VALUED
MERCHANT SERVICES

# PA DSS and what it means to you and your customers

## Turning risk into reward

VeriFone
THE WAY TO PAY™

VALUED MERCHANT SERVICES


# Merchant *In*security

92% of all compromised merchants were Level 4, according to a recent study

Trustwave Information Security & Compliance

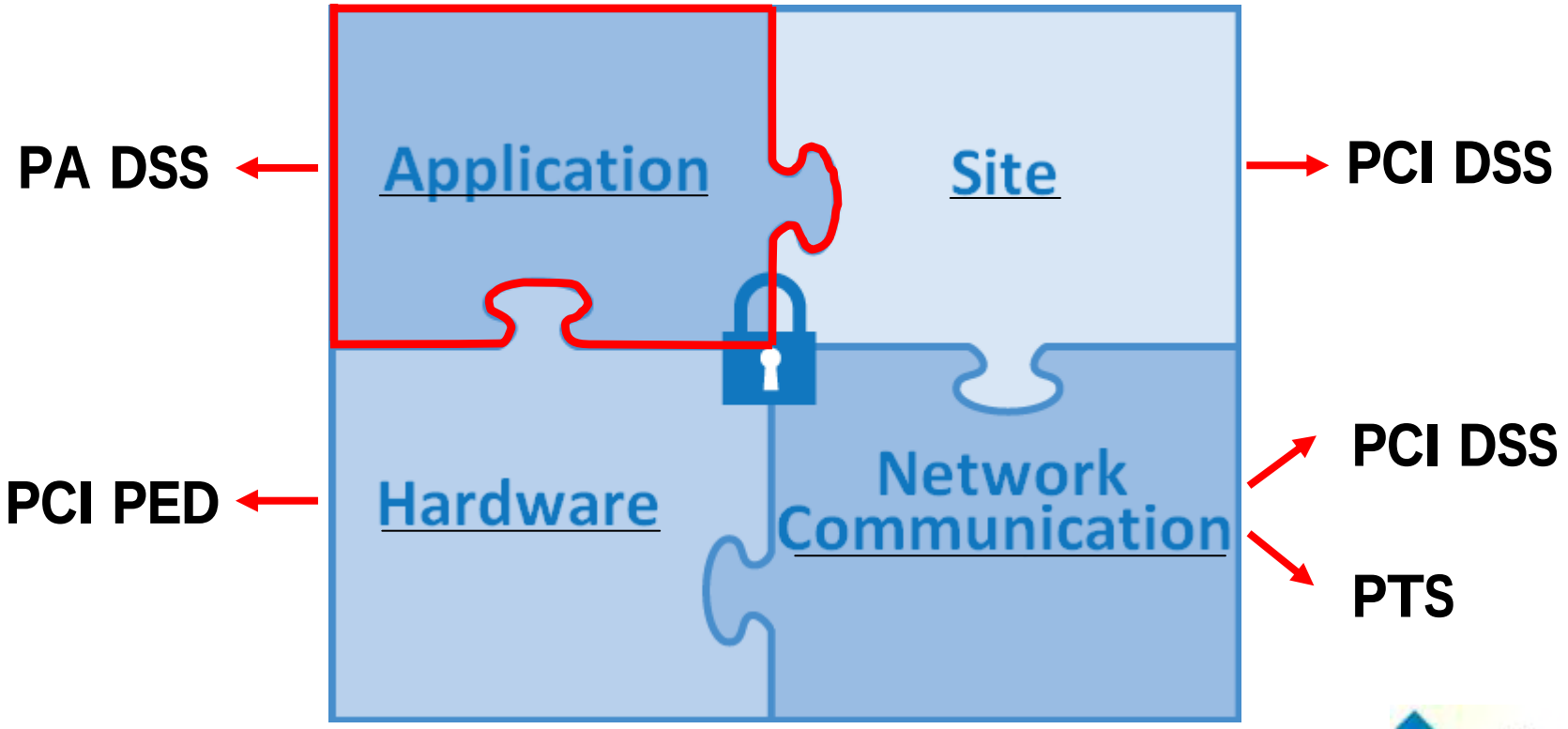
- March 2008 Global Compromise Statistics – review of 350 merchant breaches by industry leading security firm Trustwave

VeriFone THE WAY TO PAY™

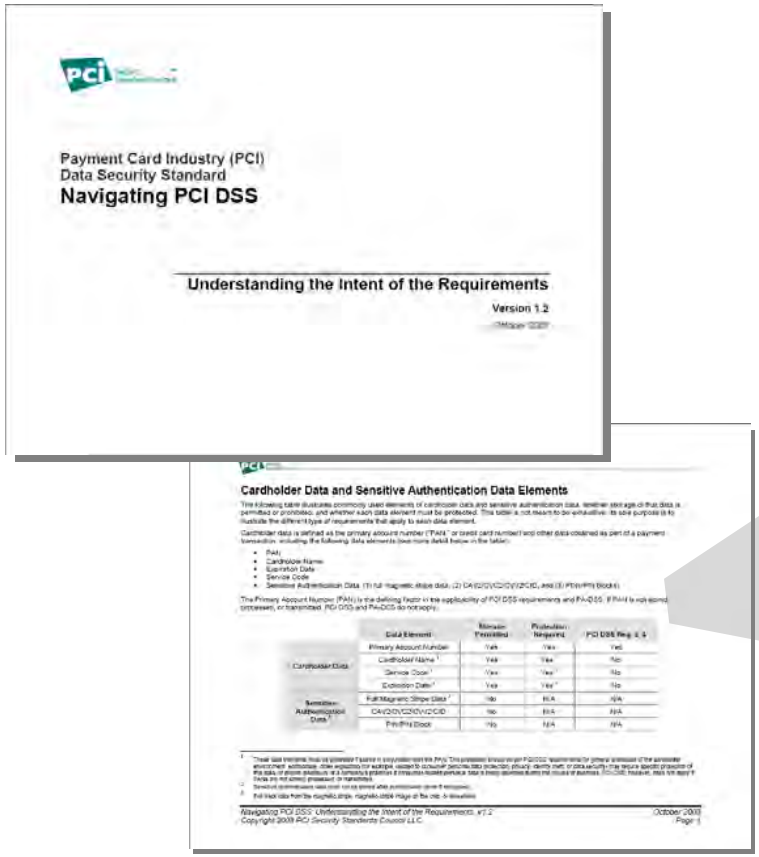
- **PCI SSC**
  - Payment Card Industry Security Standards Council
  - Founded by 5 major card associations
  - Establishes security guidelines
  - Card associations responsible for enforcement


- **Predominant mandates guiding POS terminal, transaction, and merchant data security**
  - PCI DSS – Payment Card Industry Data Security Standard
  - PA DSS – Payment Application Data Security Standard
  - PCI PED – Payment Card Industry PIN Entry Device
  - PTS - MasterCard Point of Sale Payment Transaction Security

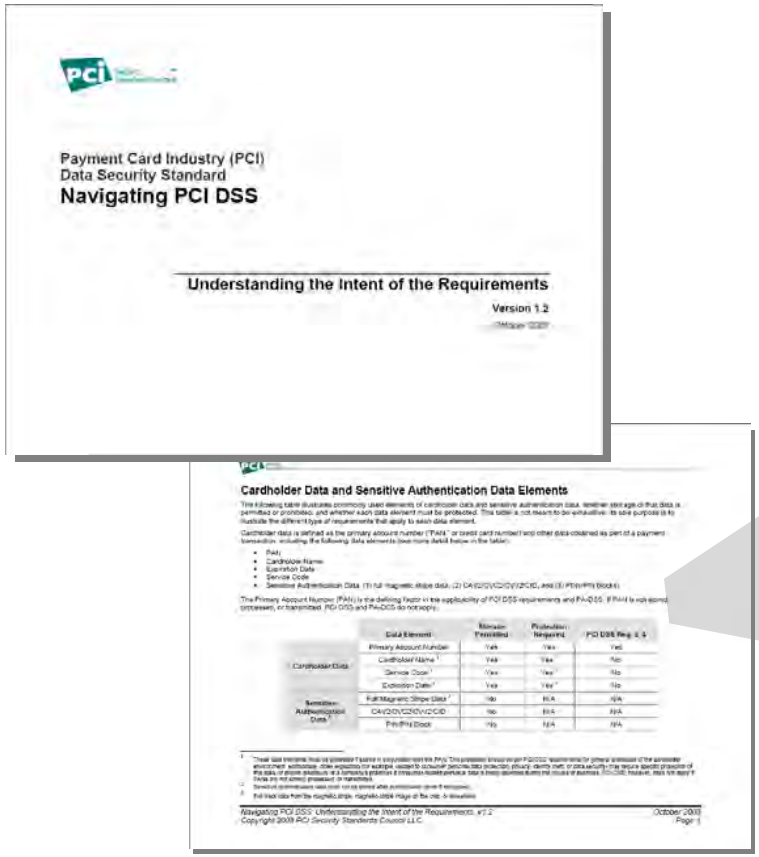
# The Security Puzzle




VeriFone
THE WAY TO PAY™




The Primary Account Number (PAN) is the defining factor in the applicability of PCI DSS requirements and PA-DSS. If the PAN is not stored, processed, or transmitted, PCI DSS and PA-DSS do not apply.




Said another way:

All payment acceptance devices process and transmit PAN data, and must be proven to not store PAN data. Therefore PCI DSS and PA-DSS does apply.

**Result: Merchant solutions involving POS terminals/payment applications do not get a free pass.**

# How does this impact stand-alone terminals?

**Payment applications that are resident in standalone point-of-sale terminals are subject to the PA-DSS requirements if:**

(1) The payment application vendor does not provide secure remote updates, troubleshooting, access and maintenance

(2) The terminals have connection to any of the merchant's systems or networks → Direct link (e.g. RS232, USB) or router

(3) Sensitive authentication data is stored after authorization → How can merchants definitively verify??

(4) The terminals connect to the merchant's acquirer or processor via anything other than a direct and private line → Other than Dial or Lease Line

# Relationship between PCI DSS and PA DSS

## PCI DSS Requirements

**Build and Maintain a Secure Network**

*Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
*Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters

**Protect Cardholder Data**

*Requirement 3:* Protect stored cardholder data
*Requirement 4:* Encrypt transmission of cardholder data across open, public networks

**Maintain a Vulnerability Management Program**

*Requirement 5:* Use and regularly update anti-virus software
*Requirement 6:* Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**

*Requirement 7:* Restrict access to cardholder data by business need-to-know
*Requirement 8:* Assign a unique ID to each person with computer access
*Requirement 9:* Restrict physical access to cardholder data

**Regularly Monitor and Test Networks**

*Requirement 10:* Track and monitor all access to network resources and cardholder data
*Requirement 11:* Regularly test security systems and processes

**Maintain an Information Security Policy**

*Requirement 12:* Maintain a policy that addresses information security

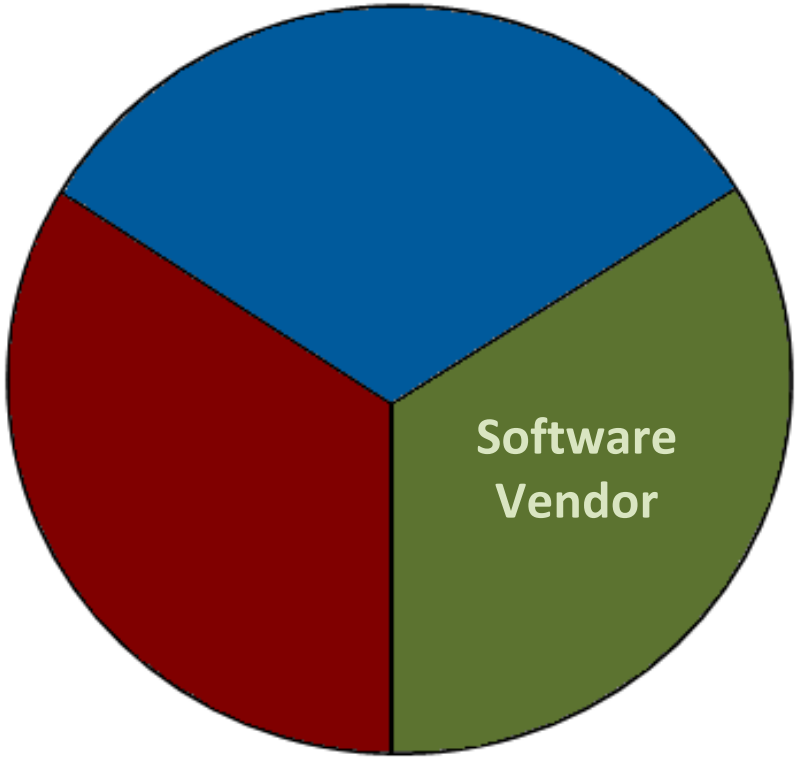
VALUED MERCHANT SERVICES

**PA DSS is a component that facilitates merchant's PCI DSS compliance**

VeriFone THE WAY TO PAY™

# Dividing the responsibilities

## PA-DSS Responsibility



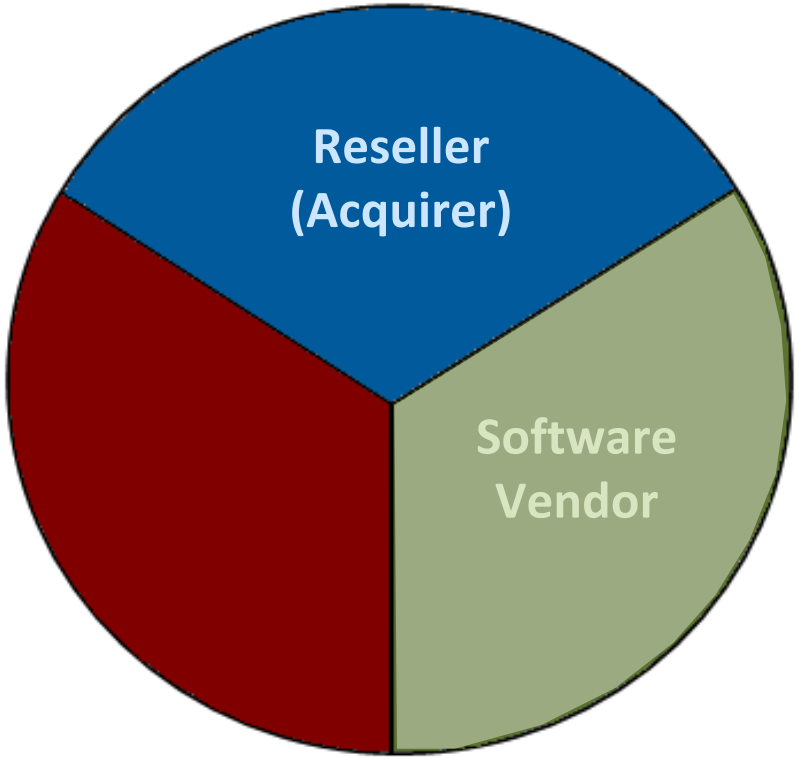

- Develop PA-DSS compliant payment applications that facilitate and do not prevent their customers' PCI DSS compliance
- Follow PCI DSS requirements when processing, storing, or transmitting card data
- Pass PA DSS audit
- Create a *PA-DSS Implementation Guide*
- Educate customers, resellers on configuring & installing in PCI DSS compliant manner

- Source: PCI PA-DSS Program Guide v. 1.2

VeriFone
THE WAY TO PAY

# Dividing the responsibilities

## PA-DSS Responsibility



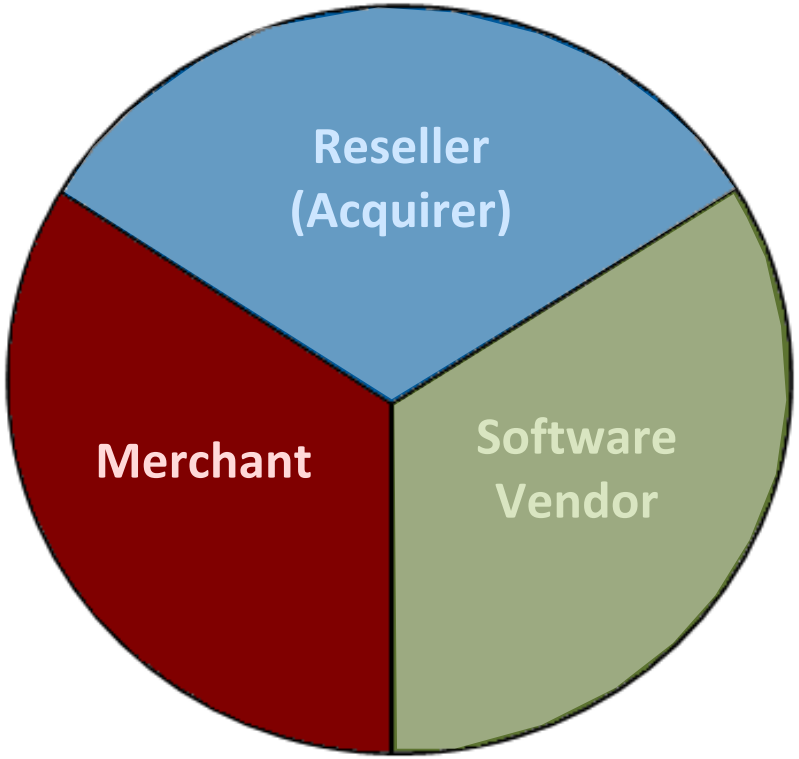

- Implementing only PA-DSS compliant payment applications into a PCI DSS compliant environment
- Configuring such payment applications according to the *PA-DSS Implementation Guide* provided by the vendor
- Configuring such payment applications in a PCI DSS compliant manner
- Servicing such payment applications according to the *PA-DSS Implementation Guide* and PCI DSS.

- Source: PCI PA-DSS Program Guide v. 1.2

VeriFone
THE WAY TO PAY™

# Dividing the responsibilities

## PA-DSS Responsibility

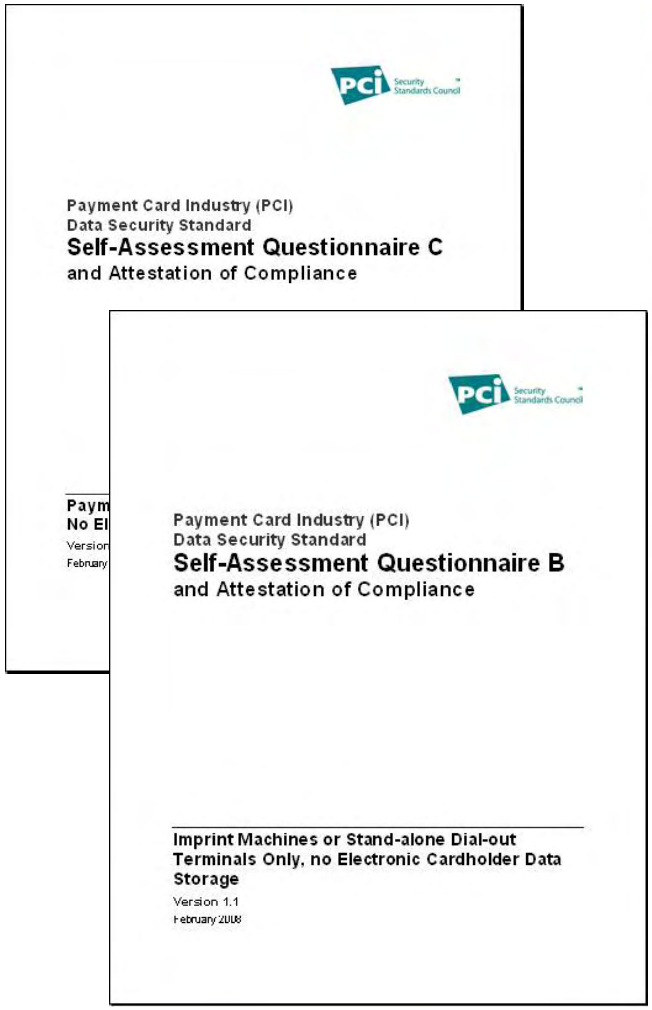



- Implementing a PA-DSS compliant payment application into a PCI DSS compliant environment
- Configuring the payment application according to the *PA-DSS Implementation Guide* provided by the vendor
- Configuring the payment application in a PCI DSS-compliant manner
- Maintaining the PCI DSS-compliant status for both the environment and the payment application configuration.

- Source: PCI PA-DSS Program Guide v. 1.2

VeriFone
THE WAY TO PAY™

# Self-Assessment Questionnaire for Level 4 Merchants




## Before you Begin

### Completing the Self-Assessment Questionnaire

SAQ C has been developed to address requirements applicable to merchants who process cardholder data via payment applications (for example, POS systems) connected to the Internet (via high-speed connection, DSL, cable modem, etc.), but who do not store cardholder data on any computer system. These payment applications are connected to the Internet either because:

1. The payment application is on a personal computer connected to the Internet, or
2. The payment application is connected to the Internet to transmit cardholder data.

These merchants are defined as SAQ Validation Type 4, as defined here and in the *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*. Validation Type 4 merchants process cardholder data via POS machines connected to the Internet, do not store cardholder data on any computer system, and may be either brick-and-mortar (card-present) or e-commerce or mail/telephone-order (card-not-present) merchants. Such merchants must validate compliance by completing SAQ C and the associated Attestation of Compliance, confirming that:

- Your company has a payment application system and an Internet connection on the same device;
- The payment application/Internet device is not connected to any other systems within your environment;
- Your company retains only paper reports or paper copies of receipts;
- Your company does not store cardholder data in electronic format; and
- Your company's payment application vendor uses secure techniques to provide remote support to your payment system.

Each section of this questionnaire focuses on a specific area of security, based on the requirements in the PCI Data Security Standard.

https://www.pcisecuritystandards.org/saq/instructions.shtml

VeriFone
THE WAY TO PAY

# How can a merchant be sure in answering these questions?

## Protect Cardholder Data

*Requirement 3: Protect stored cardholder data*

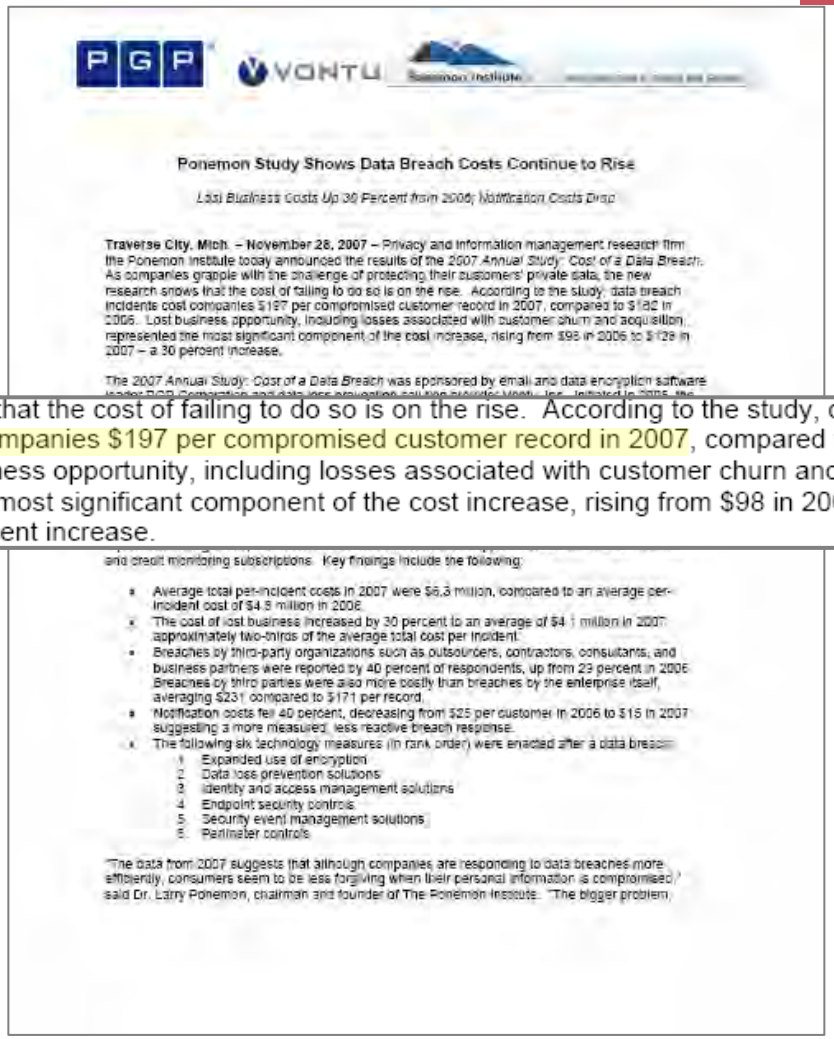
| | Question | Response: | YES | NO |
|---|---|---|---|---|
| 3.2 | Do all systems adhere to the following requirements regarding storage of sensitive authentication data? | | ? | ? |
| 3.2.1 | Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data.<br>*In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.* | | ? | ? |
| 3.2.2 | Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. | | ? | ? |
| 3.2.3 | Do not store the personal identification number (PIN) or the encrypted PIN block. | | ? | ? |
| 3.3 | Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed).<br>*Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point-of-sale [POS] receipts).* | | ? | ? |


VeriFone
THE WAY TO PAY™

# Merchant's risk of not answering with confidence

## What is at risk?

- Loss of customers
- Loss of reputation



Ponemon Study Shows Data Breach Costs Continue to Rise

*Lost Business Costs Up 30 Percent from 2006; Notification Costs Drop*

**Traverse City, Mich. – November 28, 2007** – Privacy and information management research firm the Ponemon Institute today announced the results of the 2007 *Annual Study: Cost of a Data Breach*. As companies grapple with the challenge of protecting their customers' private data, the new research shows that the cost of failing to do so is on the rise. According to the study, data breach incidents cost companies $197 per compromised customer record in 2007, compared to $182 in 2006. Lost business opportunity, including losses associated with customer churn and acquisition, represented the most significant component of the cost increase, rising from $98 in 2006 to $128 in 2007 – a 30 percent increase.

The *2007 Annual Study: Cost of a Data Breach* was sponsored by email and data encryption software

research shows that the cost of failing to do so is on the rise. According to the study, data breach incidents cost companies $197 per compromised customer record in 2007, compared to $182 in 2006. Lost business opportunity, including losses associated with customer churn and acquisition, represented the most significant component of the cost increase, rising from $98 in 2006 to $128 in 2007 – a 30 percent increase.

and credit monitoring subscriptions. Key findings include the following:

- Average total per-incident costs in 2007 were $6.3 million, compared to an average per-incident cost of $4.8 million in 2006.
- The cost of lost business increased by 30 percent to an average of $4.1 million in 2007, approximately two-thirds of the average total cost per incident.
- Breaches by third-party organizations such as outsourcers, contractors, consultants, and business partners were reported by 40 percent of respondents, up from 23 percent in 2006. Breaches by third parties were also more costly than breaches by the enterprise itself, averaging $231 compared to $171 per record.
- Notification costs fell 40 percent, decreasing from $25 per customer in 2006 to $15 in 2007, suggesting a more measured, less reactive breach response.
- The following six technology measures (in rank order) were enacted after a data breach:
  1. Expanded use of encryption
  2. Data loss prevention solutions
  3. Identity and access management solutions
  4. Endpoint security controls
  5. Security event management solutions
  6. Perimeter controls

"The data from 2007 suggests that although companies are responding to data breaches more efficiently, consumers seem to be less forgiving when their personal information is compromised," said Dr. Larry Ponemon, chairman and founder of The Ponemon Institute. "The bigger problem

- Ponemon Institute
*2007 Annual Study: Cost of a Data Breach*

VeriFone
THE WAY TO PAY™

# What is at risk?

- Loss of customers
- Loss of reputation
- Liabilities resulting from bank fines
- Litigation
- Card association fines

**Loss or theft of account information**

Members, service providers or merchants must immediately report the suspected or confirmed loss or theft of any material or records that contain Visa cardholder data.

If a member knows or suspects a security breach with a merchant or service provider, the member must take immediate action to investigate the incident and limit the exposure of cardholder data.

If a Visa member fails to immediately notify Visa Inc. Fraud Control of the suspected or confirmed loss or theft of any Visa transaction information, the member will be subject to a penalty of $100,000 per incident.

Members are subject to fines, up to $500,000 per incident, for any merchant or service provider that is compromised and not compliant at the time of the incident.

- Visa CISP website

VALUED MERCHANT SERVICES

VeriFone THE WAY TO PAY™

# Options for your customers:

- Ignore the situation
- Pay for their own audit of the payment application
- “Trust” others with claims of compliancy
- Only accept solutions that have been verified as compliant through a qualified 3rd party source

# VeriFone provides the assurance your customers need


VALUED MERCHANT SERVICES

VeriFone THE WAY TO PAY™

## Protect Cardholder Data

*Requirement 3: Protect stored cardholder data*

| | Question | Response: | YES | NO |
|---|---|---|---|---|
| 3.2 | Do all systems adhere to the following requirements regarding storage of sensitive authentication data? | | ☒ | ☐ |
| 3.2.1 | Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data.<br>*In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.* | | ☒ | ☐ |
| 3.2.2 | Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. | | ☒ | ☐ |
| 3.2.3 | Do not store the personal identification number (PIN) or the encrypted PIN block. | | ☒ | ☐ |
| 3.3 | Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed).<br>*Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point-of-sale [POS] receipts).* | | ☒ | ☐ |

VeriFone
THE WAY TO PAY™

## Protect Cardholder Data

*Requirement 3: Protect stored cardholder data*

| | Question | Response: | YES | NO |
|---|---|---|---|---|
| 3.2 | Do all systems adhere to the following requirements regarding storage of sensitive authentication data? | | ☒ | ☐ |
| 3.2.1 | Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data.<br>*In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only these data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.* | | ☒ | ☐ |
| 3.2.2 | Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. | | ☒ | ☐ |
| 3.2.3 | Do not store the personal identification number (PIN) or the encrypted PIN block. | | ☒ | ☐ |
| 3.3 | Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed)?<br>*Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point-of-sale [POS] receipts).* | | ☒ | ☐ |

# With VeriFone, you can answer YES with confidence

VALUED MERCHANT SERVICES

VeriFone THE WAY TO PAY™


# For absolute certainty…
# Demand Proof

VALUED
MERCHANT SERVICES