

Successful Strategies for Providing Secure Payment to Self-Service Kiosks

Electronic payment is built on trust—trust between the consumer and the retailer, and just as important, among the various parties involved in supporting payment solutions. In an increasingly uncertain environment, the key to maintaining this trust is highly sophisticated security measures.

Providing consumer payment as part of a Self-Service Kiosk can be a challenge and VeriFone can provide the guidance to a successful implementation.

Executive Summary

Payment drives added value in self-serve kiosks, but security is paramount.

As self-service kiosks become ever more accepted and popular to consumers, adding payment for goods and services is a natural progression. Cash and coin acceptance at self-serve kiosks has been available for over 100 years, but card payment has only been available for approximately 20 years. Card payment started in the petroleum marketplace with credit purchases for pay-at-pump, it migrated to self-serve ATM machines not physically located at a bank, and now can be found in every situation from gas stations to parking meters to vending.

This explosion in payment convenience has also exposed risks. In the last 10 years there has been increasing focus on fraudulent payment with cards at self-service kiosks and through the internet. Fear of card fraud or identity theft is a concern for over 70% of the adults in the US. Card fraud worldwide caused over \$1.4 Billion in losses and card associations, card processors and authorizers, consumers and even governments are taking significant steps to reduce fraud at all levels. The industry response has focused on three areas: consumer awareness, upgrades to security guidelines, and compliance enforcement. Card associations have fined members, authorizers and merchants. One of the largest card processors in the US was forced into bankruptcy because of their inattention and non-compliance to fraud prevention measures.

Accepting payment at a self-serve kiosk requires accepting responsibility for security of the payment system. This starts at the point of consumer entry and continues not only throughout the transaction and approval cycle, but also how consumer data is stored, printed and accessed by the merchant or kiosk. The standards for security compliance can be very involved, and they are changing so as to stay “one step ahead” of those that intend to commit fraud.

As a result, in order for self-service kiosk developers or deployers to be successful they need to either become expert in payment technologies and processes; or partner with someone whose primary business is secure payment and transactions.

For over 25 years, VeriFone has been the global leader in secure payment. One hundred times every second a secure payment transaction is enabled by VeriFone technology, whether hardware like PIN pads or terminals, software like PC Charge or RiTA, or complete payment systems such as Sapphire. VeriFone can help kiosk developers and deployers alike navigate the complexities of secure payment to provide added value to their consumer kiosk solutions.

This white paper will review the current trends in payment system security and explore some of the key industry security guidelines.

Introduction

An age-old problem with a modern twist

For centuries, wherever currency has been exchanged for goods and services, there have been some that try to acquire wealth dishonestly. In this regard, electronic payment is no different from any other form of payment. As electronic payment has increased in transaction volume and dollar value over the past two decades, it has become the target of rising fraudulent activity by individuals and sophisticated gangs who would like to take advantage of any gaps in security.

Card skimming is one of the most common types of fraud. Skimming involves making a copy of a card's magnetic stripe data, then using that "skimmed" data to create a bogus card and charge hundreds or thousands of dollars to that cardholder's account, before he or she receives the next statement. A common location for card skimming is in a restaurant, where a dishonest server could use a pocket device to read and capture the card data before returning it to the cardholder. There have even been cases where retail POS terminals have been tampered with—reprogrammed to capture card information and forward it to a third party.

But skimming is just the beginning today. There's a wide range of physical and logical schemes designed to capture magnetic stripe data, falsify a cardholder's identity, steal PINs, or break encryption codes. Among these are:

- Card Duplication – Duplicating a real card from receipt data, transaction data or a database record. With the internet and self service commerce, there is no cashier to verify identity or even if the "card" is really a card – of just a piece of blank plastic with recording tape.
- PIN Recovery – Gaining a PIN Code, and a debit card magnetic stripe by fraudulent means. Some of these techniques could be:
 - "Shoulder surfing"—Looking over a cardholder's shoulder or using a video camera when he or she is entering a PIN at an ATM or POS terminal.
 - Wireless transmitters—These can be attached to send data to unauthorized individuals with receivers in the near vicinity.

- Modifying or replacing hardware with altered devices—Terminals that have been electronically modified or swapped with devices that can capture and store PINs until the thieves can access them.
- False prompting for PINs—One of the most common attacks using computer logic is to design a software patch that prompts the customer for a PIN or other identification information, which is then captured in clear text rather than encrypted form for improper usage.

The risk of losses is substantial, and growing larger each year. *The Nilson Report* in 2005 estimated that card-based payment in the U.S. alone is approximately \$3 Trillion dollars. With that much money being processed at the POS and switched across payment networks, it has attracted the interest of some of very savvy criminals—all focused on finding any weakness that would make it possible to intercept some of those dollars. As reported in the Nilson Report, the card industry *knows and admits* to a fraud losses of 4.7 cents per \$100 in sales – which puts the US aggregate losses at \$1.4 Billion dollars. The magnitude of risk has gotten the attention of not only the retailers and acquirers, but also the many governments, regulatory agencies and solution providers such as VeriFone, which work closely together to limit fraud. These well-known agencies include:

- International Standards Organization (ISO)
- American National Standards Institute (ANSI)
- EMVCo (the organization that now watches over the global EMV specifications for smart card transactions)
- National Institute of Standards and Technology (NIST), which has recently published the Advanced Encryption Standards (AES)—highly sophisticated guidelines and specifications that will be widely used by government and commercial organizations to protect sensitive data.

In addition a number of the card associations have joined together on this issue and have issued their own guidelines for security covering everything from hardware to software to database storage and consumer receipts.

Security Trends

Better methods for identifying customers and authenticating transactions

The primary challenge to securing electronic payment in self-service kiosks is the difficulty posed by lack of face-to-face contact. Transactions do not take place in front of a bank officer or cashier who can vouch for a customer or verify identification, let alone to determine if the consumer has adequate balances to cover the payments. Instead, these purchases often occur anonymously with transactions distilled to bursts of electronic data

that often provide no verifiable proof that legitimate cardholders are interacting with the retailer or service provider. As a result, most security measures in the past have focused on positively identifying the various parties, authenticating transactions, and protecting the financial data that's sent or received.

With PIN, debit transaction losses are very low except in specific case where an individual card and its PIN are compromised. The vast majority of payment transactions today are with some form of credit card; whether a bank card such as Visa or MasterCard, a proprietary card such as an Oil Company gas card, or a travel and entertainment card such as American Express. The current industry focus is to better secure credit transactions.

Transaction authentication techniques relating to merchant to processor transmission are now very secure and reliable, however there is still the security weakness of fraud relating to "spoofing" or "duplicating" or "posing" as a legitimate consumer – a fake card. In 2003 Celent Communications reported that "cloning" or counterfeits cards resulted in ~25% of all card fraud in the US. Consequently, the industry has added additional measures so as to ensure that fraudulent activity is caught quickly, and prevented from happening in the first place. Some of these measures are:

- Velocity Checking – ensuring for an example the same card is not used simultaneously in different geographic or internet locations
- Two-component identification for credit (rather than PIN which is used for Debit) – Adding ZIP code or Phone number to verify billing address or user
- Card Present Identification – Providing a non-encoded or secondary number so as to verify that a legitimate card is present in front of the consumer. This is most popular with internet transactions or MOTO (mail order/telephone order).

While this addresses the issues of whether a real card is presented by the consumer, there are other concerns for a merchant relating to data security. Merchants must ensure that their data can not be compromised in a way that could cause fraudulent activity. Some measures even small merchants must comply are:

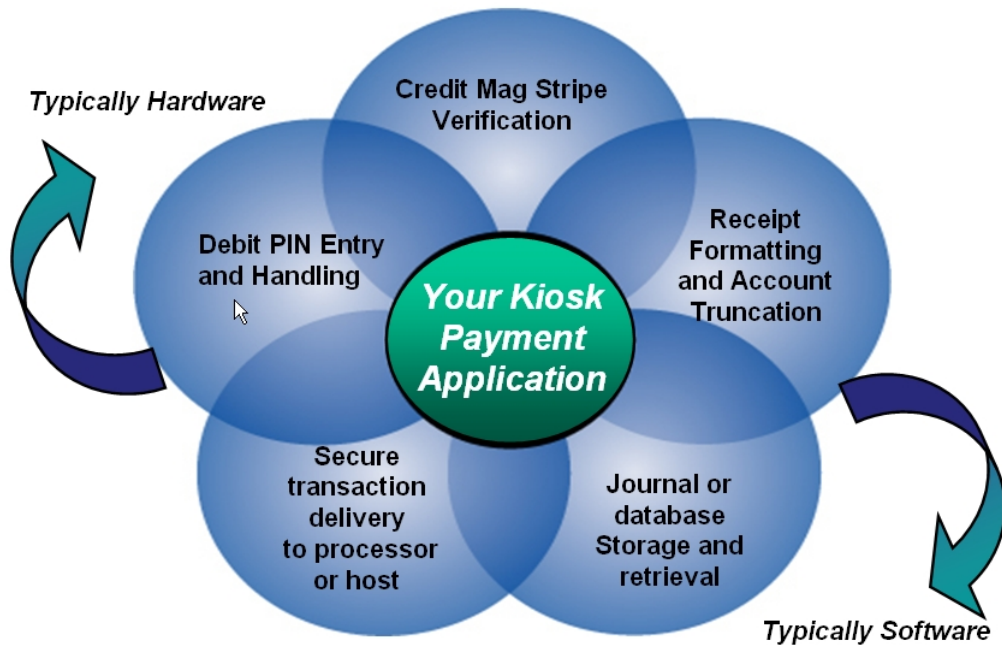
- Preventing full account magnetic stripe track data from being shown on receipts, logs or unsecured databases.
- Secure transmissions over data networks
- Secure network access, including no card holder data stored on a server connected to the Internet.

For merchants who comply with these new standards and guidelines the benefit is potentially lower transaction fees and protection of their consumer brand value and good

will. For those merchants that are more lackadaisical or, worse yet, fraudulent themselves, the penalties can be significant – up to \$500,000 per instance assessed by the card associations.

As those who commit fraud, the “fraudsters”, get smarter and the tools they use – computers and such, get cheaper and more powerful; the industry updates guidelines to stay ahead. It is unfortunately a never ending cycle.

Security Touches All Aspects of a Consumer Self-Serve Application



Implementing a comprehensive security program is much more than buying a PINPad and integrating the communication signals from it into your application. Ensuring security and fraud resistance touches just about every aspect of your application, and whether you intend to take credit, debit, gift cards, or something else. You have to secure not only the consumer information when they swipe their card or enter their PIN, but the receipt, the data that is stored for dispute resolution from the processor, the journal tape at the cashier, or the records you send up for settlement or

batch control. It all has to be secure and typically with not only physical means like PIN Pads, but also logical security like databases.

As well, all the security components have to work together seamlessly and fast. The different stakeholders – processors, card associations, and standards groups have to continually stay ahead of the fraudsters so changes to guidelines and specifications are frequent and often mandatory. For example, in 1989 when you encrypted a PIN code the “key” or number used to encrypt it might have been 64 digits long. At that time, it would take a computer costing over 5 million dollars more than 3 days to crack an encrypted message. Today a computer you can buy over the internet and delivered tomorrow for less than \$5K can crack that message in about 3 hours. As a result, the industry has changed the “key” to be much longer, in some cases 256 digits, so that even with the most advanced computers available today might take months or years to crack just one message. And your software you wrote in 1989? Probably has been re-written for security guideline or mandates at least 4 times and certified with every processor you intend to do business with at least every 2 years.

Two Key Standards and Guidelines: PCI and PABP

The need for more comprehensive and verifiable security techniques

Currently within the industry there are two key guidelines for point-of-sale (POS) transaction data; Payment Card Industry (PCI) guidelines and Payment Application Best Practices (PABP). Sponsored and supported by Visa and MasterCard, as well as others, the combination of PCI and PABP gives a solid foundation for improved transaction security practice. Of course, this is in addition to the typical network security elements like secured socket layer (SSL) encryption.

PCI

PCI establishes a unified standard guideline covering the systems, policies and procedures for security associated with the entry, storage, transmission, and processing of card data.

If merchants, or their systems, do not comply with the PCI standards, the card associations or networks can impose a variety of sanctions. They can:

- Impose restrictions on card acceptance
- Permanently prohibit card acceptance
- Impose fines depending on the severity of the incident, up to \$500,000 per incident.

As well, the Card Associations have also declared a “Safe Harbor” to those that do comply with the standards, but unfortunately have a security breach. This Safe Harbor absolves those complying merchants from any restrictions or fines imposed by the Card Associations, but does not affect any civil liability card holders or consumers would take against the merchant.

Some highlights of the PCI Data Security standard are:

- Install and maintain a firewall configuration to protect data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored data
- Encrypt transmission of cardholder data and sensitive information across public networks
- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security

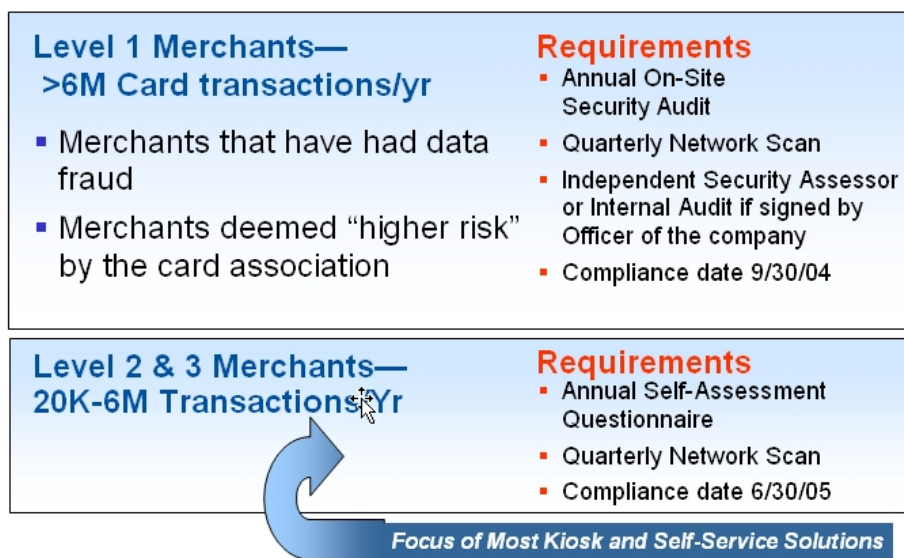
The PCI Standard has two sections of interest to those in the self-service kiosk industry. PCI-DSS (Data Security Standard) which is intended to provide the guidelines for protection of cardholder data, wherever that data resides within a transaction system; and PCI-PED (PIN Entry Device) which covers devices that accept PIN entry from consumers. Both these guidelines are designed to cover the entire solution – hardware and software – throughout the entire transaction system.

As part of the PCI standard, devices are certified for PCI-PED compliance by a 3rd party. Standards change approximately every 3 years, and a device certification is granted for 6 years beyond the next release of the specification. Hence, devices could be appropriate for up to 9.5 years, but changes and recertification of devices is more likely better planned every 5 years.

For those companies that are interested in Debit with PIN acceptance for their solutions, PCI-PED is of critical importance. Many kiosk systems are built using touch screens. This environment has proven to be acceptable with consumers, easy to maintain, and provides an excellent user interface. Unfortunately, almost all touch screens built on a PC-monitor platform are not PCI-PED compliant and therefore can not be used for PIN

entry. There are alternatives such as small PCI-PED complaint PIN pads or touch screen terminals provided by VeriFone that can be integrated into virtually any existing kiosk application to help enable debit card payment.

PCI Compliance is more than hardware. As the guideline instructs, it is the whole solution and as a result merchants are required to do compliance testing. This testing is scaled to the number of transactions that the merchant does or other factors, such as previous fraud actions, that may make more stringent compliance assessment required.



PABP

PABP, developed VISA, is a compliance program that addresses security and risks associated when full magnetic stripe data or associated identification values are stored after authorization by payment applications. The practices provide guidelines for developers or others that manage card data. Acquirers and processors are responsible for ensuring that their merchants and service providers comply with the practices and confirm the security of their systems and applications.

The key highlights of the PABP guidelines are:

- Do not retain full magnetic stripe or CVV2 data
- Protect stored data
- Provide secure password features
- Log application activity

- Develop secure applications
- Protect wireless transmissions
- Test applications to address vulnerabilities
- Facilitate secure network implementation
- Cardholder data must never be stored on a server connected to the Internet
- Facilitate secure remote software updates
- Facilitate secure remote access to application
- Encrypt sensitive traffic over public networks
- Encrypt all non-console administrative access

Taken together PCI and PABP offer the best design standards to implement transaction security for US based payment applications. Payment applications outside of the US, may have to comply with other standards and certifications such as those provided by Europay, Visa and MasterCard (EMV). These standards typically cover transactions that are not only magnetic stripe based, but also include smart (chip) card use as well. Since many of the payment systems outside of the US do not process transactions in real-time, additional security measures must be in place. The EMV standards were specifically designed to address these added security needs.

VeriFone Solutions Meet the Need

The most comprehensive security protection in the payment industry

VeriFone has consistently been a leader in providing security for POS transactions. We have integrated a comprehensive suite of security protections; whether hardware, software or full solutions.

- Omni Family of Terminals
 - VeriShield terminal file authentication
 - PCI-PED Certification
 - EMV Certification for smartcard or international certifications
 - Secure wireless transactions
- PIN Pads
 - PCI-PED Certification
 - EMV Certification for smartcard or international certifications
 - Touch Screen display PCI-PED certified PIN Pads
- Certified Software Solutions
 - PCCharge - PC based payment engine whether used stand alone or integrated into another application.

- RiTA – Hosted multi-threaded transaction engine available on cross-platform computing environments like AS400, Linux or Microsoft Server
- SecureKit – PIN Injection software for ANSI compliant injection facilities.

Summary

Building a more secure future

The payment industry will continue to see efforts by unauthorized individuals to gain improper access to information and financial data. These efforts will grow more sophisticated with the never-ending expansion of computer power. For acquirers, processors, and merchants, sophisticated new security methods and procedures will help in a number of ways. Reduced fraud rates will lower operating costs, putting money back into the pockets of everyone. New customers will be attracted to innovative forms of electronic payment combined with value-added applications, as they feel more secure about the level of protection provided. In addition, existing customers will also enjoy increased confidence in the industry’s ability to protect personal information and safeguard funds—leading to greater customer satisfaction and long-term retention.

VeriFone is continuing to take a leadership role in helping to drive the development and implementation of new security standards, and by being first to market with fully compliant PCI-PED products, including touch screen terminals perfect for kiosk implementations. The company offers an exceptionally broad line of hardware and software solutions that incorporate the latest technology and support widely accepted security standards.

The next generation of consumer oriented self-service kiosks need secured, trusted, electronic payment. VeriFone, as the global payments industry leader since 1981, can help you deliver secured payment in your kiosk applications that are certified not only today, but with the ability to continue that security and certification well into the challenges and opportunities of tomorrow.

For more information on VeriFone Kiosk Solutions, please email retail@verifone.com or visit www.verifone.com.



© 2006 VeriFone, Inc. All rights reserved. VeriFone, the VeriFone logo, Omni, PCCharge, Verix, Vx, and VeriShield are either trademarks or registered trademarks of VeriFone in the United States and/or other countries. All features and specifications are subject to change without notice. 3/06 Rev A.