Rice University
September 23, 2010
AGENDA

• Introduction to Fraud Training
• Merchant Standard Procedures
• Card Present
• Card Not Present
• Breach Procedures
• Intro to PCI Compliance
• Self-Assessment Questionnaires
• Approved Scanning Vendors (ASVs)
• Resource Links
• Questions
The Importance of Training

This training serves to provide you with the knowledge and skills necessary to ensure credit card security. It is important to recognize that everyone, not just the credit card companies, benefit from the effective application of credit card security measures:

Your customers
• Appreciate your ability to reduce the threat of identity theft
• Trust you to complete transactions without creating duplicate or invalid charges
• Enjoy peace of mind, knowing that their credit card information is in good hands

The university
• Takes pride in a skilled workforce
• Values your ability to build customer confidence
• Needs your help in limiting potential losses, fines & penalties

... and you!
• Will have confidence in your ability to safely and efficiently do your job
• Will recognize and evaluate key security features on valid cards
• Will be alert to the warning signs of fraud
• Will know that you can make informed decisions under pressure
Throughout the next few sections, you will learn about your role in retail fraud prevention and the appropriate steps to take if you feel that your unit's credit card security has been compromised. It is critical that you read, retain and refer to this information, as needed, so that your customers and the University are served as safely and efficiently as possible. Each section covers a unique and important part of credit card safety. This training is comprised of the following sections:

• **Card-Present Fraud Prevention** explores credit card security features and other prevention tactics for Card-Present (in-store) transactions.

• **Card-Not-Present Fraud Prevention** explores credit card security features and other prevention tactics for Card-Not-Present (mail, phone & online) transactions.

• **What to do if Security is Compromised** explains the steps for reporting a questionable card or customer, while ensuring your personal safety and the safety of other customers and co-workers.
Who It Applies To

This training is applicable to all campus personnel who have access to credit card information, either as a processor of credit card transactions or as a reviewer of reports that contain identifying credit card data. Throughout this training, the term “Rice Employee” is expanded to include anyone who has access to credit card information working in any capacity for the University including:

- Staff
- Students
- Faculty
- Administrators
- Temporary employees
- Volunteers

**Note:** The term "merchant" refers to any campus unit or department which accepts credit cards for payment - either in person or via other means, e.g. via the web.
Merchant Standard Procedures

Merchant Location requirements

1. Protect cardholder information so that only the last four digits of the credit card number are displayed or printed. Never send unencrypted Primary Account Numbers (PAN) by e-mail.

2. Store only credit card information that is critical to the business: name, account number, and expiration date.

3. Store only cardholder data that is encrypted or truncated, never credit card numbers.

4. Ensure that all transmissions of sensitive credit card data are encrypted.

5. Never store the three or four-digit Card Verification Value (CVV2) code in any form.

6. Do not release credit card information in any form unless there is a legitimate business purpose and then only after the request for information is reviewed and approved by the unit’s management.

7. Store and secure cardholder data in locked containers, in secured areas with limited access. Examples include electronic data, customer receipts, merchant duplicate receipts, reports, etc. Limit the amount of data stored and retention time to that which is required for business, legal, and/or regulatory purposes as documented by the department.

8. Perform an annual review of critical data storage to ensure that all security requirements are met.
Merchant Standard Procedures

9. Dispose of cardholder data according to a schedule based on business, legal and/or regulatory requirements as documented by the department. Cardholder data must be disposed of by overwriting or degaussing magnetic media; paper must be cross-shredded.

10. Provide all third party vendors with the University's credit card procedures.

11. Maintain written proof that all third party vendors are certified as PCI compliant.

12. Give any third party vendors access to credit card data only after a formal contract is signed that outlines the security requirements and requires adherence to the Payment Card Industry Security requirements.

13. Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.

14. Have procedures to help all personnel distinguish between employees and visitors, in areas where cardholder data is accessible.

15. Destroy or completely and securely remove all restricted data from computers and electronic media (including back-ups) before disposal, re-use, or re-assignment.
Security Elements

Each brand of credit card uses a set of unique design features and security elements to help merchants verify a card’s legitimacy. By knowing what to look for on a card, you can avoid inadvertently accepting a counterfeit card or processing a fraudulent transaction.

• Check the first digit in the account number. The first digit should always match the designated first digit for the card brand….AMEX=3, Visa=4, MasterCard=5, and Discover =6.
• Check for signs of tampering on signature panel. The word VOID or correction fluid on the signature panel means the card is invalid.
• Check the account number and security code (CVV2) on the signature panel. It should match the PAN on the front of the card
• If any card security features are missing or look altered, notify your supervisor and place a Code 10 call to the Authorization Center.
What to Look For On All Cards (using Visa as an example)

Compare the printed and embossed numbers.
A four-digit number is printed below the first four digits of the embossed account number on all valid Visa and MasterCard. These numbers should be identical. If the numbers are not identical or the printed number is missing, the card is not valid and should not be accepted.
Card Present transactions are those in which both the card and cardholder are present at the point of sale. Rice Merchants are required to take all reasonable steps to assure that the card, cardholder, and transaction are legitimate. Proper card acceptance begins and ends with sales staff and is critical to customer satisfaction and profitability.

**Doing it right at the point of sale**

Whether you are experienced or new to the job, following these few basic card acceptance procedures will help you to do it right, the first time and every time. The illustration below provides an overview of the card acceptance steps that are to be followed at the point of sale. Each step is explained in greater detail in this section.
Card Present - Transactions

It Pays to Swipe the Stripe
On the back of every credit and debit card, is a Magnetic stripe. The stripe contains the cardholder name, card account number, and expiration date, as well as special security information designed to help detect counterfeit cards. When the stripe is swiped through the terminal, this information is electronically read and relayed to the card issuer, who then uses it as crucial input for the authorization decision.

Note:
• Swipe the card to request transaction authorization.
• Hold the card throughout the entire transaction.

Verifying the Account Number
• Only the last four digits of the account or credit card number should be printed on a transaction receipt.
Card Present - Transactions

If a card doesn’t read when swiped

In some instances, when a card is swiped, the terminal will not be able to read the magnetic stripe or perform an authorization. When this occurs, it usually results from one of three causes:
• The terminal’s magnetic-stripe reader is dirty or out-of-order.
• The card is not being swiped through the reader correctly.
• The magnetic stripe on the card has been damaged or demagnetized.

Note: Damage to the card may happen accidentally, but it may also be a sign that the card is counterfeit or has been altered.
# Authorization Responses

During the authorization process, you should receive one of the responses listed in the following table, or one that is similarly worded:

<table>
<thead>
<tr>
<th>Response</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved</td>
<td>Card issuer approves the transaction. This is the most common response—about 95% of all authorization requests are approved.</td>
</tr>
<tr>
<td>Declined or Card Not Accepted</td>
<td>Card issuer does not approve the transaction. The transaction should not be completed. Return the card and instruct the cardholder to call the card issuer for more information on the status of the account.</td>
</tr>
<tr>
<td>Call, Call Center, or Referrals</td>
<td>Card issuer needs more information before approving the sale. Most of these transactions are approved, but you should call your authorization center and follow whatever instructions you are given. In most cases, an authorization agent will ask to speak directly with the cardholder or will instruct you to check the cardholder’s identification. <em>(See: Signature unsigned cards for acceptable forms of ID)</em>.</td>
</tr>
<tr>
<td>Pick-Up</td>
<td>This response indicates that the card issuer would like the card to be confiscated from the customer. However, Rice Employees should not attempt to pick up credit cards, even when the card issuer requests this action, as this could potentially cause confrontation and safety issues.</td>
</tr>
<tr>
<td>No Match</td>
<td>The embossed account number on the front of the card does not match the account number encoded on the magnetic stripe. Swipe the card again and re-key the last four digits at the prompt. If a “No Match” response appears again, it means the card is counterfeit. Discreetly notify your supervisor that it is necessary to make a Code 10 call.</td>
</tr>
</tbody>
</table>
Signature and Identification

The final step in the card acceptance process is to ensure that the customer signs the sales receipt and to compare that signature with the signature on the back of the card. When signing the receipt, the customer should be within your full view, and you should check the two signatures closely for any obvious inconsistencies in spelling or handwriting.

While checking the signature, you should also compare the name, account number, and signature on the card to those on the transaction receipt.
• Match the name and last four digits of the account number on the card to those printed on the receipt.
• Match the signature on the back of the card to the signature on the receipt. The first initial and spelling of the surname must match.

Note: The embossed name and signature do not need to be the same.
For suspicious or non-matching signature, notify your supervisor discreetly that it is necessary to make a Code 10 call.

Note: If the transaction is accepted with a non-matching signature and it turns out to be fraudulent, your business may be liable, even if all other procedures were followed.
While checking card security features, also make sure that the card is signed. An unsigned card is considered invalid and should not be accepted. If a customer gives you an unsigned card, the following steps must be taken:

1. Check the cardholder’s ID. Ask the cardholder for some form of official government identification containing their photograph, such as a driver’s license or passport. Social Security Cards are not acceptable forms of identification. The ID serial number and expiration date should be written on the sales receipt before you complete the transaction.

2. Ask the customer to sign the card. The card should be signed within your full view, and the signature checked against the customer’s signature on the ID. A refusal to sign means the card is still invalid and cannot be accepted. Ask the customer for another signed credit card.

3. Compare the signature on the card to the signature on the ID. If the cardholder refuses to sign the card, and you accept it, you may end up with financial liability for the transaction should the cardholder later dispute the charge.

Note: The words “Not Valid Without Signature” appear above, below, or beside the signature panel on most credit cards.
In Lieu of Signature

“See ID” in lieu of signature
Some customers write “See ID” or “Ask for ID” in the signature panel, thinking that this is a deterrent against fraud or forgery; that is, if their signature is not on the card, a fraudster will not be able to forge it. In reality, criminals don’t take the time to practice sign signatures: they use cards as quickly as possible after a theft and prior to the accounts being blocked. They are actually counting on your not to look at the back of the card and compare signatures—they may even have access to counterfeit identification with a signature in their own handwriting.
“See ID” or “Ask for ID” is not a valid substitute for a signature. The customer must sign the card in your presence, as stated above.

Note: A refusal to sign means the card is still invalid and cannot be accepted. Ask the customer for another signed credit card.
Suspicious Behavior

In addition to following all standard card acceptance procedures, be on the lookout for any Customer behavior that appears suspicious or out of the ordinary.

At the point of sale

• Purchasing large amounts of merchandise with seemingly no concern for size, style, color, or price
• Asking no questions or refusing free delivery on large items (for example, heavy appliances or televisions) or high-dollar purchases
• Trying to distract or rush sales associates during a transaction
• Making purchases, leaving the store, and then returning to make more purchases
• Making purchases either right after the store opens or just before it closes

Of course, peculiar behavior should not be taken as automatic proof of criminal activity. Use common sense and appropriate caution when evaluating any customer behavior or other irregular situation that may occur during a transaction. You know what kind of behavior is normal for your particular place of business.

If you feel really uncomfortable or suspicious about a cardholder or transaction, notify your supervisor discreetly that it is necessary to make a Code 10 call. In any situation where making the call with the customer present feels inappropriate or unsafe, complete the transaction, return the card, and make the call immediately after the customer leaves. See: Code 10 Calls for additional information.
Card Present - Code 10 Calls

Code 10 calls

Code 10 calls allow Rice merchants to alert card issuers of suspicious activity and to take appropriate action when instructed to do so. You or your supervisor should make Code 10 call to the voice authorization center whenever you are suspicious about a card, cardholder, or a transaction. The term “Code 10” is used so the call can be made at any time during a transaction without arousing a customer’s suspicions. To make a Code 10 call, you or your supervisor will call the credit card company’s voice authorization center, and say, “I have a Code 10 authorization request.”

It is important to note that Code 10 calls can be time consuming. The call may first be routed to a representative of your merchant bank who may need to ask you for some merchant or transaction details. You will then be transferred to the card issuer and connected to a special operator who will ask you a series of questions that can be answered with a simple Yes or no.

- Be prepared with merchant #, cardholder #, expiration date, and amount of sale.
- When connected to the special operator, answer all questions calmly and in a normal tone of voice. Your answers will be used to determine whether the card is valid.
- Follow all operator instructions.
- If the operator tells you to pick up the card, do so only if recovery is possible by reasonable and peaceful means. Rice employees are not obligated or expected to confiscate credit cards.
Card Present - Code 10 Calls

Making a Code 10 call after a transaction

Sometimes you may not feel comfortable making a Code 10 call while the cardholder is at the point of sale, or you may become suspicious of a cardholder who has already left the store even if the transaction was not completed.

It is important to know that Code 10 calls can be made even after a cardholder leaves the store. A Code 10 alert at that time may stop fraudulent card use at another location, or perhaps during a future transaction at your store.

Be prepared to provide as much customer information as you can - e.g. name on card, type of card (e.g. MasterCard) and card number.

**Code 10 Authorization Telephone Number**

1-800-944-1111  MC and VISA
1-800-528-5200 AMEX
Minimize Key Entered Transactions

Find causes and look for solutions

<table>
<thead>
<tr>
<th>Key-Entry Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damaged Magnetic-Stripe</td>
<td>Check magnetic-stripe readers regularly to make sure they are working.</td>
</tr>
<tr>
<td>Dirty Magnetic-Stripe</td>
<td>Clean magnetic-stripe reader heads several times a year to ensure continued good use.</td>
</tr>
<tr>
<td>Magnetic-Stripe Reader Obstructions</td>
<td>Remove obstructions near the magnetic-stripe reader. Electric cords or other equipment could prevent a card from being swiped straight through the reader in one easy movement.</td>
</tr>
<tr>
<td>Spilled Food or Drink</td>
<td>Do not place any food or beverages near the magnetic stripe reader. Falling crumbs or an unexpected spill could soil or damage the machines.</td>
</tr>
<tr>
<td>Anti-Theft Devices that Damage Magnetic Stripes</td>
<td>Keep magnetic anti-theft deactivation devices away from any counter area where customers might place their cards. These devices can erase a card's magnetic stripe.</td>
</tr>
<tr>
<td>Improper Card Swiping</td>
<td>Swipe the card once in one direction, using a quick, smooth motion. Never swipe a card back and forth. Never swipe a card at an angle; this may cause a faulty reading.</td>
</tr>
</tbody>
</table>
Card Not Present Requirements

**Merchant web site requirements**
- Visa/MasterCard require that certain content or features be included on your Web site. The following elements are intended to promote ease of use for online shoppers and reduce cardholder disputes and potential chargebacks.

**Complete description of goods and services.**
- Remember you have a global market, which increases opportunities for unintended misunderstandings or miscommunications. For example, if you sell electrical goods, be sure to state voltage requirements, which vary around the world.

**Customer service contact information.**
- This includes e-mail address and phone number. Online communication may not always be the most time-efficient or user-friendly for some customers. Including a customer service telephone number as well as an e-mail address promotes customer satisfaction.

**Return, refund, and cancellation policy.**
- This policy must be clearly posted on the merchant Web site.

**Delivery policy.**
- Rice Merchants set their own policies about delivery of goods, that is, if they have any geographic or other restrictions on where or under what circumstances they provide delivery. Any restrictions on delivery must be clearly stated on the web site.

**Country of origin.**
- The permanent address of your establishment must be listed on the web site including the street name, number, city, state, country, and zip code.
eCommerce/Web Best Practices

Suggested best practices for Rice Merchant Web sites include:

• Encourage cardholders to retain a copy of the transaction.
• Indicate when credit cards are charged.
• Provide order-fulfillment information.
  – State timeframes for order processing and send an e-mail confirmation and order summary within one business day of the original order.
  – Provide up-to-date stock information if an item is back-ordered.
• Explicitly state customer service timeframes.
  – Ideally customer service e-mails or phone calls should be answered within two business days.
• State directly on the main Web site which security controls are used to protect customers.
  – For instance, Rice Merchants should clearly state that Rice is PCI compliant.
Card Not Present Suspicious Behavior/Transactions

Be on the lookout for any of the following signs of suspicious customer behavior/transactions

- **Hesitation**: Beware of customers who hesitate or seem uncertain when giving you personal information, such as a zip code or the spelling of a street or family name. This is often a sign that the person is using a false identity.

- **Rush orders**: Urgent requests for quick or overnight delivery—the customer who “needs it yesterday”—should be another red flag for possible fraud. While often perfectly valid, rush orders are one of the common characteristics of “hit and run” fraud schemes aimed at obtaining merchandise for quick resale.

- **Random orders**: Watch out also for customers who don’t seem to care if a particular item is out of stock —”You don’t have it in red? What colors do you have?”—or who order haphazardly—”I’ll take one of everything!” Again, orders of this kind may be intended for resale rather than personal use.

- **Suspicious shipping address**: Scrutinize and flag any order with a ship to address that is different from the billing address on the cardholder’s account.

- **Requests to ship merchandise to post office boxes or an office address** are often associated with fraud.

- **If you experience fraud on sales** that are shipped, consider creating a list of those zip codes to identify possible areas where high fraud rates are common. Verify any order that has a ship-to address in these areas.

- **If your business does not typically service foreign customers**, use caution when shipping to addresses outside the United States, particularly if you are dealing with a new customer or a very large order.

- **When examining what appears to be an unusual order**, keep in mind that if the sale sounds too good to be true, it probably is.
Address Verification Service

• Address Verification is the verification of the billing address of the consumer’s credit card.
• AVS is required for all key entered transactions.
• No attempt at AVS can result in higher fees assessed for the processing of the transaction.
Potential Cost of a Security Breach

- Fines of $500,000 per incident for being PCI non-compliant
- Increased audit requirements
- Potential for campus wide shut down of credit card activity by merchant bank
- Cost of printing and postage for customer notification mailing
- Cost of staff time (payroll) during security recovery
- Cost of lost business during register or store closures and processing time
- Decreased sales due to marred public image and loss of customer confidence
Breach Investigation

- Merchant should notify processor at first sign of possible breach.
- Processor will notify Visa/MasterCard to begin required forensic investigation/audit.
- A merchant must demonstrate that prior to the compromise, the compromised entity had already met the compliance validation requirements, demonstrating full compliance.
- If merchant can show proof of full PCI compliance, merchant may be granted “safe harbor” and all potential fines waived.
PCI-DSS Program

- Visa established defined standards for protecting sensitive information
- The Payment Card Industry (PCI) Data Security Standard (DSS), with which all Members, Merchants, and Service Providers must comply
- PCI DSS reflects “Walls of Security”
- Minimizes risk of intrusion by erecting multiple layers of security measures
- Benefits of PCI DSS Compliance:
  - Customer Service “Safe”
  - Cost Containment
  - Public Image
- If breached, subject to fines up to $500,000 per incident by non compliant Merchant
# Merchant Requirement for Securing Cardholder Information

## Summary of Card Company Requirements Governing Cardholder Information Security

<table>
<thead>
<tr>
<th>Storage of Cardholder Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Do not store the following under any circumstance:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destruction of Cardholder Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Destroy or purge all media containing obsolete transaction data with cardholder information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Use of Agents or Third Parties (Vendors, Processors, Software Providers, Payment Gateways, or Other Service Providers)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Advise each merchant bank or processing contact (representing each of your card brands) of any agents that engage in, or propose to engage in, the processing or storage of transaction data on your behalf—regardless of the manner or duration of such activities.</td>
</tr>
<tr>
<td>• Make sure these agents adhere to all rules and regulations governing cardholder information security. Any violation by your agent may result in unnecessary financial exposure and inconvenience to your business.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reporting a Security Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>• In the event that transaction data is accessed or retrieved by any unauthorized entity, notify the merchant bank or processing contact for each card brand immediately.</td>
</tr>
<tr>
<td>• This report will not only minimize risk to the payment system, but protect your customers in the most responsible manner. Systems and procedures are in place to immediately stop the unauthorized use of compromised data, but are effective only when you do your part to promptly report a security incident.</td>
</tr>
</tbody>
</table>

We continue to work on your behalf to reduce payment card fraud, and offer this communication to enhance your awareness, minimize risk, and protect your customers. If you have any questions or would like to have more information, please visit our web sites or contact your representatives for any of the card brands sponsoring this correspondence.
# Merchant Levels Defined

- Based on Visa transaction volume over a 12-month period

- Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) from a merchant Doing Business As ("DBA")

- Merchant levels are defined as:

<table>
<thead>
<tr>
<th>Merchant Level*</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any merchant-regardless of acceptance channel-processing over 6,000,000 Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.</td>
</tr>
<tr>
<td>2</td>
<td>Any merchant-regardless of acceptance channel-processing 1,000,000 to 6,000,000 Visa transactions per year.</td>
</tr>
<tr>
<td>3</td>
<td>Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.</td>
</tr>
<tr>
<td>4</td>
<td>Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants-regardless of acceptance channel-processing up to 1,000,000 Visa transactions per year.</td>
</tr>
</tbody>
</table>

* New merchant level definitions effective of July 18, 2006.
** Any merchant that has suffered a hack that resulted in an account
# PCI Compliance Validation Basics

<table>
<thead>
<tr>
<th>Level</th>
<th>Validation Action</th>
<th>Validated By</th>
<th>Due Date</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 1     | •Annual On-site PCI Data Security Assessment  
    •and  
    •Quarterly Network Scan | •Qualified Security Assessor or Internal Audit if signed by Officer of the company  
    •Approved Scanning Vendor | 9/30/04  
    New level 1 merchants have up to one year from identification to validate. |
| 2     | •Annual PCI Self-Assessment Questionnaire  
    •and  
    •Quarterly Network Scan | •Merchant  
    •Approved Scanning Vendor | 9/30/2007  
    New level 2 merchants: |
| 3     | •Annual PCI Self-Assessment Questionnaire  
    •and  
    •Quarterly Network Scan | •Merchant  
    •Approved Scanning Vendor | 6/30/05 |
| 4*    | •Annual PCI Self-Assessment Questionnaire  
    •and  
    •Quarterly Network Scan | •Merchant  
    •Approved Scanning Vendor | Validation requirements and dates are determined by the merchant's acquirer |

*The PCI DDS requires that all merchants perform external network scanning to achieve compliance. Acquirers may require submission of scan reports and/or questionnaires by level 4 merchants.

**Visit->My Global: [www.globalpaymentsinc.com](http://www.globalpaymentsinc.com) -> Industry Initiatives -> Safeguarding Cardholder Information - > Visa CISP link**
The PCI DSS Self-Assessment Questionnaire

What is the PCI DSS Self-Assessment Questionnaire?

• A validation tool intended to assist merchants and service providers in self-evaluating their compliance with the Payment Card Industry Data Security Standard (PCI DSS).

• There are four versions of the SAQ to choose from to meet your business need.

• The multiple versions of the SAQ are to assist with meeting the various scenarios, depending on how your organization stores, process, or transmits cardholder data.
Selecting the SAQ that Best Apply to Your Organization

• There are five SAQ Validation categories (not to be confused with the four versions)

Validation Type One: Complete SAQ - A

• Card is not present (e-commerce or mail/telephone-order)
• Do Not store, process, or transmit cardholder data on your premises
• You rely entirely on a third party to handle these functions
• You have confirmed the third party is PCI DSS compliant
• You only have paper receipts or reports And they are not received electronically
• AND you Do Not store any cardholder data in an Electronic format

Note: If your cardholder transactions are face-to-face, Do Not use SAQ A
Selecting the SAQ that Best Apply to Your Organization

Validation Type Two: Complete SAQ - B

• You Only use an imprint machine to take the payment card information (Knuckle Buster)

• You do not transmit cardholder data over a phone line or the Internet

• Keep only paper copies of the receipts

• And Do Not store cardholder data in an electronic format
Selecting the SAQ that Best Apply to Your Organization

Validation Type Three: Complete SAQ – B

- Process cardholder data only via Imprint Machine or stand-alone dial out terminal
- Stand-alone, dial out terminal is connected via a phone line to processor only
- Dial-out terminal is not connected to any other systems within your environment
- Dial-out terminal is Not connected to the Internet
- You retain only paper reports or paper copies of receipts
- **AND** you Do Not store cardholder data in an electronic format
Selecting the SAQ that Best Apply to Your Organization

Validation Type Four: Complete SAQ – C

• Payment Application is connected to Internet to transmit cardholder data
• Do Not store cardholder data on any computer systems
• The payment application system and Internet access device (PC) is not connected to any other systems within your environment
• You only keep paper reports or paper copies of receipts
• Do Not store cardholder data electronically
• AND the payment application software Vendor uses secure techniques to provide remote support to your payment application system

NOTE: Can be card present, ecommerce or mail/telephone order environment
Selecting the SAQ that Best Apply to Your Organization

Validation Type Five: Complete SAQ – D

• All Merchants that do not fall under Validation Types One – Four
• Some of the questions May Not Apply to your organization such as wireless technology, custom applications, custom codes, data centers etc. If there are questions that do not apply, indicate N/A
SAQ References

- https://www.pcisecuritystandards.org/saq/index.shtml
Approved Scanning Vendor Definition

- Merchants must have websites and IT infrastructures with internet-facing IP addresses scanned by an ASV (Approved Scanning Vendor).
- Merchants must contract with the ASV to perform periodic scans of all active, outward facing IP addresses (or domains) and devices.
- The ASV must scan:
  - Firewalls
  - External routers
  - Web servers
  - Application servers
  - Domain name servers
  - Mail servers
  - Virtual Hosts
  - Wireless LANS
Global Payments Preferred Partners

Security Metrics

- On-line PCI SAQ with automated reporting of results to Global Payments
- No cost pre-enrollment consultation for merchants
- Automated e-mail reminders on compliance status
- If a Merchant requires scanning to validate their PCI DSS compliance the “Quarterly Site Certification” service includes scans for up to 10 IP’s or domains per merchant location enrolled
- Help Desk support for the SAQ, Network Scans and general consultation on remediation
- Cost is $180 per SAQ.

Trustwave/Trustkeeper

- User friendly interface for electronic SAQ completion
- Quarterly network scans of up to 10 IP addresses per merchant location enrolled
- Help Desk support for the SAQ, network scans, support with using the system and general consultation on remediation
- Provides Global Payments with view access to your compliance documents
- Merchant must contract directly with Trustwave.
- Contact: Jeremy Coram: 312-873-7267
Approved Scanning Vendors

- A list of Approved Scanning Vendors can be viewed at:
  
  [https://www.pcisecuritystandards.org/pdfs/asv_report.html](https://www.pcisecuritystandards.org/pdfs/asv_report.html)
Resource Links

- https://www.pcisecuritystandards.org/
- https://www.pcisecuritystandards.org/saq/index.shtml
- https://www.pcisecuritystandards.org/pin/
Contact

- Susan Sutton
  Global Payments
  Phone: 512-260-1018
  Email: susan.sutton@globalpay.com
Q & A