective fraud prevention technology, which is available today and proven to reduce fraud.

VeriFone notes in general that the Federal Reserve's questions and alternatives in the area of "Adjustments for Fraud Prevention Costs" are heavily weighted around the notion that most fraud prevention costs incur within the Card Issuer. In fact, VeriFone asserts, most fraud costs are born by the merchants in the form of their purchase of secure payment equipment and the many billions of dollars spent by merchants to achieve PCI compliance to address weaknesses in the current payment infrastructure, *and most opportunities to reduce fraud are found in further improving security at the merchant level*. As the Federal Reserve notes in its question # 10, P 81743, the Act requires that "the Board should consider fraud-prevention and data security costs of each party to the transaction". VeriFone has developed a response that is focused on the broad cost of fraud prevention and data security and how the Federal Reserve, within its mandate provided by the Dodd-Frank Act, can use debit card interchange fees to improve security for Debit Cards.

Specifically, VeriFone recommends that the Federal Reserve develop a mechanism for a portion of the interchange fee wherein that portion becomes an incentive for those who can most effectively improve security, that is the merchants, to improve security. We recommend that the Federal Reserve work with the PCI Security Council and the Secure Point of Sale Vendor Association (SPVA) to create a fee mechanism that is technology-specific, reflects the cost-benefit of various technologies, and can vary as security threats evolve.

VeriFone Responses to Specific FTC questions:

VeriFone is limiting its responses to those questions relating to security, and how the allowance of an additional fee to the Debit Card Issuer can result in improved security.

As noted in the paper issued by the Federal Reserve, (Page 81741), the most commonly reported fraud types were counterfeit card fraud, lost and stolen card fraud, and card-not-present fraud. VeriFone notes that the security expenses and activities discussed by the Federal Reserve in its paper are not those oriented around avoiding the loss of data, but instead are the activities focused on avoiding fraudulent cards subsequently being used in the payment industry and false charge-backs. VeriFone believes it is much more cost effective to avoid the loss of data in the first place. In order to address the way a fee provided to the Card Issuing Bank can reduce such data loss and hence reduce fraud, it is important to understand how the loss occurs in the first place. Most card data is stolen from the card payment industry in one of the following means:

- Hackers break into the databases of a Merchant or steal data as it traverses a retailer's network, on the way to the processor.
- Hackers break into the databases of a Payment Processor or ISO that serves the Merchants.
- Hackers skim data from insecure payment devices or through card handling at restaurants.

There are technologically sound, cost-efficient mechanisms available today to ensure that these risk areas are secured and these are further discussed in later pages of this document. Briefly addressing the above risks, however:

Securing Merchant Databases & Networks

This risk area is being addressed today by VeriFone and is competitors, in conjunction with Payment Processors, by encrypting card data in the "Tamper Resistant Security Module" of our payment terminals and then the data is de-encrypted only when it arrives at the Payment Processor. The Processor hands a token back to the merchant so that the transaction can be tracked and retrieved to handle charge-backs etc. The merchant's employees do not have access to the security keys, so even bribery of a merchant's employees cannot unlock the data. The security around this technique is defined by the PCI Security Standards Council standard on Point to Point Encryption Technology and PCI DSS Compliance v 1.0 dated October 2010. This solution is being sold to larger merchants at a price that is usually less than the savings that this approach allows the larger merchant to realize in reduced PCI audit costs. That is, the larger merchant achieves the higher level of security and substantially reduces its PCI audit costs at the same time, for a net overall cost saving. About two-thirds (by payment volume) of Payment Processors in the United States have adopted VeriFone's encryption method, and VeriFone believes that the remainder will, in 2011, adopt and offer to merchants at least some encryption method.

The Federal Reserve could take no action, and over time the improved economics for the larger merchants, who have been the main targets of hacking, will result in this risk area being made secure. VeriFone notes, however, that not all larger merchants are adopting this new capability as rapidly as

might be expected, mainly due to the normal reticence of any organization to change. Hence VeriFone recommends below a mechanism that will help speed up the adoption of this security improvement.

Securing databases of Payment Processors and Large ISOs.

VeriFone notes that in this category only one large ISO has been hacked and that organization has implemented the encryption of its data. VeriFone's partner in this area, RSA, now offers to Payment Processors and Large ISOs the ability for them to encrypt their data. About 2/3 of the industry's payment transactions flow through organizations that have agreed to a secure form of encryption, and VeriFone believes that within the next year or so all such organizations will be encrypting their data. Given the lack of hacking in this area historically, and the industry's movement to encryption, we believe that there is little benefit in taking further action to accelerate or enforce adoption in this portion of the industry.

Skimming of Data from Payment Devices

VeriFone would like to emphasize to the Federal Reserve that this is where most card data theft incidents occur today and where the greatest opportunity exists to address fraud in the Payments Industry. The Payment Industry has standards relating to security of payment devices. The security specifications are laid out by the PCI Counsel, and enforcement of when and where such standards should be adopted is controlled by the major card brands. There are significant weaknesses in the present process for ensuring security of payment devices:

a) A significant segment of devices do not meet the PCI standards, and the major card brands lack the ability to require compliance. This segment is card-acceptance equipment at the gas pump. Because the major gasoline brands issue their own cards, they are not willing to be subject to edicts that arise from the major card brands that comprise the PCI counsel. As a result, of the 400,000 gas pumps in United States that accept payment cards, less than 10% have security that meets PCI standards. The Payment Industry Overview included in this response provides more data as to how card data, including pin numbers, is stolen from gas pumps. VeriFone believes that the single biggest improvement the Federal Reserve could take to improve fraud in the payment industry would be to ensure that all gas stations implement equipment that meets PCI security standards.

b) In the United States, many retailers are still in the process of installing equipment that meets PCI 1.4 level of security. Because there already have been documented instances of this equipment being hacked, the PCI Counsel has already laid out level 2.0 and level 3.0 security standards, and the equipment manufacturers are in the process of improving their equipment to meet such standards. However, only in the UK is there a deadline to implement level 2.0 standards; no such deadline exists in the United States.

c) In restaurants in the United States, waiters often take credit cards "out back" for five minutes or so to process through a card-acceptance terminal. With the growing availability of cheap magnetic-stripe readers, fraudulent waiters are able to read the card data and use this information to produce a duplicate card. In Europe, this is avoided through the use of the chip-and-pin system, whereby customers are not willing to give up their pin number, so they require the waiters to bring the card-acceptance terminal to the table so they can enter their pin number. The equipment used in Europe is readily available at a

relatively low cost and is already used by some restaurants in the United States. VeriFone recommends that the Federal Reserve's interchange structure should address this weakness in the U.S. payments industry.

d) Another area where card data is stolen is in instances where direct sales and home service agents write down the consumer's card number and expiry date on a piece of paper for later keying into web site for authorization. In the debit-card context, of course this happens with signature, not pin-required cards, but most debit cards will operate in signature mode. This is referred to in the industry as card-not-present transactions and they normally have a higher interchange fee to address the risk. VeriFone recommends that the Federal Reserve continue to allow a higher interchange fee for card-not-present debit card usage.

e) The world is not uniform. Fraud on U.S. participants can occur from international areas as well. For instance, a U.S. traveller in another country that has low security standards can have card data hacked. A U.S. merchant that accepts a card from an international traveller may be accepting a duplicate of a stolen card. These instances arise from the fact that we still use mainly magnetic-stripe cards in the United States. In Western Europe and Latin America, almost all cards include a security chip, but the merchants there continue to accept mag-stripe cards because they would otherwise lose revenue from U.S. residents travelling to those countries. If the United States were to adopt the use of chip-based cards, many other countries would quickly shut down the ability of their payment devices to read magnetic stripe cards, and VeriFone recommends that the United States should also follow this path, establishing a deadline for all cards to include a chip, at which time the magnetic readers in payment devices would be shut down. This would eliminate the ability of fraudsters to have any outlet for their stolen magnetic-stripe card data.

Recommendation

VeriFone notes that the Federal Reserve has been provided mechanisms in the Dodd-Frank Act in which the Federal Reserve can adjust the fee charged by Debit Card Issuers, and is being required by the Act to use this to reduce fraud in the debit-payment infrastructure. To achieve this, VeriFone recommends that the Federal Reserve orient its approach to fraud prevention to providing a combination incentive for implementing secure equipment and disincentive for retaining insecure equipment. We need to prevent criminals from getting useful card data rather than trying to prevent them from using stolen data. For the Federal Reserve to protect Americans and American businesses, it is necessary to protect data from being stolen in the first place.
.

Providing a higher fee to Card Issuers for transactions coming through secure equipment would perversely represent a dis-incentive for merchants to upgrade their equipment. Instead, it is recommended that the Federal Reserve allow a higher average fee (on all the Card Issuer's debit card transactions) based on the percent of transactions that come from secure equipment. But the card issuer must generate this higher fee by charging a differential fee – a higher fee on non-secure equipment and a lower fee on transactions coming from secure equipment.

With regard to what equipment is considered secure, VeriFone suggests the following points system be used to assess equipment security and appropriate interchange fees:

Equipment Security Level	Points
Equipment that doesn't meet PCI 1.4	3x
Waiters etc take possession of credit cards to process out of sight of the customer	3x
Card not present	3x
Equipment meets 1.4, not PCI 2.0	2x
Equipment meets 2.0, not PCI 3.0	1.5x
Equipment meets PCI 3.0	1x
Equipment accepts dynamic card data (NFC or Chip based)	.5x
Or: All data is encrypted throughout the merchant's process	.5x

The "x" would be adjusted so that the Card Issuer is able to achieve an overall security fee that meets the fee allowed based on its mix of secure and insecure equipment. And these ratios would be adjusted from time to time by the Federal Reserve in conjunction with the PCI Counsel and the SPVA.

The PCI Council should be specifically requested to continue to provide recommendations with regard to equipment security levels to the Federal Reserve that do not favor one group of merchants over another, nor differentiate its standards based on criteria such as "unattended" or "attended", except to the degree that they have a bearing on the degree of risk.

The SPVA should be specifically requested to develop a data base that can be accessed by the Card Brands, Card Issuers, and Payment Processors that compiles the mix of security equipment used by each merchant.

With regard to specific questions raised by the Federal Reserve, P 81742:

1) VeriFone recommends that the Board adopt standards that rely on technology solutions recommended by the PCI counsel and the SPVA, and which evolve as fraud threats also evolve. We recommend this because the Federal Reserve's tools are operating through Card-Issuing banks, which are too far removed from the actual source of card theft, and too fragmented, to be doing anything but trying to "bolt the door after the horse has left the barn". The Federal Reserve, working with the PCI Counsel and SPVA can determine actual technology solutions that evolve.
2) Technology-specific standards should be adopted in conjunction with industry associations, such as the PCI counsel and the SPVA. The mechanism of weighting the points awarded to various security technologies is one that can be flexible and adjusted based on the relative cost of each technology versus the risk of not adopting such technology.

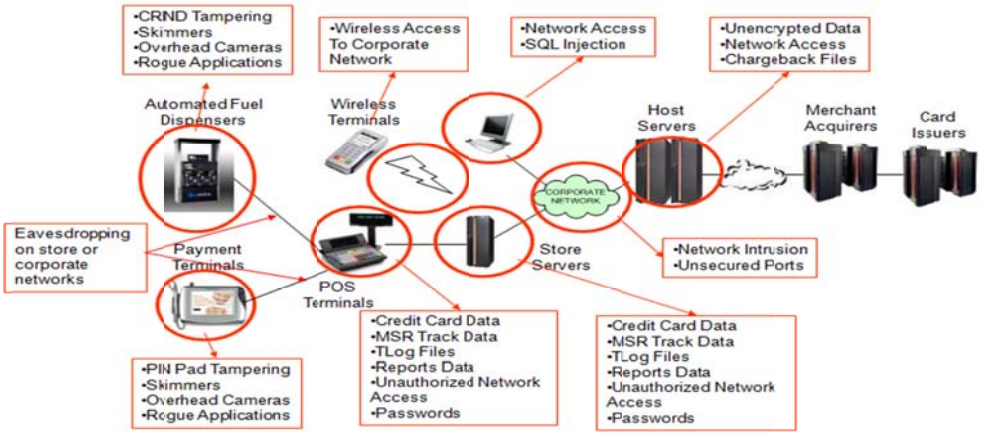
3) VeriFone believes that the fraud-prevention activity of an issuer is not very pertinent to reducing fraud, and instead the Federal Reserve should focus on reducing fraud at its source, not bolting the door afterwards at the card issuer.
4) VeriFone's recommendation would provide a mechanism that addresses both signature and pin-based debit transactions. We note that fraud, especially charge-backs, is higher with signature-based debit transactions, and believe that having a higher interchange fee on signature-based debit transactions would help steer transactions to be pin-based.
5) VeriFone believes that the Federal Reserve's approach should be to look at all the sources of fraud and provide a mechanism that is balanced to address them all.
6) VeriFone notes again that the Federal Reserve seems too focused on fraud-prevention activities within the Issuer, whereas the Act did not refer to fraud prevention within the Issuer's organization, but instead "*require(s) issuers to take effective steps to reduce the occurrence of, and costs from, fraud in relation to electronic debit transactions, including through the development and implementation of cost-effective fraud prevention technology" (§706 A II). And "'(IV) the fraud prevention and data security costs expended by each party involved in electronic debit transactions (including consumers, persons who accept debit cards as a form of payment, financial institutions, retailers and payment card networks);" ((§706 B IV)* As VeriFone has noted, most fraud is initiated out of the direct control of the issuers, and thus the steps Issuers need to take to reduce fraud must include influencing those others in the payments system who can reduce the fraud. VeriFone's recommended system will achieve this.
7) Again, the Federal Reserve is, we believe, erroneously focused just on fraud prevention within the Card Issuer. The fee mechanism recommended by VeriFone would itself be the "cost" that is allowed to be reimbursed under the Act.
8) VeriFone's recommendation would result in a mechanism that results in a different fee for each Issuer; we do not recommend a safe-harbor fee, since this would eliminate the ability to influence others in the payment system that can actually effect change.
9) VeriFone recommends that the Board work with the PCI counsel and SPVA to update the standards annually, in small increments so that the effect on the payments industry is measured and focused.
10) In question 10, the Federal Reserve agrees that its rule-making must take into account the Fraud Prevention and Data Security Costs of each party to the transaction, which is the theme that VeriFone is pointing out in its response.

One other comment: the Federal Reserve's paper (page 81723, § II): it is stated that "overall, roughly one quarter of the merchant locations in the United States that accept debit cards have the capability to accept PIN-based debit transactions". VeriFone believes this ratio is widely off the mark, since around two-thirds of merchants have pin entry devices provided by VeriFone or its competitors. There may be a subtlety in the word "capability" and the lower percent is driven by offering from Payment Processors, but by far the majority of merchants have the equipment necessary to transact PIN-based debit transactions.

The remainder of this paper is provided by VeriFone to help educate the Federal Reserve on the Fraud-Prevention and Data Security Costs incurred in the industry outside of the Card Issuers' direct efforts.

Payment Industry Overview

The payment card industry is fundamental to our financial system, processing over $2.5 trillion of card transactions annually.[1] The industry is composed of numerous entities that enable card payments through a chain of reading devices, storage and transmission. Following is a general overview of the payment card process:



A diagram of various payment value chains is provided in the Appendix, along with a definition of key terms used in this paper.

General magnetic card data (Track 2 is used by the payments industry) is comprised of the following fields:

Routing	Middle 6	Last 4	Discretionary Data
		(Receipt Printing)	((PIN Verification Indicator (PVKI), PIN Verification Value (PVV), Card Verification Value (CVV) and other issuer specific information))
435688	298101	1588	20017632108900331272[2]

When a credit card is first swiped, in most instances in the U.S., a verification process commences, which determines that the card is legitimate, that the account has sufficient funds or available

---

1 Including credit, debit, prepaid, ATM, and POS cards. Today, credit cards are responsible for more than $2.5 trillion in transactions a year and are accepted at more than 24 million locations in more than 200 countries and territories. (Source: American Bankers Association, March 2009)

2 In addition, with Chip-and-PIN cards, there is a pin number electronically embedded in the card, which is verified in the point-of-sale device when the user enters a pin number. This verification doesn't require any connection to the card issuing bank, so has been popular in countries where the communications infrastructure is weak.

credit line, and an authorization code for that transaction is provided to the merchant. But settlement of the funds does not take place at this time.

The magnetic card data, along with authorization code, and transaction time stamp, is sent to the merchant's Payment Processer, often immediately, but sometimes in a bulk process or batches at regular time intervals. Many merchants also store the card data in their computer systems, as described later. The Payment Processor pays the merchant and also stores this data, parsing the transactions out to the various Card Issuing Banks for reimbursement. The Card Issuing Banks also hold the data and use it to create the customer's monthly bill.

While the payment card process can be secure, unfortunately, that is not the current state of the industry. The payment card industry has seen regular increases in the amount of security breaches over the last 10 years, resulting in substantial harm to consumers and the industry.

- In its 2009 report Verizon's Business RISK Team found, "More electronic records were breached in 2008 than the previous four years combined, fueled by a targeting of the financial services industry and a strong involvement of organized crime."[3]

- According to the Ponemon Institute, "Since 2005 when the Privacy Rights Clearinghouse began tracking the data breach incidents, more than 250 million customer records containing sensitive and confidential information have been lost or stolen. Ponemon Institute research indicates that data breaches have serious financial consequences on an organization. According to this year's Ponemon Institute *Annual Cost of a Data Breach* study, the average cost of a data breach has risen to $202 from last year's $197 per customer record."[4]

- More than 900 million records were compromised over the 2004 – 2009 period, according to the Data Breach Investigations Report from global provider Verizon Business [5]

- The 2009 Identity Fraud Survey Report released by Javelin Strategy & Research confirms that the number of identity fraud victims has increased 22 percent to 9.9 million adults in the United States, while the total annual fraud amount only increased slightly by seven percent to $48 billion over the past year. [6]

- Reports of data breaches in the United States increased 47 percent in 2008 from the year before, mostly as a result of lost or stolen equipment, and accidental exposure of data online, according to a new study from the nonprofit Identity Theft Resource Center.[7]

- There were 656 reports of breaches in 2008, compared with 446 for 2007, and an estimated 35.7 million records were potentially breached based on notification letters and information from breached companies, the study released in January of 2009 found. [8] The openness of

---

3 *See*, http://newscenter.verizon.com/press-releases/verizon/2009/verizon-business-2009-data.html.

4 Fourth Annual Cost of Data Breach Study, Ponemon Institute©

5 "2010 Data Breach Investigations Report" by Verizon Risk team in cooperation with the United States Secret Service http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

6 "2009 Identity Fraud Survey Report", Javelin Strategy & Research, February 9, 2009, http://www.idsafety.net/report.html

7 "Identity Theft Resource Center's 2008 Breach Report", January 5, 2009, http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml

8 "Identity Theft Resource Center's 2008 Breach Report", January 5, 2009

criminals in their pursuit of hacking equipment is illustrated by the recent advertisement in Appendix Two where engineers are being solicited to build such equipment.

- About 7.5% of U.S. adults lost money as a result of some sort of financial fraud in 2008, in large part because of data breaches, according to a recent Gartner survey. [9]

- Payment card fraud claimed 36% more victims in 2008 than other fraud types, such as new account and checking account scams. [10]

All of this has occurred despite the payment card industry's adoption of a set of control requirements to protect cardholder information – known as the Payment Card Industry Data Security Standard (PCI DSS). Verizon's Business RISK Team, in fact, found that "over three-quarters of organizations suffering payment card breaches within our caseload were found not compliant with PCI DSS or had never been audited."[11]

- At attended locations, the payment devices are now protected by the third generation of this standard.

- At unattended locations[12], there is very little protection against data fraud. While there are standards that have been defined to prevent fraud, currently there are no compliance mandates to require that the unattended locations be secured against payment fraud and thus unattended locations are the most insecure part of the payment chain. For example, there are 800,000 fuel pumps or 1.6M fueling locations where there is virtually no protection afforded to consumers as they swipe their cards and enter their PINs. [13]

- The most prevalent way the industry discovers hacking at these unattended locations is when fraudulent transactions are made with the stolen card data. Sometimes the hackers wait a considerable period before using fraudulent cards to ensure they maximize the time during which the hacking continues un-noticed. Thus, there is no way of knowing how many hacking devices are installed today. There could be hundreds or thousands installed waiting to be activated.

- Hacking devices are often installed by criminal gangs, most with overseas links.

VeriFone as the industry leading manufacturer of point of sale equipment, is very concerned about consumer confidence and protection relating to the use of such equipment. Verifone finds the current state of cybercrime and lack of Payment Card Industry preventive action intolerable. Moreover, criminals are getting more inventive and aggressive. Before the situation becomes grave, the industry needs to act seriously, forcefully, and comprehensively – and we need the assistance of government to ensure that occurs. VeriFone has proposed a series of concrete steps that can be

---

9 Garter Research Report G00165825, Avivah Litan, February 27, 2009, not publically available

10 Garter Research Report G00165825, Avivah Litan, February 27, 2009, not publically available

11 2009 Data Breach Investigations Report, Verizon Business RISK Team, April, 2009 at 41. http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

12 Unattended locations include Gas Pumps, Transit Payment locations, independent ATM's, and vending machines.

13 Internal VeriFone study of total number of fuel pumps in the United States less pumps without payment including fleet pumps, marinas, government, airports, privately operated (transit agencies, etc.) and states that do not allow payment at the pump (New Jersey, etc.)

taken to stem the tide. We are now calling on government to join us to make this effort successful. Right now, close oversight is essential, and, should that fail, greater intervention will be necessary.

The Details – Unattended Terminal Hacking Has Been Unaddressed for Years

The payment card industry has known about the vulnerability of unattended payment locations for years. In 2006, one major Card Brand issued two Data Security Alerts, one of which said in part: [14] [15]

> "Organized crime rings are increasingly targeting merchants to obtain magnetic stripe data ("track data") and Personal Identification Numbers ("PINs"). Recently, these attacks have focused on Automated Fuel Dispensers ("AFDs") typically found at gasoline stations. Members and their merchants that operate AFDs should be alerted to the following attack strategy and take steps to reduce potential threats. In most cases, criminals are attaching a skimming device to the AFDs card reader in order to directly capture account data. In some isolated cases, PINs have been captured through modifications of the PIN pad. These skimming devices may read and store track data and PINs while allowing a legitimate authorization to occur. The device is typically left in place for several days until the criminal returns and disconnects it."

Yet despite this, the Card Brands (American Express, Discover Financial Services, JCB International, MasterCard, and Visa) have announced no plans to fine retailers with unattended terminals who fail to update to the level of security now being implemented by other retailers with attended terminals that are subject to fines for failure to comply. [16]

Methods Used by Criminals

Breaches in payment security systems mainly arise from one of the following methods:

A) Failure to protect stored card data, permitting it to be stolen from Merchant or Payment Processor.

With the reduced use of sprocket paper that previously recorded credit card data, the risk from sales people keeping credit card data is reduced, but many merchant stores still maintain the

---

14 "Visa U.S.A. Inc. Data Security Alert", September 29, 2006, attached as "Visa Alert_AFD_Sept_2006.pdf" and available here: http://usa.visa.com/merchants/risk_management/cisp_alerts.html

15 "Visa U.S.A. Inc. Data Security Alert", November 17, 2006, attached as "20071117_datasecurityalert_petroleum.pdf" and available here: http://usa.visa.com/merchants/risk_management/cisp_alerts.html

16 "Update on Visa's Compliance Policy to Facilitate Triple Data Encryption Standard Usage", April 22, 2009, attached as "Visa TDES Compliance Update.pdf" and available here: http://usa.visa.com/merchants/risk_management/cisp_alerts.html

data. The often-cited need is to hold the data until the bulk process to the Payment Processor commences. However, most larger merchants send the data at the time of the transaction with what is termed "host capture". Another reason many merchants maintain the data simultaneously in their own systems for a lengthy period is to enable them to handle "charge backs" – where a customer has challenged a charge on their bill, and the merchant needs to provide proof of signature for the transaction. In addition, some merchants also save the card information and expiration date for return and refund processing. Many merchants also use credit card data as the basis for their own tracking of consumer behavior and their loyalty programs. For each of these cited reasons for holding the data, however, alternatives do exist in the industry that don't require holding the card data by the merchant.

With unencrypted data being held by the Merchant and Payment Processor, hackers are able to access this data by either placing a worm in the Merchant or Payment Processor's data systems, or by co-opting an employee to assist. Considering the high value that is associated with this data, co-opting employees is financially quite viable for the hackers.

B) Failure to protect card data at the Point of Sale device, enabling the use of a skimming device.

Hackers have designed a number of devices to collect credit card data at the time it is inserted into the POS device. These are generally one of the following:

i. An overlay device with a magnetic reader, which is installed on the outside of an unattended payment device, looking like part of the original device. This additional magnetic reader stores the card data, which is retrieved by removing the overlay device periodically.

ii. The overlay devices are enhanced by placing a camera near the unattended device so that the entry of PIN numbers can be recorded, and using time stamps, later paired up with the credit card data. PCI-PED-compliant devices have a shield around the keypad to prevent this.

iii. In some cases, at unattended terminals, a membrane keypad is installed over the real PIN entry keypad to capture the consumers PIN's as they are entered. PCI-PTS compliant devices have a keyboard with individual keys, so they are not amenable to overlay devices.

iv. An internal device inserted in the POS equipment.

Unattended terminals are the favorite location for these devices, because there is often a large amount of space within the terminal mechanism, and because the terminals are normally serviced at night. The servicing agents are either co-opted or falsely represented, but either way the insertion is relatively easy. The device can be sophisticated, because the bulk of equipment used in many unattended terminals has very little security and a source of power is available. The hacking devices can be large enough to have a built-in Wi-Fi transmitter to a data gathering device that can be collected regularly without approaching the terminal. The devices are simply wired to the card reader and PIN pads to collect data as entered. An example of this type of hacking is discussed at www.krebsonsecurity.com [17] Most

[17] http://krebsonsecurity.com/2010/07/skimmers-siphoning-card-data-at-the-pump/ (Also see Appendix Three)

PIN data for ATM-card usage on an unattended terminal is single-DES encrypted by the PIN-pad device, but never-the-less PIN data can be stolen by providing an overlay PIN-pad, or a camera device. It is also possible, though no data is available to prove it has been done by hackers, to break single-DES encryption during a PIN debit transaction. Recent data break-ins to major payment processors may give hackers sufficient data to more easily compromise single-DES encryption.

v. Very small devices have also been found inserted into credit and debit card attended Point of Sale equipment. Non PCI-PTS compliant equipment can be tampered with quite readily and data can be read from the magnetic head and PIN-pad. Where they are PCI- PTS compliant, an overlay device with a separate magnetic head is sometimes inserted in the track where the credit card is swiped. The installation of this tampered equipment is usually accomplished by impersonating the equipment's maintenance staff or through social engineering to distract employees.

PIN hacks, which take place primarily at older, more vulnerable point of sale devices, hurt consumers more severely than simply credit card data, because they allow hackers to withdraw cash directly from the consumer's account. Such thefts are difficult to resolve with the customer's bank because the consumer has to prove that the withdrawal was made by someone fraudulently.

With all of these methods, the result is that hackers produce counterfeit cards. If they don't have ATM-PIN number data, the cards are used to buy goods. By circulating the hacked cards widely, they are able to circumvent enough of the Issuing Bank's security methods to make the process financially worthwhile. A favorite way for thieves to verify if a counterfeit card will work is to run it through an unattended gas station. Where ATM-PIN number is available, the payoff is very substantial, since this obviates many security systems and entire bank accounts can be emptied before the customer notices.

A Flawed Attempt to Secure Data and Prevent Hacking – the PCI Security Standards Council

To reduce fraud, the Credit/Debit Card industry established the PCI Security Standards Council (PCI SSC) in 2006. This is led by a policy-setting Executive Committee composed of representatives from the founding Card Brands -- American Express, Discover Financial Services, JCB International, MasterCard, and Visa. In addition there is a Management Committee, also from the Card Brands, and an Advisory Board drawn from Participating Organizations[18]. This body adopted a series of security standards that have the potential to substantially enhance security at Payment Processors, many Merchants, and in new Point of Sale devices. They are known as PCI DSS (for data security) and PCI PTS (for pin transaction security).

While the PCI SSC sets the standards, the date merchants must adopt those standards remains the individual responsibility of the Card Brands,[19] and there are insufficient incentives for members acting alone to fully deal with non-compliant Merchants. As a result, the Card Brands do not impose

[18] Merchants, payment devices and services vendors, processors, financial institutions and others that participate in the payments processing industry may qualify as participating organizations.

[19] Anti-trust regulations prohibit the Card Brands imposing penalties in a coordinated manner.

penalties in every non-compliant situation, provide exemptions to some Merchants or groups of Merchants, and change enforcement of standards deadlines, all based on various criteria. Through Payment Processors, they individually prioritize enforcement based on the volume of Merchant transactions, the potential risk, exposure introduced into the payment system, and other factors. They acknowledge that the costs-of-breach are related to the direct financial exposure of the issuing banks rather than the inconvenience, including identity theft, of customers.

While one brand may be seen as the main enforcer of security standards, it also has to be sensitive to its own financial success and competitive pressures may limit its ability to enforce standards. Thus, the threat by a group of merchants to put up a notice that they do not accept a particular card brand might influence that brand to delay enforcement of a standard.

All of this means that while the PCI SSC has established security standards for both Data and PIN Entry Devices,[20] these standards are not sufficient to ensure transactions are secure. With regard to Data, the PCI SSC has established standards that relate to the type and method of storing data and security around it, but the Card Brands have created enforcement criteria that segments based on the size of the Merchant (see table one).

With regard to PIN Entry Devices, the PCI SSC has also established strong standards that ensure data cannot be tapped between the magnetic head reader, PIN entry device, screen, and the central electronics. However, in the U.S., the Card Brands have not announced fines if merchants do not use terminals compliant with the latest standards in unattended instances, such as gas stations, where the fraud incidents are most prevalent. Visa did announce its own, less-secure standards for unattended PIN devices[21], but then specifically stated that lack of compliance with this standard on existing unattended PIN devices in the U.S. will not result in fines. The major beneficiaries of this large exemption are the gasoline dispensers, and it is noted that Gasoline Brands' own credit cards represent competition to the Card Brands.

It should be noted, however, that Shell Oil has provides a substantial incentive for its franchisees to upgrade their equipment to be PCI-PTS compliant, but there has been little action by other brands.

Unattended PIN entry devices would benefit substantially from having PCI-PTS compliant devices installed. Such compliant devices would ensure that data cannot be hacked with electronics installed within the device, and substantially reduces the ability of hackers to determine PIN numbers from key overlays or remote video cameras. Requiring security compliant devices in attended situations, but not requiring compliant devices in unattended situations, suggests insufficient emphasis on card-holder security by the Card Brands when establishing enforcement of the various standards.

---

[20] The PCI SSC has not established standards for credit card readers without PIN entry.

[21] Visa announced a requirement, independent of the PCI SSC, that new unattended (*e.g.* Gas Station) PIN devices should be upgraded from single-DES to triple-DES encryption. Along with marketing efforts by VeriFone, this requirement had been having the side-effect of causing many Gas Stations to upgrade to PCI-PTS compliant equipment, but Visa has specifically stated that lack of compliance with its standard on existing unattended PIN devices in the United States will not result in fines.

As shown in the following table, about one third of all Visa transactions are estimated to not be conducted through PCI compliant systems:

Table One

Merchant Level	Annual Visa Transactions per Merchant	% Total Visa Transactions	Number of Merchants	PCI Compliant
1	> 6M	50%	362	93%
2	1M – 6M	13%	702	88%
3	20K – 1M ecommerce only	5%	2,627	57%
4	< 1M	32%	>6M	"low"

As of 3/31/09, Per Diane Greenhaw, Visa, Digital Transaction News, 4/23/09

In sum, the major issues with the present security process are that:

1. The Card Brands act alone in enforcing the standards and have often been leaving it to just one brand as the major enforcer of standards, which places that brand at a competitive disadvantage and so reduces its incentive to enforce standards.

2. The major Card Brands base their enforcement criteria on the risk-benefit to the Card Issuing Banks rather than reflecting the cost to customers of having their financial data stolen, their credit cards rejected, and sometimes their bank accounts emptied.

3. Retailers are expected to incur the costs of security compliance, and incur the liability for breaches, but see little direct benefit to their businesses for being compliant.

4. Unattended payment locations are a major source of counterfeit information, have the least secure PIN systems, and merchants can apparently exert sufficient influence on the major Card Brands to avoid significant security improvements in unattended locations.

The PCI *Data* Security Standards are somewhat effective at preventing certain types of data breaches when faithfully implemented and executed on an ongoing basis. However, due to their cost, complexity, and selective enforcement by the Card Brands of PCI-PED standards, PCI DSS is not universally effective in protecting merchants and consumers from falling victim to credit card fraud

Appendix One

Overview of Traditional Payment Value Chains

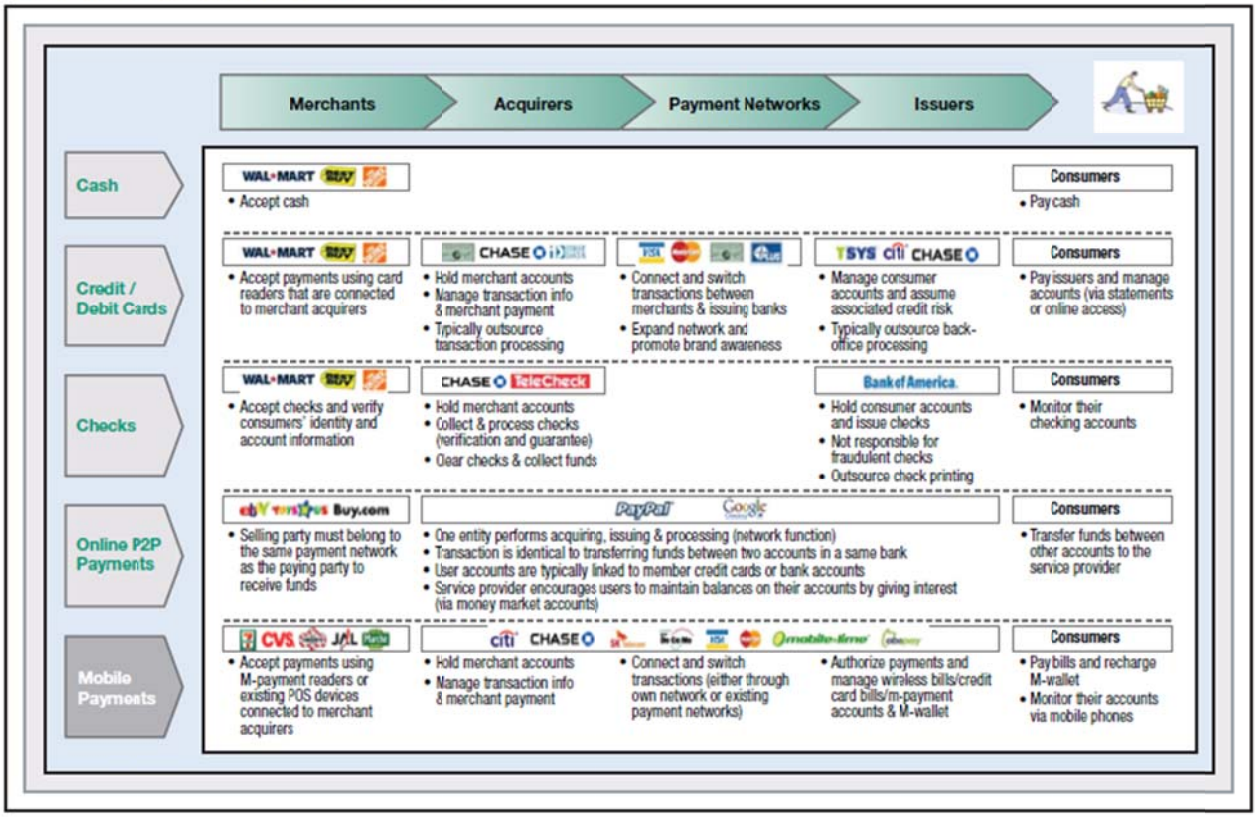


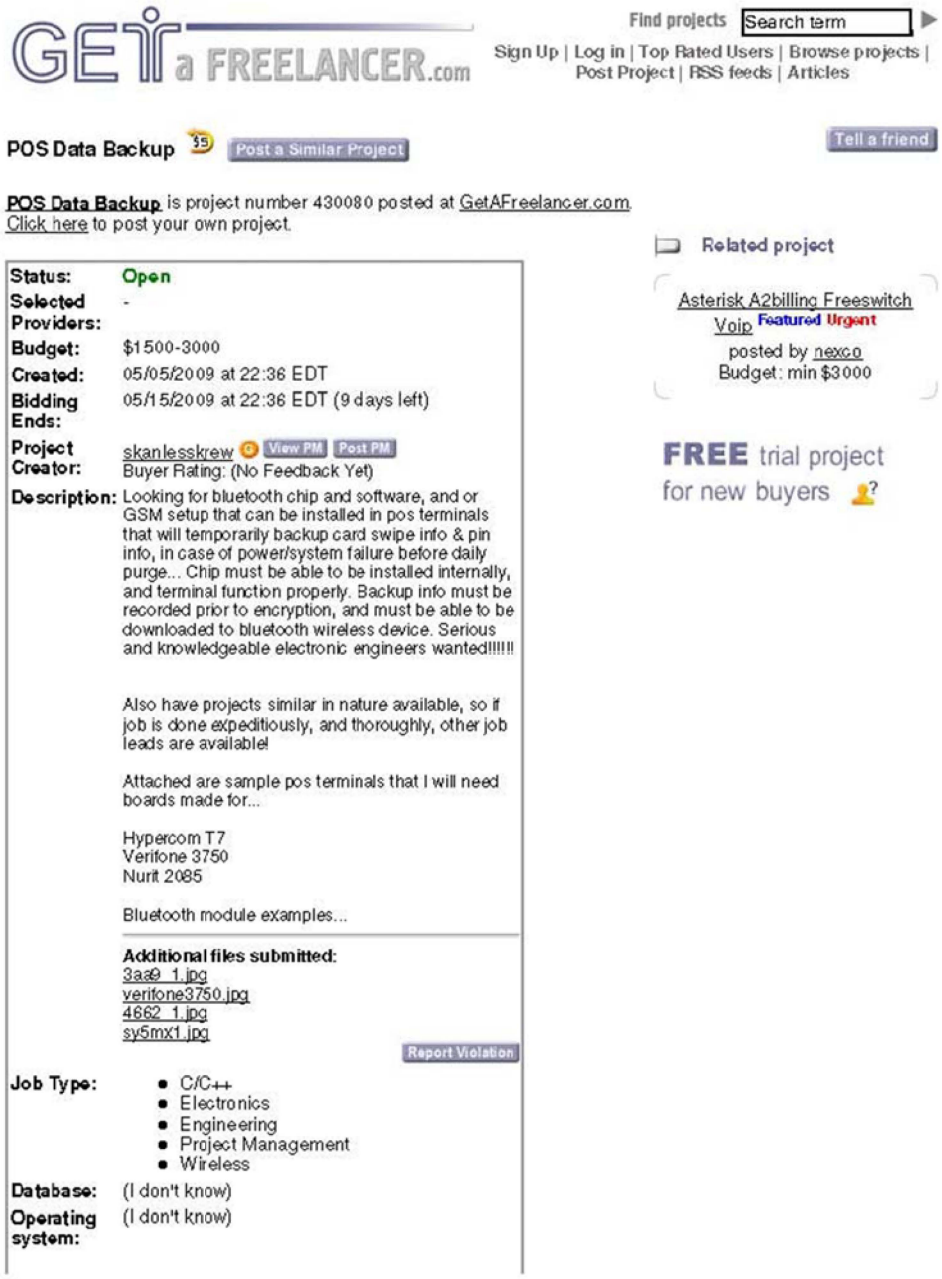
Chart Source: ABI Research

Definitions

Acquirers	Accept transactions from Merchants, pay merchants. Pass the transaction on to the Card Issuing Bank, usually via a Payment Network
AFD	Automatic Fuel Dispensers
PCI	Payment Card Industry
PCI DSS	Data Security Standards. These provide controls around data held by the merchants, Acquirers, Networks and Issuers.
PCI PTS	Pin Security Device. (Formally known as PCI-PED, [pin entry device]). These standards relate to the point of sale device used to enter a pin number.
PCI SSC	Security Standards Council
PIN	Personal Identification Number
POS	Point of Sale device
PPISC	Payments Processing Information Sharing Council
SPVA	Secure POS Vendors Alliance, www.spva.org

Appendix Two

This is an example of a May 5th request for an engineer to design a device to be inserted into a payment terminal so as to extract card data via blue tooth wireless. There is no legitimate use for such a device.



GET a FREELANCER.com

Find projects Search term

Sign Up | Log in | Top Rated Users | Browse projects | Post Project | RSS feeds | Articles

POS Data Backup Post a Similar Project

Tell a friend

POS Data Backup is project number 430080 posted at GetAFreelancer.com.
Click here to post your own project.

Status:	Open
Selected Providers:	-
Budget:	$1500-3000
Created:	05/05/2009 at 22:36 EDT
Bidding Ends:	05/15/2009 at 22:36 EDT (9 days left)
Project Creator:	skanlesskrew View PM Post PM Buyer Rating: (No Feedback Yet)
Description:	Looking for bluetooth chip and software, and or GSM setup that can be installed in pos terminals that will temporarily backup card swipe info & pin info, in case of power/system failure before daily purge... Chip must be able to be installed internally, and terminal function properly. Backup info must be recorded prior to encryption, and must be able to be downloaded to bluetooth wireless device. Serious and knowledgeable electronic engineers wanted!!!!!! Also have projects similar in nature available, so if job is done expeditiously, and thoroughly, other job leads are available! Attached are sample pos terminals that I will need boards made for... Hypercom T7 Verifone 3750 Nurit 2085 Bluetooth module examples... **Additional files submitted:** 3aa9_1.jpg verifone3750.jpg 4662_1.jpg sy5mx1.jpg Report Violation
Job Type:	• C/C++ • Electronics • Engineering • Project Management • Wireless
Database:	(I don't know)
Operating system:	(I don't know)

Related project

Asterisk A2billing Freeswitch Voip Featured Urgent
posted by nexco
Budget: min $3000

FREE trial project for new buyers

Appendix Two (continued)

Bid count:	1
Average bid:	$ 2800

See more: pos, pos terminals data loggers, pos recorder, online pos, wireless pos system, looking electronic engineer, pos bids, hypercom verifone, data recorder project, electronic engineer required, record pos data, similar project bluetooth, wireless device project, chip, j2me access bluetooth modul, j2me bluetooth obex example, projects related wireless devices, looking csr bluetooth programmer, locking csr bluetooth programmers, power system analysis design forum, basics etap power system analysis, power system analysis design review, pasha software power system, pos software verifone, data leads

View Project Clarification Board | Post Message on Project Clarification Board

Messages Posted: **1**

If you are the project creator or one of the bidders Log in for more options

Bid on This Project

Service Providers	PMB	Bid	Delivery Within	Time of Bid	Provider Rating
ProfessorDmitrij	View PM Post PM	$ 2800	40 days	Today 03:45 EDT new bid	(No Feedback Yet)

1.- Estimated Cost $ 2800 2.- Estimated Delivery Time 40-50 Day 3.- Milestones to Reach and time to reach Milestones 12 Day 4.- Quality Control Testing and interim reports and results every 12 days Do you have a large project so I call your maximum price which would be consistent with the qualitative work

-- Perform action on this bid --

Bid on This Project

[Outsourcing Web Design] [Secure Forms] [GAF Top Users] [View All Projects]

What is GetAFreelancer.com? (Read about the company)

Our mission is to find the best possible **freelance workers** at the best possible price. Outsourcing is hiring an outside organization to perform services such as information processing and applications development. Find **freelance programmers**, **web designers**, **copywriters** and **translators**. GetAFreelancer.com helps webmasters, web designers, programmers, software developers and business owners to develop their projects. Our escrow feature is developed to protect both buyers and sellers.

Web Development doesn't have to be expensive. **Outsourcing** will cut your expenses by more than 50%. Deposit money and don't purchase until your project is completed. GetAFreelancer.com is one of the largest sites of its kind. We have earned a good reputation and you can trust us.

Find Webmaster Resources and Webmaster Forum. Take a look at Search Engine Submission.

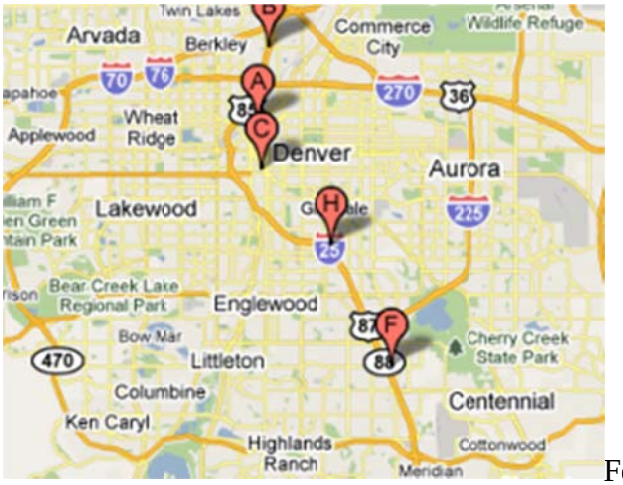
Plendo Sweden AB © 2004-2009 PRIVACY POLICY - TERMS - AFFILIATES - API - CONTACT - FAQ RSS 0.167

Appendix Three

http://krebsonsecurity.com/2010/07/skimmers-siphoning-card-data-at-the-pump/

Skimmers Siphoning Card Data at the Pump

Thieves recently attached bank card skimmers to gas pumps at more than 30 service stations along several major highways in and around Denver, Colorado, the latest area to be hit by a scam that allows crooks to siphon credit and debit card account information from motorists filling up their tanks.



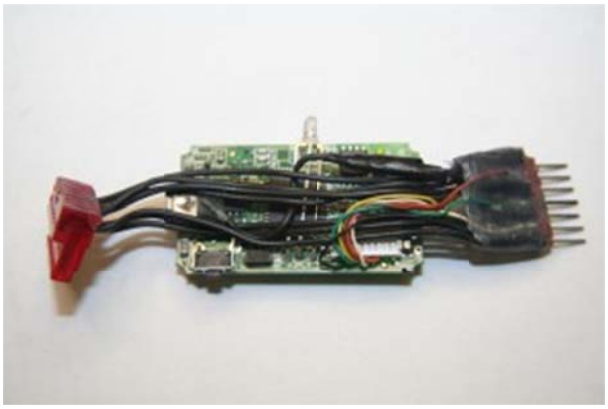
Forced to re-issue an unusually high number of bank cards due to fraudulent charges on the accounts, a regional bank serving Colorado and surrounding states recently began searching for commonalities among the victimized accounts. The financial institution, which shared information with KrebsOnSecurity.com on the condition that it not be named, found that virtually all of the compromised cardholders had purchased gas from a string of filling stations along or not far from Interstate 25, a major North-South highway that runs through the heart of Denver.

Several **Valero** stations along the I-25 corridor reached by phone acknowledged being visited over the past week by local police and **U.S. Secret Service** agents searching for skimmer devices. The stations declined to comment on the record, but said investigators left a bulletin stating that stations in the area had been targeted and urging them to be on the lookout for suspicious activity around the pumps.

Mark Gallick, a Secret Service agent with the Denver field office, confirmed that a bulletin on skimmers was circulating among gas stations in the area, but refused to comment further.

Similar attacks on gas station pumps recently have hit other parts of the country: Police in Arizona also are dealing with a spike in reports about skimmers showing up at gas pumps, prompting **Gov. Janice Brewer** this month to urge the Arizona Department of Weights and Measures to increase their inspection efforts in looking for skimmers at gas stations.

Appendix Three (continued)



Bluetooth-enabled gas pump skimmer. Photo: Alachua County, Fla. Sheriff's Office

Bluetooth based wireless skimmers have been found attached to a slew of gas station pumps throughout the Southeast, particularly in Florida. Wireless skimmers allow thieves to pull up to the compromised station and download stolen card data with a laptop while sitting in their car. Many wireless skimmers run on rechargeable batteries, but skimmers attached to the insides of a gas pump can easily be made to draw on the pump's power source in order to continue stealing card data indefinitely.

"Our device is not the traditional skimmer but rather a Bluetooth enabled equivalent of a thumb drive programmed to capture the data as it was transmitted from point A to point B inside the gas pump itself," said **Lt. Stephen Maynard**, the public information officer for the **Alachua County, Fla. Sheriff's Office**, which dealt with skimmer compromised pumps earlier this year.

The gas pumps compromised in the Denver-area attacks showed no outward signs of having been tampered with or altered, according to several sources. My source at the bank said all of the pumps in question contained a device on the inside of the pumps designed to record data stored on the back of cards inserted into the compromised pumps, but he wasn't sure whether the skimmers were designed to transmit the stolen data wirelessly.

My source said the hacked pumps in Denver tended to be on the outside edges of the gas station, those hardest to see by clerks in the station. In a wrinkle that could be part of an effort to drive customers to the compromised pumps, the source said, customer service representatives at the bank also received complaints from victim account holders who reported getting phone calls promising them gift cards if they purchased gas at specific stations in the Denver area.

About VeriFone

VeriFone Systems, Inc. ("VeriFone") (NYSE: PAY) is the global leader in secure electronic payment solutions. VeriFone provides expertise, solutions and services that add value to the point of sale with merchant-operated, consumer-facing and self-service payment systems for the financial, retail, hospitality, petroleum, government and healthcare vertical markets. VeriFone solutions are designed to meet the needs of merchants, processors and acquirers in developed and emerging economies worldwide.

VeriFone's products are sold around the world. In addition to the Point of Sale hardware, VeriFone also provides security solutions, terminal management solutions, application development and Payment Processing solutions that enable many parts of the payment value chain. Revenue in Fiscal Year 2010 was over $1 Billion. VeriFone has about 2,600 employees.