



Protecting Cardholder Information: The Elusive Goal

An innovative solution that ensures payment transactions and cardholder information are encrypted continuously at the point of sale provides retailers the most comprehensive and effective means yet of thwarting criminal attempts to capture payment card data. And it requires no changes to most POS applications or systems.

Executive Summary

The retail environment is a tempting target for criminals intent on capturing cardholder information to create counterfeit payment cards or commit other fraudulent acts. Retailers may have hundreds or thousands of store locations, with many times that number of connected payment terminals and devices, systems, and networks. Employees often number in the tens of thousands, and high turnover results in many being in their first few years on the job. New store openings, new system deployments, and upgrades of current payment systems create an ever-changing payment environment for large and small retailers alike that is extremely difficult to continually secure—leading to a likelihood of data breaches.

While growing numbers of retailers are in compliance with the latest Payment Card Industry Data Security Standard (PCI DSS) control objectives, this is not enough to prevent compromises of cardholder data. The National Retail Federation (NRF) recently stated, “It is unlikely PCI will ever be able to keep pace with the continually evolving sophistication of the professional hacker, or anticipate every possible variation of future attacks.”

The biggest problem is that current PCI DSS guidelines do not require cardholder information to be encrypted end-to-end. Customer identities, primary account number (PAN) data, and full-track card data are often “in the clear” during authorization in the payment terminal, and when transmitted to a retailer’s or acquirer’s host processing server. This gives criminals all the opportunities they need.

VeriFone’s VeriShield Protect is an exclusive, turnkey solution that encrypts cardholder information the moment a card is swiped, and maintains this encryption while cardholder data is in a retailer’s POS system, network, or server. This helps protect against data compromises, even in the event of security breaches. And it often requires minimal changes to POS software, retail systems, or store procedures.

Content

Executive Summary	2
Are Data Compromises in the Cards?	4
Addressing Payment System Vulnerabilities	5
Changing the Game: Focusing on Data Compromises Rather Than on Data Breaches	7
Achieving End-To-End Encryption with VeriShield Protect	8
VeriShield Protect	9
Semtek Decryption Appliance	10
Cipher Device Metrics Server (CDMS)	12
Paying Significant Benefits for Retailers, Acquirers, and Processors	13
Conclusion	14

Are Data Compromises in the Cards?

Security breaches involving payment cards have been in the news with distressing regularity in recent years.

“Banks claim credit card breach affected 94 million accounts...”

“Security breach fallout reaches 200,000 debit card holders...”

“Hackers steal credit-card numbers from R.I state web site...”

“Credit card company reaches settlement for data breach...”

Unfortunately, the handling and storage of card data by retailers presents a constant threat of fraud and identity theft. Robert McCullen, chief executive of AmbironTrustwave Holdings, a Chicago-based security firm that has serviced about 30,000 businesses, says that in the past two years it has handled more than 200 incidents of POS breaches, and the number of incidents in 2006 doubled over the previous year.

An October 2007 study of more than 280 card compromise investigations conducted by Trustwave found that:

- 74% of all cardholder data compromises occurred in traditional brick-and-mortar environments with card-present transactions
- 71% of the data compromises targeted point-of-sale (POS) system software, with online shopping carts a distant second at 21%
- 61% of the data compromises were the fault of a third party—such as a POS developer, integrator, or IT technician—not following the latest PCI DSS guidelines, leaving merchants vulnerable to attack.
- An overwhelming 96% of the data compromises are occurring because non-compliant software solutions are storing payment card track data post authorization—which is never permitted under PCI DSS rules—and merchants are not aware of this until it is too late.

Without a doubt, retailers are at considerable risk of a data breach today, and the liability from these breaches can be daunting. Forrester Research says that a payment security breach can cost from \$90 to \$305 per record, meaning that the cost of a single, significant breach involving thousands or millions of records could run into the millions or even billions of dollars.

The Ponemon Institute's "2007 Annual Study: U.S. Cost of a Data Breach" studied the costs incurred by 35 organizations that suffered a data breach and found that the average cost per reporting company was more than \$6.3 million per breach.

In addition to the monetary impact, there is also the potential damage to the relationship between an organization and its customers. According to a new study by Javelin Strategy & Research, security breaches caused 55% of victims to be less trusting of the breached organization with their account information, and 30% said they would never again purchase goods or services from the affected organization. Some 33% of those surveyed said they closed their accounts after the breach, and 29% said they would not maintain a relationship with the breached organization in the future. Industry experts point out it can take years to regain customer loyalty once it has been lost, if it can be regained at all.

Although stored data in non-compliant software has been the primary point of attack, many schemes are targeting pre-authorization data and other system and network vulnerabilities as well.

Although stored data in non-compliant software has been the primary point of attack, many schemes are targeting pre-authorization data and other system and network vulnerabilities as well.

Addressing Payment System Vulnerabilities

The greatest difficulty for retail organizations, processors, and acquirers is not identifying the vulnerabilities in today's payment systems, but rather addressing those vulnerabilities in an effective manner. The complexities of the typical payment system provide a myriad of opportunities for criminal attacks, and it's virtually impossible to lock down every one. (See Figure 1.)

Payment System Vulnerabilities

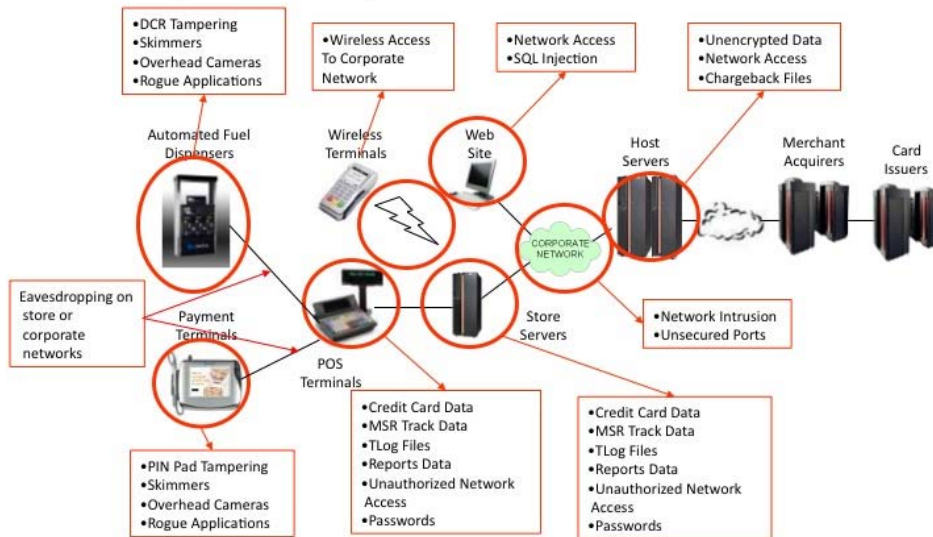


Figure 1

Attacks can take place against countertop payment devices or automated fuel dispensers using skimmers or rogue applications downloaded into the devices and designed to capture credit card and magnetic stripe reader track data, or even concealed overhead cameras. Electronic cash registers are attractive targets of theft as well. Wireless or wired networks invite eavesdropping to intercept valuable data. Even store servers, host servers, and corporate networks are in play—with data often moving unencrypted between points of processing.

To address these vulnerabilities and protect customer card data, the card associations that make up the PCI Security Standards Council—including American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International—developed the PCI DSS guidelines. PCI DSS is a multifaceted security guideline that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protections. This comprehensive standard is intended to help organizations proactively protect customer account data.

For many organizations, complying with PCI DSS requires:

- Upgrades or modifications to ensure ALL applications that capture, manage, transmit, or store cardholder information within the enterprise meet PA DSS (formerly PABP)

- Upgrade of the existing wired/wireless networking infrastructure to state-of-the-art, high-security routers, switches, and hubs
- Wholesale changes to passwords and other system access security policies within the enterprise
- Costly, annual audits from approved third-party auditors

Even with these efforts, the chances that all criminal attacks on cardholder data can be thwarted are small. There are simply too many points of potential failure, where unencrypted copies of data may be stored, or encryption keys may be held within insecure devices such as PC-based POS systems or servers that criminals could use to extract cardholder data. No two retail systems are alike, so no single solution can protect against all data breaches. Security monitoring and auditing can be difficult or costly, particularly on the most complex networks. Plus any system change—no matter how small—is costly and time-consuming, and requires end-to-end recertification.

Further, as cardholder security measures become more sophisticated, so too do the methods used to find ways to breach these protections. A system or network is only secure until the next upgrade, employee or third-party provider issue, or yet-to-be discovered security flaw is exploited.

Being in compliance with PCI DSS guidelines does not necessarily mean an organization is secure, simply that it is compliant.

Changing the Game: Focusing on Data Compromises Rather Than on Data Breaches

While it may be impossible to ever effectively lock down every element of a payment system infrastructure to prevent cardholder *data breaches*, there is an answer to virtually eliminate *data compromises*: end-to-end encryption.

- *"All debit and credit card transactions should be encrypted from end to end. That should be the minimum. It's astonishing that isn't the standard of PCI, which only requires encryption when transmitting over a public network such as IP. "*

—William Homa Ex-CIO, Hannaford Bros. Supermarkets

A system or network is only secure until the next upgrade, employee or third-party provider issue, or yet-to-be discovered security flaw is exploited. Being in compliance with PCI DSS guidelines does not necessarily mean an organization is secure, simply that it is compliant.

According to a story in the *Boston Globe*, Hannaford Bros.—a 350-store supermarket chain located in the Northeastern United States—suffered a breach of its payment systems that may have provided criminals access to an estimated four million credit and debit cards issued by 70 banks across the country. The data was stolen sometime between when customers swiped their cards at the store’s payment devices and when the transactions were authorized. The problem is that Hannaford, like most retailers, was routinely transmitting customer information and full card track data in the clear between payment devices and the processing host. The most concerning element of the story is that Hannaford’s process apparently fully complied with the latest industry standards for payment security at the time the data was intercepted.

That’s why PCI DSS’s stipulation that “transmission of all cardholder data across open, public networks must be encrypted” is not nearly enough. To effectively secure cardholder information, all primary account number (PAN) and magnetic-stripe card track data must be encrypted at the POS, from the instant the card is swiped until the transaction is received by the processing host.

End-to-end encryption offers a number of key benefits:

- Increased security
- Protection of card data
- Better safeguards for consumer information
- Reduced expenses in complying with PCI DSS objectives and guidelines as they continue to evolve.

In the past, encrypting non-PIN transactions at payment devices and maintaining that encryption until received by the processing host would have been exceptionally challenging and prohibitively expensive for most retailers. Now, there is an effective solution from VeriFone, the worldwide leader in payments.

Achieving End-to-End Encryption with VeriShield Protect

VeriFone’s VeriShield Protect is a revolutionary payment card security solution that virtually ensures data cannot be compromised, even in the event of a breach. Just as important, it can be economically implemented without requiring any changes to most existing POS or enterprise applications, and while transmitting data over the same PCI-compliant networks in use today.

VeriShield Protect encrypts all cardholder information and card track data—from PIN or non-PIN cards—continuously from the

That’s why PCI DSS’s stipulation that “transmission of all cardholder data across open, public networks must be encrypted” is not nearly enough. To effectively secure cardholder information, all primary account number (PAN) and magnetic-stripe card track data must be encrypted at the POS, from the instant the card is swiped until the transaction is received by the processing host.

moment a card is swiped until the data is received and decrypted using a high-performance appliance in a retailer's secure data center or at the processing host of a third-party service provider, acquirer, or processor. In addition, VeriShield Protect offers merchants and acquirers real-time monitoring of their security status and level of risk within their entire payment system infrastructure.

The solution consists of three components:

- VeriShield Protect—For encryption at the retail POS
- A secure Decryption Appliance—For high-performance decryption at a secure host processing site
- Cipher Device Metrics Server (CDMS)—Real-time monitoring system from Semtek

Let's take a closer look at the three components.

VeriShield Protect

VeriShield Protect is a turnkey solution that employs a highly sophisticated technology called Hidden Triple Data Encryption Standard (H-TDES™), an encryption technology created by Semtek Innovative Solutions Corporation. VeriFone and Semtek have partnered to help VeriFone's retail clients deal with the epidemic of payment card data breaches that are now constantly in the news.

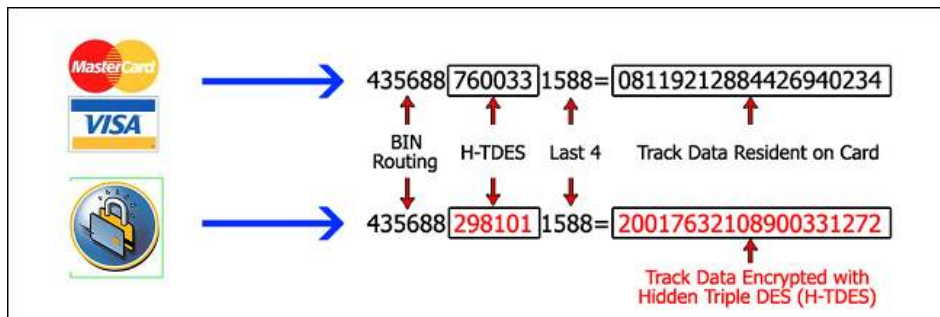


Figure 2

When a payment card is read (see Figure 2), patented algorithms encrypt most card data while preserving essential portions—such as bin routing identifiers to prompt clerks for PIN-based transactions or the last four numbers of the PAN for printing receipts and researching chargebacks—in unencrypted form.

All encryption takes place in VeriFone's existing PCI PED-approved payment devices, so not even the terminals are "aware"

the data is encrypted. Each device is also protected by VeriShield Retain file authentication, which prevents rogue applications or other unauthorized software from being downloaded and installed.

VeriShield Protect's end-to-end encryption effectively shields the merchant from the details of the consumer's card account data, so the retailer is never in possession of the data. It is compatible with all types of cards (credit, PIN debit, signature debit, loyalty, fleet, pre-paid, and gift cards). Encryption can be eliminated, if desired, for certain classifications of cards, such as loyalty or house cards.

While VeriShield Protect may not remove all liability in the unlikely case of a data compromise, the fact that a merchant never is in possession of unencrypted data would likely reduce any penalties that might be assessed.

VeriShield Protect's end-to-end encryption effectively shields the merchant from the details of the consumer's card account data, so the retailer is never in possession of the data.

Semtek Decryption Appliance

The Semtek Decryption Appliance is used to decrypt the H-TDES-encrypted cardholder data, once the transaction has been authorized and the data has been transmitted to a secure host-processing server.

There are three ways to handle the VeriShield Protect solution: Semtek-Hosted, Retailer-Hosted, or Processor-Hosted.

Semtek-Hosted Solution

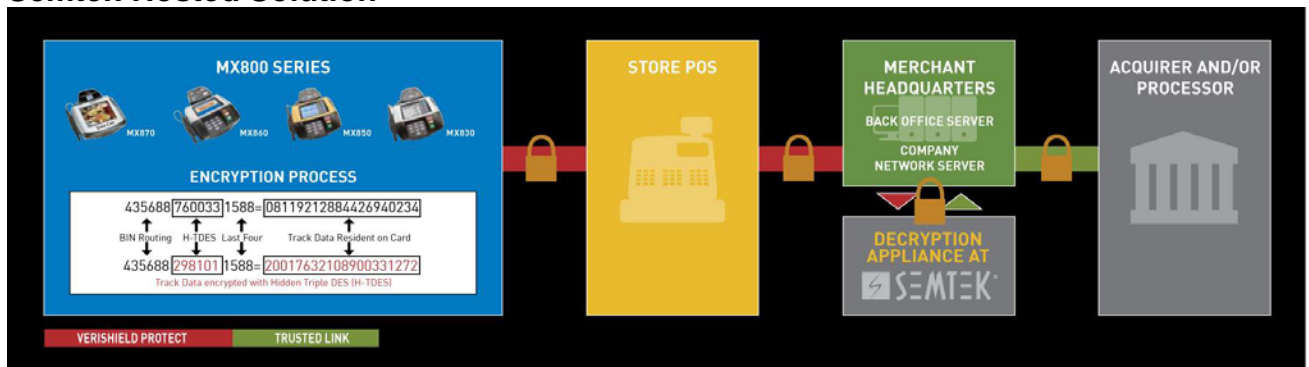


Figure 3

With the Semtek-Hosted option (see Figure 3), retailers enjoy the ultimate peace of mind. Once the retailer's network gateway has been modified to communicate with the Decryption Appliance, all implementation, maintenance, upgrades, and support are managed by Semtek's highly professional staff in a secure data center. This enables the retailer to focus on its core business and

leave the information technology concerns to a provider well-equipped to handle any challenges.

Retailer-Hosted Solution



Figure 4

The Retailer-Hosted option (Figure 4), under which the Semtek Decryption Appliance is installed in a secure environment at the retailer's data center, provides the ultimate control and flexibility for the retail organization. Although Semtek does provide maintenance and support through a comprehensive Service Level Agreement (SLA), all operational and security responsibilities lie with the retailer.

Some modifications of the retailer's network gateway are likely to be needed to communicate with the appliance, but no changes will be required for most POS applications or for the networks used to transmit payments. This approach is tailor-made for retailers with established IT organizations accustomed to managing complex security solutions.

Processor-Hosted Solution



Figure 5

The Processor-Hosted option (Figure 5) provides the optimal end-to-end solution from a security perspective. By encrypting payment data at the POS and not decrypting it until the

transaction is completely out of the merchant's payment infrastructure and at the processor's secure data site, the retailer is removed entirely from the risks inherent in payment transactions, from the management control required over the Decryption Appliance.

Depending upon implementation, no or minimal changes may be required to a retailer's payment gateway, further reducing implementation complexity and costs. Obviously, this option requires the close involvement and support of the retailer's payment processor in setting up and managing the Semtek Decryption Appliance.

Cipher Device Metrics Server (CDMS)

The final component of the VeriShield Protect solution is CDMS, a highly sophisticated monitoring and alert system provided by Semtek that offers retailers and acquirers a real-time understanding of the security status and risks involved in processing payments.

How CDMS Works

The Decryption Appliance pushes data out to the CDMS during the authorization process via a secured connection and web services. The CDMS accesses a database to compare digital signatures for individual transactions, provides metrics on how devices are performing from a security standpoint, and has the ability to initiate fraud alerts in real time for issuers, processors, and even regulatory agencies.

In addition to flagging fraudulent activity, alerts can be used to notify retailers or processors when a task must be completed to remain compliant, such as in the case of "rolling over" encryption keys. Rather than "rear-view" audits—which often provide information that's too little too late—all parties in the payment chain get the real-time information they need, down to a transaction level.

Processors can also use CDMS to obtain a definitive real-time view of their entire portfolio on transactions, without having to rely on merchant self-reporting. By using CDMS's XML API, processors can create PCI-compliant status reports for merchants by appending it to existing reports, or can offer the reports as a new service. Reports on all of the data tracked by the CDMS are available 24/7 via VeriFone's XML API or web portal.

By encrypting payment data at the POS and not decrypting it until the transaction is completely out of the merchant's payment infrastructure and at the processor's secure data site, the retailer is removed entirely from the risks inherent in payment transactions, from the management control required over the Decryption Appliance.

To ensure integrity and compliance with PCI DSS guidelines, the Decryption Appliances do not export any track data or PANs. Instead, one-way hash codes of selected data elements are exported from the Decryption Appliances to the CDMS.

Paying Significant Benefits for Retailers, Acquirers, and Processors

The VeriShield Protect solution provides a wide range of benefits for all entities in the payment chain.

To begin, the solution allows retailers to cost-effectively address three of the most difficult and expensive PCI DSS requirements.

- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Requirement 5: Restrict physical access to data

VeriShield Protect not only helps retailers meet each of these requirements right at the payment device without requiring changes to most POS applications farther upstream, but it also goes well beyond what's specified in PCI DSS Requirement 4 by encrypting data for transmission between a retailer's payment devices and POS terminals, across the retailer's private internal WANs, and over other internal networks.

Among the other key benefits are:

- Cardholder data is never exposed in the clear in the POS environment
- Real-time monitoring improves encryption compliance and reduces the impact of costly audits, loss-prevention methods, and potential breaches
- There's little or no impact on current POS systems and payment networks—no degradation of performance, and no changes required for most existing software
- BIN range checking continues to function as is, and non-payment cards can be processed without encryption, if desired
- Cardholders are not impacted

- Hosted Semtek solution provides a worry-free, hassle-free option—with Semtek handling all the details.

Conclusion

From customer-activated payment systems to POS and Internet-based payment solutions and peripherals, VeriFone has the right solutions to meet the payment needs of multi-lane retailers, acquirers, and processors.

VeriFone makes it easy for merchants to accept a variety of card-based payments and enjoy the revenue-generating potential of value-added services at the point of sale. VeriFone system solutions:

- Are used by millions of shoppers daily in supermarkets, drug stores, video stores, and mass merchandisers
- Support credit, debit, electronic benefits transfer (EBT), loyalty cards, gift cards, and other forms of electronic payment
- Bring new technologies such as check conversion and imaging, smart cards, and electronic signature capture to the point of sale
- Are built with a commitment to reliability, security, and ease of use.

With VeriShield Protect, VeriFone offers retailers, acquirers, and processors the assurance that payment transactions and cardholder data are secure at the POS. Even if a data breach were to occur, end-to-end encryption will virtually eliminate the possibility of a data compromise. PCI DSS compliance costs can be substantially reduced. And a sophisticated monitoring solution enables retailers and processors to track transaction security and fraud risks in real time.

VeriShield Protect is available today on VeriFone's MX800 Series products. It will also be available on VeriFone's V^x Solutions and Secure PumpPAY platforms in the coming months.

For further information about VeriFone's exclusive VeriShield Protect, call your VeriFone sales representative or log onto VeriFone.com/verishield-protect. Lock down payment systems with VeriShield Protect.