FAU Payment Card Industry (PCI) Training

Welcome to the FAU PCI training website!

You will find all the information you need on this site to become PCI certified for FAU.
PCI Certification is required for all employees that handle credit card payment transactions at FAU

There are several criteria that FAU must pass each year to stay certified with the credit card industry and Bank of America.

- Server Scanning - all server hardware directly related to credit card processing must be scanned by a certified scanning company for possible unauthorized access.
- Technical Compliance - all PCs that have direct access to these servers must be up-to-date on all security patches.
- Self Assessment Questionnaire - FAU must complete a self assessment questionnaire on all requirements for PCI Compliance.
- Employee Training - all employees directly related to the collection of credit cards must have access to training material on PCI compliance.

Chapter 1 - Introduction

Welcome to the Payment Card Industry Security Standards (PCI) training guide. We hope that you will enjoy the flexibility that this online course has to offer and make use of the supplementary tools that we have provided under the Materials link on the course Home page.

Course Contents

Throughout the next few chapters, you will learn about your role in retail fraud prevention and the steps you should take if you feel that your store's security has been compromised. It is critical that you read and retain the information provided in each chapter so that you can serve your customers and the University as safely and efficiently as possible. Each chapter covers a unique and important part of credit card safety:

- Chapter 1 – FAU Policy, outlines the general rules and guidelines instituted by FAU for credit cards and its implementation.
- Chapter 2 – Payment Card Industry (PCI) Data Security Standard, discusses credit card acceptance, security, and CISP certification policies.
- Chapter 3 – Card-Present Fraud Prevention, explores credit card security features and other prevention tactics for Card-Present (in-store) transactions.
- Chapter 4 – Card-Not-Present Fraud Prevention, explores credit card security features for Card-Not-Present (mail order, phone & online) transactions.
- Chapter 5 - What to do if Security is Compromised, explains the steps to reporting a questionable card or customer, while ensuring your personal safety and the safety of your customers and co-workers.

Notice: Throughout this course, the term “FAU Employee” is expanded to include anyone working in a capacity for the University including:

- Administration
- Staff
- Faculty
- OPS
- Students
- Volunteers

Chapter 1 - Introduction

Course Benefits

Above all else, this course 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 your 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 card is in good hands

Your Employer

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

... And You

- Show confidence in your ability to safely and efficiently do your job
- Know that you can make informed decisions under pressure
- Can recognize key security features on valid cards
- Are alert to the warning signs of fraud

Chapter 1 - Introduction

Throughout this chapter you will learn about the credit card acceptance and security guidelines instituted by FAU.

Accepted Forms of Electronic Payment

FAU Merchants may accept the following electronic payment cards:

- Visa (1)
- MasterCard
- Discover
- American Express

FAU Merchants also may accept these other forms of electronic payment:

- Debit Cards
- Web Checks

This course will focus on the security features and policies implemented by the Payment Card Industry (PCI) Data Security Standard. However, you can access information on the unique security features of Visa, MasterCard, Discover, and American Express cards by clicking the Other Information link on the menu. There, you will find links to the security documents published by each of the card companies.

(1) Visa can not be used for paying tuition and fees.

Chapter 1 - Introduction

In this section, we will present and discuss each section of PCI Procedures. It is critical that you read this information carefully and ask your supervisor for assistance if you require further information or clarification regarding your responsibilities.

Accountability / Applicability

These procedures apply to all individuals who have access to credit card information in any form at any merchant location of Florida Atlantic University.

As stated, if you have access to credit card information as part of your job responsibilities at FAU, you are accountable for the security of that information.

Employee Commitment

It is the responsibility of all university employees and third parties having access to cardholder data to protect the information as a sacred trust at all times. Cardholder information should be disclosed only for a required business purpose.

All FAU Merchants, employees, and third parties with access to credit card information are responsible for safeguarding the information and associated cardholder data that is entrusted in their care. Credit card and cardholder data can only be shared with others when it is done as a part of normal business procedures, such as processing payments or giving transaction receipts to a supervisor at the end of a shift.

When a university employee suspects the loss or theft of any materials containing cardholder data, it is vitally important to immediately notify the supervisor and the director of the merchant location.

Upon confirmation of loss or theft, the supervisor or director of the merchant location must contact IRM and the Controller’s Office. IRM will assess the loss or theft and contact the FAU Police Department as necessary.

Designated staff in these departments will implement the procedures for security breaches that are available on the PCI Website. If you ever feel that there may have been a breach in the security of credit card information, regardless of whether or not you are directly involved, alert your supervisor immediately. They will be able to assess whether or not a loss or theft of information is likely, and will respond to the situation by contacting the proper authorities.

Examples of lost or stolen materials containing cardholder data include, but are not limited to:

- A credit card
- Daily credit card terminal tapes
- Computer files containing cardholder data

We will define the exact steps to take if you feel that security has been compromised later in this course.

Chapter 1 - Introduction

Definitions

Cardholder Information Security Program (CISP)

Security requirements for FAU Merchants that are accepted by the Payment Card Industry as the standard for protecting credit card information.

Payment Card Industry (PCI)

The association of credit card providers. The university accepts the following credit cards: VISA, MasterCard, American Express and Discover as well as Debit Cards and Electronic Checks.

Merchant Location

Any university business unit that accepts credit cards as a form of legal tender, including retail and Web-based operations.

Encrypted or Truncated

Data converted to a code or shortened for security purposes.

Validation Code

The unique three- and four-digit codes printed on the back of credit cards requested as proof that a credit card is in the possession of the individual making or completing a transaction with a merchant. (Also referred to as a Security Code or CVV2 code.)

Degaussing

The process of completely removing information from electronic media so that it can no longer be retrieved.

Cross Shredding

The process of using a shredder to cut paper both vertically and horizontally to more completely destroy documents.

Third Party

Companies or individuals that have a relationship with the University to supply goods and/or services. For purposes of this policy, the third party must have access to cardholder information either directly or indirectly.

Audit Logs

A registry that shows the identifier, date, and time that the stored data is accessed.

Self-Assessment

The PCI required annual review of procedures and processes to ensure compliance with current security standards.

External Scans

A process performed by a PCI-certified assessment partner to scan the IP address of the Web portals that accept credit card information for vulnerability in firewalls, virus protection, software, and security.

Chapter 1 - Introduction

Procedures

FAU requires a number of standards to protect credit card information held and/or used at the University. Responsibilities and requirements for the following persons and units are listed below.

- Employees with access to credit card information:
    1. Must complete the FAU on-line credit card information security training (PCI)
- Merchant locations:
    1. Must provide each employee with a unique password that expires after sixty days to access credit card data (other than single transaction processing).
    2. Must protect cardholder information so that only the last four digits of the credit card number are displayed or printed.
    3. Must store only credit card information that is critical to business-name, account number, and expiration date.
    4. Must store only cardholder data that is encrypted or truncated.
    5. Must never store the three- or four-digit validation code in any form.
    6. Must 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. Must provide secure access of the cardholder data at all times if wireless connections are used.
    8. Must store and secure cardholder data in locked containers, marked as confidential, in secured areas with limited access. Examples include electronic data, customer receipts, merchant duplicate receipts, reports, etc.
    9. Must perform an annual review of critical data storage to ensure that all security requirements are met.
    10. May dispose of cardholder data after one year. If disposed of, cardholder data must be disposed of by overwriting or degaussing magnetic media; paper must be cross- shredded.
    11. Must provide all third party vendors the University's credit card procedures.
    12. Must provide all third party vendors with a unique user ID that includes a password that expires every sixty days.
    13. Must give all 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.
- University Controller's Office and IRM:
    1. Must annually review, update, and post official written procedures regarding credit card information security.
    2. Must perform an annual self-assessment.
    3. Must schedule and perform regular parameter scans by the compliance partner and follow-up to correct identified weaknesses.

KEY POINTS

- FAU Payment Card Industry Security Standards (PCI) explains your role and responsibilities at FAU as someone who handles credit card and cardholder information. You should read and be familiar with all of its requirements.
- Prior to being given access to credit card information, all FAU Employees are required to complete a PCI training class offered by the University
- In order to maintain your FAU position as someone who handles credit card information, you must renew your PCI training annually.
- FAU Merchants accept the following types of electronic payments:
  - Visa (Visa is not accepted as payment for tuition and fees)
  - MasterCard
  - Discover
  - American Express
  - Debit Cards
  - Electronic Checks

Chapter 2 - Payment Card Industry (PCI) Data Security Standard

Almost daily, theft of identities and personal information is reported in the news. When our customers offer their bankcard at the point of sale, over the Internet, on the phone, or through the mail, they need assurance that their account information is safe. In response to this need, the Payment Card Industry Security Standards (PCI) were developed and adopted here at FAU. Since June 2001, PCI has served to ensure that members, merchants, and service providers maintain the highest information security standards.

About the Program

WHAT

PCI is a critical component to minimizing risk and maximizing protection. Mandated since June 2001, this robust program is intended to protect cardholder data-wherever it resides.

WHO

FAU Merchants must be PCI-compliant and are responsible for ensuring their compliance. The program applies to all payment channels, including: retail outlets, mail/telephone order, and online payments.

HOW

To achieve PCI compliance, FAU Merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standards, which offers a single approach to safeguarding sensitive data for all card brands. PCI compliance validation identifies and corrects vulnerabilities by ensuring appropriate levels of cardholder data security are maintained.

WHY

By complying with PCI requirements, FAU Merchants and service providers not only meet their obligations to the Payment Card Industry, but also build a culture of security that benefits all parties.

Chapter 2 - Payment Card Industry (PCI) Data Security Standard

Objectives

Completing the reading and activities in this chapter will enable you to:

- Understand the 12 Payment Card Industry Security Standards
- Understand the rules and requirements of PCI
- Know your responsibilities as a FAU Merchant or FAU Employee handling credit card information
- Identify the penalties for PCI non-compliance

Payment Card Industry (PCI) Data Security Standard

The Payment Card Industry (PCI) Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for credit card data protection. The PCI Security Standards Council's mission is to enhance credit card data security by fostering broad adoption of the PCI Security Standards. The 12 PCI Security Standards are as follows:

Build and Maintain a Secure Network

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

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

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

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Chapter 2 - Payment Card Industry (PCI) Data Security Standard

Who Must Comply

PCI applies to all FAU Merchants - meaning any FAU location accepting electronic payments as legal tender. All FAU Merchants and Employees having access to cardholder information, regardless of size, must comply with the PCI Data Security Standard.

Beyond basic data security, full implementation of the PCI Data Security Standards benefits merchants in several ways.

- Customer service - Customers seek out merchants they feel are "safe." Confident consumers are loyal customers. They come back again and again, and share their experiences with others.
- Cost containment - By protecting your customers, you also minimize your own exposure to risk and the direct and operational costs associated with compromised cardholder information.
- Public image - Information security is a frequent topic of media attention. An incident of data loss or compromise not only hurts your customers; it can seriously damage your public image.

FAU Rules

All FAU Merchants and Employees must follow basic card acceptance rules for all electronic transactions. Careful and consistent adherence to the FAU rules outlined in this section will help you to enhance customer satisfaction and increase your store's profitability. If you have any questions about any of the FAU rules presented here, ask your supervisor for assistance.

Dollar Minimums and Maximums

Always honor valid credit cards, regardless of the dollar amount of the purchase. Imposing minimum or maximum purchase amounts is a violation of our merchant services agreement.

No Surcharging

Always treat electronic transactions like any other transaction; that is, you may not impose any surcharge on a credit card transaction. You may, however, offer a discount for cash transactions, provided that the offer is clearly disclosed to customers and the cash price is presented as a discount from the standard price charged for all other forms of payment.

Taxes

Include any required taxes in the total transaction amount. Do not collect taxes separately in cash.

FAU Rules (Continued)

Laundering

Deposit transactions only for your own business. Depositing transactions for a business that does not have a valid merchant agreement is called laundering or factoring. Laundering is not allowed; it is a form of fraud associated with high chargeback rates and the potential for forcing merchants out of business.

Deposit Time Limits

Deposit your transaction receipts daily, or as soon as possible. For card-not-present transactions, the transaction date is the ship date, not the order date. Transactions deposited more than 30 days after the original transaction date may be charged back to you.

Delivery of Goods and Services

Deliver the merchandise or services to the cardholder at the time of the transaction. Cardholders expect immediate delivery of goods and services unless other delivery arrangements have been made. For card-not-present transactions, cardholders should be informed of delivery method and tentative delivery date. Transactions cannot be deposited until goods or services have been delivered.

Delayed Delivery

For a delayed delivery, obtain two authorizations: one for the deposit amount and one for the balance amount. Some merchandise, such as a customized item, requires delivery after the transaction date. In these delayed-delivery situations, the customer pays a deposit at the time of the transaction and agrees to pay the balance upon delivery of the merchandise or services.

To complete a delayed-delivery transaction, you should:

- Create two transaction receipts-one for the deposit and one for the balance. Write "Deposit" or "Balance", as appropriate, on the receipt.
- Obtain an authorization for each transaction receipt on their respective transaction dates. Ensure an authorization code is on each receipt; if your POS device does not automatically print authorization codes on sales receipts, write the codes on the receipts so they are clearly identifiable as such.
- Write "Delayed Delivery" along with the authorization code on each transaction receipt. You may deposit the receipt for the deposit portion of the transaction before delivery of the goods or services. However, you must not deposit the transaction receipt for the balance amount prior to delivery.

Data Storage

Merchants should also be aware of the following data security requirements:

- Magnetic-Stripe Data. Do not store magnetic-stripe data after receiving authorization. After a transaction is authorized, the full contents of track data, which is read from the magnetic stripe, must not be retained on any systems. The account number, expiration date, and name are the only elements of track data that may be retained if held in a PCI-compliant manner.
- Avoid Security Code Storage. The Security Code, also known as the Card Verification Value 2 (CVV2), is the 3- or 4-digit value that is printed on the back of credit cards. All FAU Merchants and Employees are prohibited from storing security code data. When asking a cardholder for their security code, merchants must not document this information on any kind of paper order form or store it on any database.

Cardholder Information

Keep cardholder account numbers and personal information confidential. Cardholders expect you to safeguard any personal or financial information they may give you in the course of a transaction. Keeping that trust is essential to fraud reduction and good customer service. Cardholder account numbers and other personal information should be released only to your merchant bank or processor, or as specifically required by law.

Penalties for Non-Compliance

The Payment Card Industry has established fines of up to $500,000 per incident for security breaches when merchants are not PCI compliant.

In addition, it is required that all individuals whose information is believed to have been compromised must be notified in writing to be on alert for fraudulent charges. As such, the potential cost of a security breach can far exceed $500,000 when the cost of customer notification and recovery is calculated.

Potential Cost of a Security Breach

- Fines of $500,000 per incident for being PCI non-compliant
- 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

Chapter 2 - Payment Card Industry (PCI) Data Security Standard

KEY POINTS

- PCI applies to all FAU Merchants, Employees and Service Providers.
- It is important for all FAU Merchants, Employees, and Service Providers with access to cardholder information to know, understand, and adhere to all 12 Payment Card Industry (PCI) Data Security Standards.
- All FAU Employees who process credit card information as part of their normal job function must have a working knowledge of FAU Policy and PCI requirements, and how to apply each within the scope of their responsibilities.
- Penalties for non-compliance may include: -Potential fines of $500,000 per incident -Additional cost of data recovery procedures -Marred public image -Loss of customer confidence.

Chapter 3 - Card-Present Fraud Prevention

Many FAU Merchants offer both in-store and online shopping options. For this reason, it is important that you learn about the steps you can take to prevent fraud during both Card-Present (in-store) and Card-Not-Present (online and telephone) transactions.

In this chapter, we will guide you through the key steps you can take in preventing retail fraud when processing Card-Present transactions. It is critical that you take the time to read, retain, and put these techniques into action, so that you can provide your in-store customers with the best possible service and security.

Objectives

Completing the reading and activities in this chapter will enable you to:

- Practice the process of safe and effective Card-Present processing.
- Identify the key security features on credit cards.
- Locate additional security verification information.
- Understand the importance and application of Code 10 Calls.

Card-Present Transactions

Card-Present transactions are those in which both the card and cardholder are present at the point of sale. Merchants associated with this sales environment include traditional retail outlets such as those at the Pharmacy and Recreation Center.

FAU 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 should be followed at the point of sale. Each step is explained in greater detail in this section.

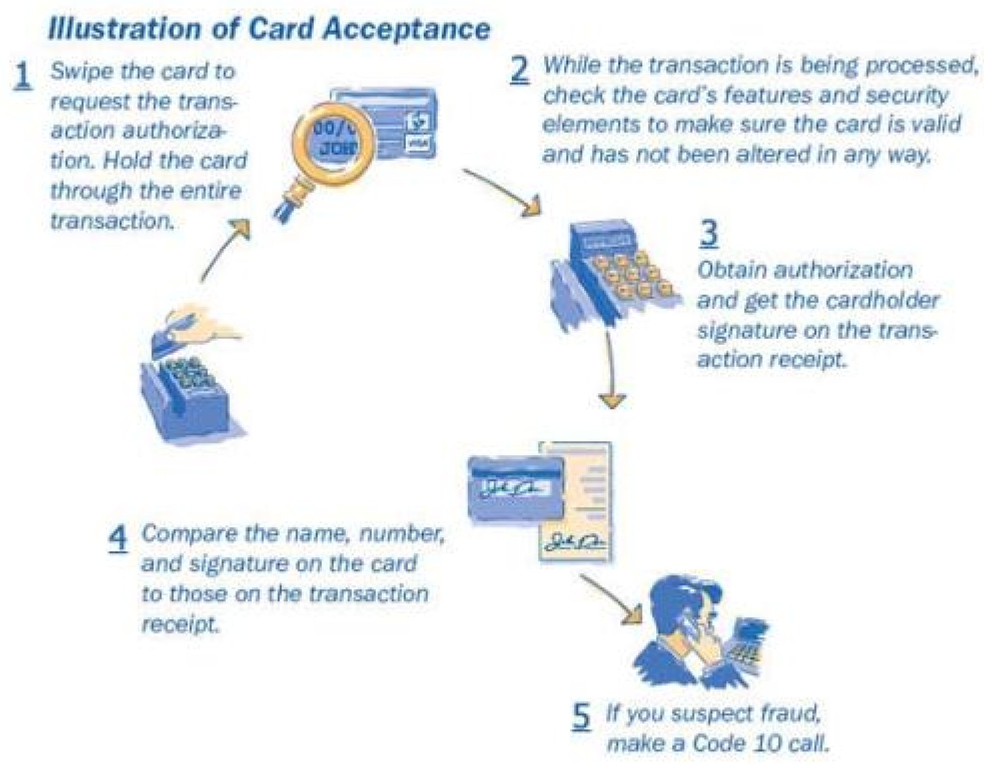


Illustration of Card Acceptance

1 Swipe the card to request the transaction authorization. Hold the card through the entire transaction.

2 While the transaction is being processed, check the card's features and security elements to make sure the card is valid and has not been altered in any way.

3 Obtain authorization and get the cardholder signature on the transaction receipt.

4 Compare the name, number, and signature on the card to those on the transaction receipt.

5 If you suspect fraud, make a Code 10 call.

Chapter 3 - Card-Present Fraud Prevention

It Pays to Swipe the Stripe

On the back of every credit and debit card, you'll find a magnetic stripe. It 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.

- Swipe the card to request the transaction authorization.
- Hold the card through the entire transaction.

Verifying the Account Number

Most Point of Sale terminals also allow merchants to verify that the account number embossed on the front of the card is the same as the account number encoded on the card's magnetic stripe. How you check the numbers depends on your POS terminal. In some cases, the magnetic stripe number is displayed on the terminal or printed on the sales receipt. In others, the terminal may be programmed to check the numbers electronically. In such instances, you may be prompted to enter the last four digits of the embossed account number, which will then be matched against the last four digits of the account number on the magnetic stripe.

Only the last four digits of the account or credit card number should be printed on a transaction receipt. If the numbers don't match, you will receive a "No Match" message. In such instances, you should notify your Supervisor discreetly, and they will decide whether or not it is necessary to make a Code 10 call.

If a Card Won't Read When Swiped

In some instances, when you swipe a card, the terminal will not be able to read the magnetic stripe or perform an authorization. When this occurs, it usually means one of three things:

- 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.

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

If a card won't read when swiped, you should:

- Check the terminal to make sure that it is working properly and that you are swiping the card correctly.
- If the terminal is okay, take a look at the card's security features to make sure the card is not counterfeit or has not been altered in any way (see Card Features and Security Elements).
- If the problem appears to be with the magnetic stripe, follow store procedures. You may be allowed to use the terminal's manual override feature to key-enter transaction data for authorization, or you may need to make a call to your voice-authorization center.
- For key-entered or voice-authorized transactions, make an imprint of the front of the card. The imprint proves the card was present at the point of sale and protects your business from potential chargebacks if the transaction turns out to be fraudulent. The imprint can be made either on the sales receipt generated by the terminal or on a separate manual sales receipt form signed by the customer.

Key-entered transactions are fully acceptable, but they are associated with higher fraud and chargebacks rates. In addition, when transactions are key-entered, the benefits associated with special security features-such as the expiration date and Card Verification Value 2 (CVV2)-are not available.

Minimize Key-Entered Transactions

These best practices can help you keep key-entered transactions at acceptably low levels and should be incorporated into your daily operations and staff training and review sessions.

Find Causes and Look for Solutions

If your key-entry rates are greater than one percent per terminal or sales associate, you should investigate the situation and try to find out why. The following chart summarizes the most common reasons for high key-entry rates and provides possible solutions.

Key-Entry Cause	Solution
Damaged Magnetic-Stripe Readers	Check magnetic-stripe readers regularly to make sure they are working.
Dirty Magnetic-Stripe Readers	Clean magnetic-stripe reader heads several times a year to ensure continued good use.
Magnetic-Stripe Reader Obstructions	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.
Spilled Food or Drink	Remove any food or beverages near the magnetic stripe reader. Falling crumbs or an unexpected spill could soil or damage the machines.
Anti-Theft Devices that Damage Magnetic Stripes	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.
Improper Card Swiping	• 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.

Credit Card Features and 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.

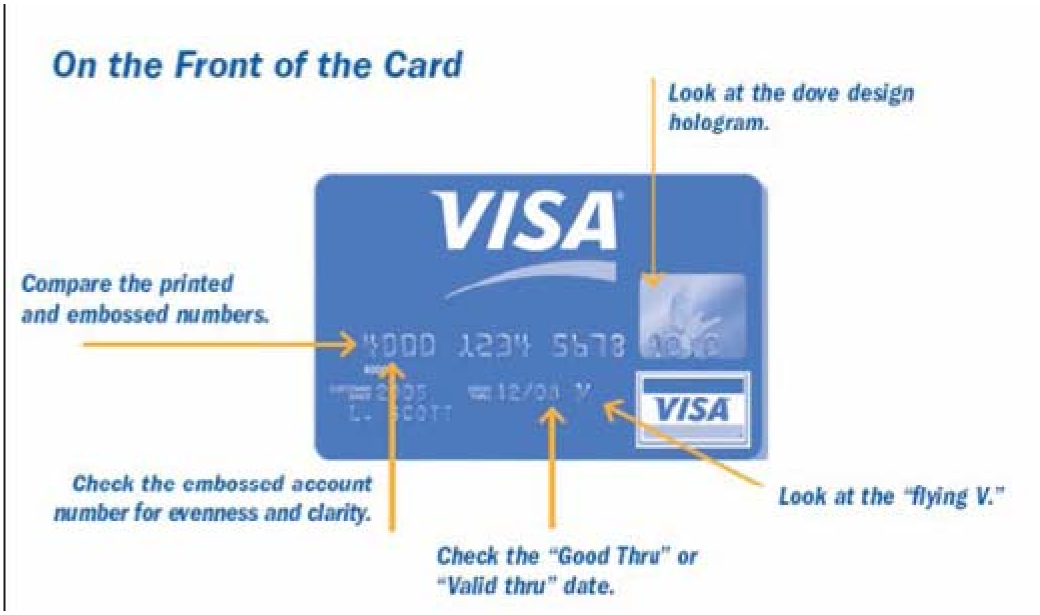
After you have swiped the card, while you are waiting for authorization, take a few seconds to look at the card's basic features and security elements. Checking card features and security elements helps to ensure that the card is valid and has not been altered in any way.

Chapter 3 - Card-Present Fraud Prevention

Holding Onto the Card

You should always keep payment cards in your possession during transaction processing. Holding onto the card gives you time to check card features and security elements and to compare the cardholder signature on the card with the signature on the transaction receipt.

What to Look for on All Cards (Using Visa as an Example)


On the Front of the Card
Look at the dove design hologram.
VISA
Compare the printed and embossed numbers.
4000 1234 5678 9010
VISA
Check the embossed account number for evenness and clarity.
Look at the "flying V."
Check the "Good Thru" or "Valid thru" date.

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.

Note: Check the first digit in the account number.
The first digit should always match the designated first digit for the card brand:

- American Express - 3
- Visa - 4
- MasterCard - 5
- Discover - 6

Check the embossed account number for evenness and clarity.

Look closely at the embossed account number for any signs that the card has been flattened and re-embossed. On valid cards, the numbers will be crisp and even; on altered cards, they may have fuzzy edges, or you may be able to see "ghost images" of the original numbers. The last grouping of numbers is embossed into the hologram. Pay special attention to that area, where ghost images are easiest to spot.

Check the "Good Thru" or "Valid Thru" date.

Make sure the date of the transaction is no later than the date on the card. If the transaction date is after the "Good Thru" date, the card has expired. In such instances, an authorization request can be called in to your authorization center, or you can ask the customer for a card that is currently valid.

Always request an authorization on an expired card. If the Issuer approves the transaction, proceed with the sale.

Never accept a transaction that has been declined.

Look for the embossed character.

Each credit card company has their own unique character embossed on the front of their cards. Visa cards display a stylized embossed "V" located to the right of the "Good Thru" date on all valid Visa cards. If this character is missing or is not a "flying V", the card should not be accepted. Master Cards issued before June 1, 2006 have a scripted "MC" in this area, and Discover Cards have a stylized "D" in between the "Member Since" and "Valid Thru" dates.

Note: MasterCards issued after June 1, 2006 will not have the "MC" Security Character. Cards issued before June 1, 2006

will continue to be valid until their expiration date or June 2010, which ever comes first.

Look at the design hologram.

Visa, MasterCard, and Discover all employ a holographic security design on their cards. The key for all holograms is that they should reflect light, appear three-dimensional, and the image in the hologram should appear to move or shift when the card is tilted back and forth. If the image looks flat or doesn't move, the card may be counterfeit.

On Visa cards, a dove should appear in the hologram and it should seem to "fly" when the card is tilted back and forth. MasterCards have interlocking globes showing the continents with the word "MasterCard" in the background. The Discover card hologram shows a celestial sphere made of interlocking rings and an arrow pointer. The word "DISCOVER" appears in very small letters on the shaft of this arrow. The background of the image consists of a repetitive wave pattern with stars scattered throughout.

Note: The hologram on MasterCards and Diners Club cards may appear on the back of the card. See the MC Security and DC Security document in the Materials section of the course Home page for more information.

Look at the signature panel.

The signature panel is similar for all card types. It should be white with the brand name of the card written repeatedly at an angle across the length of the panel. For example, Visa card signature panels display the word "VISA" reprinted in a diagonal pattern in blue, or blue and gold. On MasterCards, the word "MasterCard" is repeated at an angle in red, yellow, and blue, while "Discover Network" appears diagonally on the signature panel of Discover Cards.

In addition, the words "Authorized Signature" and "Not Valid Unless Signed" must appear either above, below, or beside the signature panel of most credit cards.

Check the account number and security code (CVV2).

The account number, followed by a three- or four-digit code, may be printed on the signature panel in inverse italics (leaning left). The 3- or 4-digit code is a security and validation code, also referred to as the CVV2. The CVV2 is used primarily in Card-Not-Present transactions to verify that the customer is in possession of a valid credit or debit card at the time of the sale.

When Something Doesn't Look Right

If any card security features are missing or look altered, notify your supervisor so that they can decide whether or not it will be necessary to place a Code 10 call to your authorization center.

Authorization

The authorization process allows the card issuer to approve or decline a transaction. In most cases, authorizations are processed electronically in a matter of moments. However, to protect against fraud, the card issuer may request additional information about the transaction. If properly done, authorizing a transaction is quick and easy, and protects merchants against fraud and chargebacks.

Authorization Responses

Authorization should be seen as an indication that account funds are available and a card has not been reported as lost or stolen. It is not proof that the true cardholder or a valid credit card is involved in a transaction.
During the authorization process, you should receive one of the responses on the following table, or one that is similarly worded.

Response	Meaning
Approved	Card issuer approves the transaction. This is the most common response-about 95% of all authorization requests are approved.
Declined or Card Not Accepted	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.
Call, Call Center, or Referrals	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.
Pick-Up	This response indicates that the card issuer would like the card to be confiscated from the customer. However, FAU 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.
No Match	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. Notify your supervisor discreetly that it is necessary to make a Code 10 call.

When a transaction is approved, the POS terminal automatically prints a sales receipt. When a negative or alert message is received, the response is displayed on the POS terminal, and no sales receipt is printed. Whatever the message, you should continue to treat the customer courteously so as not to arouse alarm or suspicion.

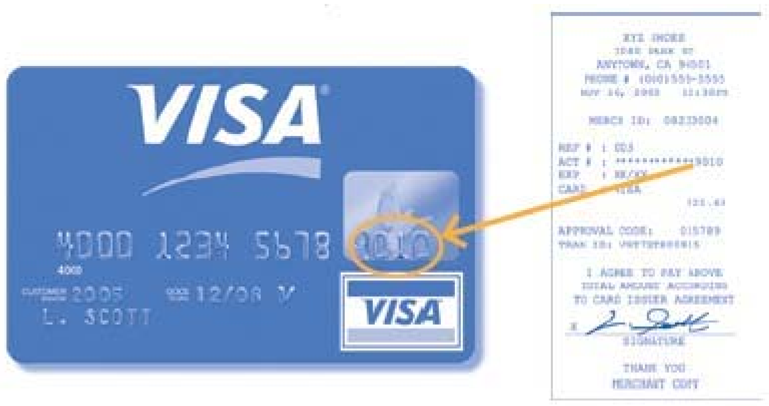
What to Look for on All Cards (Using Visa as an Example)

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.

1. Match the name and last four digits of the account number on the card to those printed on the receipt.
2. 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.



XYZ SHOES
1040 PARK ST
ANYTOWN, CA 94501
PHONE # (000)555-5555
NOV 16, 2003 12:30PM

MERCH ID: 08233004

REF # : 003
ACT # : ************9010
EXP : XX/XX
CARD : VISA
$21.43

APPROVAL CODE: 015789
TRAN ID: [illegible]

I AGREE TO PAY ABOVE
TOTAL AMOUNT ACCORDING
TO CARD ISSUER AGREEMENT
X
SIGNATURE

THANK YOU
MERCHANT COPY

For suspicious or non-matching signatures, 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.

Chapter 3 - Card-Present Fraud Prevention

Unsigned Cards

While checking card security features, you should 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.

Remember: The words "Not Valid Without Signature" appear above, below, or beside the signature panel on most credit cards.

"See ID"

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 signatures: they use cards as quickly as possible after a theft and prior to the accounts being blocked. They are actually counting on you 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.

Remember: 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, you should 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 when 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.

Code 10 Calls

Code 10 calls allow FAU Merchants to alert card issuers to suspicious activity and to take appropriate action when instructed to do so. You or your supervisor should make a Code 10 call to your 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 at 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.

- 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. **FAU Employees are not obligated or expected to confiscate credit cards.**

Making Code 10 Calls 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 you can make Code 10 calls even after a cardholder leaves the store. A Code 10 alert at this time may help stop fraudulent card use at another location, or perhaps during a future transaction at your store.

KEY POINTS

- Card-present transactions are those in which both the card and cardholder are present at the point of sale.
- Proper card acceptance begins and ends with sales staff and is critical to customer satisfaction and profitability.
- On the back of every credit card, you'll find a magnetic stripe. It contains the cardholder name, card account number, and expiration date, as well as special security information designed to help detect counterfeit cards.
- Key-entered transactions increase the possibility of a security breach. Everyone should work together to minimize key-entered transactions.
- You should always keep payment cards in your possession during transaction processing. Holding onto the card gives you time to check card features and security elements and to compare the cardholder signature on the card with the signature on the transaction receipt.
- If any of the credit card security features is missing or looks altered, alert your supervisor, and if necessary, make a Code 10 call to your authorization center.
- While checking card security features, you should also make sure that the card is signed. An unsigned card is considered invalid and should not be accepted.

Chapter 4 - Card-Not-Present Fraud Prevention

Every day, the number of purchases conducted via the mail, telephone, and Internet increases. These transactions are significantly different from traditional in-store sales, in that the customer and credit card are not present at the merchant location during the transaction, making it especially difficult to detect fraud.

Of necessity, card acceptance procedures for these “card-not-present” transactions are different from in-store purchases. FAU Employees who conduct card-not-present transactions must exercise extreme caution and follow procedures precisely in order to verify—to the greatest extent possible— the cardholder’s identity and the validity of the purchase. This chapter covers basic card acceptance procedures for mail, telephone, and Internet transactions. It also includes resources and best practices that all card-not-present merchants can use to prevent fraud and chargebacks.

Objectives

Completing the reading and activities in this chapter will enable you to:

- Understand the requirements for internet sales using the FAU TouchNet system.
- Safely and effectively process card-not-present transactions, including international and internet transactions.
- Ensure proper security code (CVV2) processing and interpret CVV2 result codes.
- Verify billing addresses with the Address Verification Service (AVS).
- Identify and successfully react to suspicious transactions.

Internet Payment Processing

FAU has been collecting secure online payment processing for Web applications through the TouchNet Payment Gateway and Paypath. The current version offers expanded applications and functionality, giving customers of FAU Merchants access to self-service payment processing through this behind-the-scenes Web application.

The TouchNet/Paypath Payment Gateway is the official on-line payment system of FAU. Regularly scheduled server scans are performed, and identified weaknesses (if any) are addressed to provide the most secure environment for our merchants and customers. TouchNet conforms to federal security regulations as well as the Payment Card Industry Standards.

Merchant Web Site Requirements

The Payment Card Industry Standards require that you include certain content or features 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 e-mail address promotes customer satisfaction.

Return, refund, and cancellation policy

This policy must be clearly posted on the merchant Web site.

Delivery policy

FAU 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

You must disclose the permanent address of your establishment on the Web site including the street name, number, city, state, country, and zip code.

Best Practices for the Web

- Encourage cardholders to retain a copy of the transaction (print receipt).
- Indicate when credit cards are charged. Credit cards should not be billed until merchandise has been shipped.
- 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, FAU Merchants should clearly state the fact that FAU is PCI compliant

Manual Processing of Card-Not-Present Transactions (Only Where Specifically Authorized)

Authorization is required on all electronic payment transactions. Authorization should occur before any merchandise is shipped or service performed. The following processes are critical for fraud prevention during card-not-present transactions.

Ask for Card Expiration Date

Whenever possible, card-not-present merchants should ask customers for their card expiration, or "Good Thru," date and include it in their authorization requests.
Including the date helps to verify that the card and transaction are legitimate. A mail order, telephone order, or Internet order containing an invalid or missing expiration date may indicate counterfeit or other unauthorized use.
TouchNet will not allow processing of payments if any information is incorrect.

Ask for the Security Code (CVV2)

The security code or Card Verification Value 2 (CVV2) is a three- or four-digit security number printed on the back of credit cards to help validate that a customer is in possession of a legitimate card at the time of an order. Studies show that merchants who include security code validation in their authorization procedures for card-not-present transactions will reduce their fraud-related chargebacks.

Security Code Processing

To ensure proper security code processing for card-not-present transactions, merchants should:

- Ask card-not-present customers for the three- or four-digit security code located beside or below the signature panel on the back of their credit or debit cards only when this code can be entered directly into an authorization terminal.
- If the customer provides a security code, submit this information with other transaction data (card expiration date and account number) for electronic authorization.

Indicator	**What It Means**
0	Security Code/CVV2 is not included in authorization request
1	Security Code/CVV2 is included in authorization request
2	Cardholder has stated that security code/CVV2 is illegible
3	Cardholder has stated that security code/CVV2 is not on card

- Evaluate the Security Code/CVV2 result code you receive with the transaction authorization, and take appropriate action based on all transaction characteristics.

CVV2 Result Code	**Recommended Action**
M- Match	Complete the transaction taking into account all other characteristics and verification data.
N - No Match	View a "No Match" response as a sign of potential fraud, which should be taken into account along with the authorization response and any other verification data. You may also want to resubmit the CVV2 to ensure a key entry error did not occur.
P - CVV2 Request Not Processed	Resubmit the authorization request.
S - CVV2 Code should be on card, but the cardholder reports that is isn't	Follow-up with the customer to verify that the correct card location has been check for the CVV2 code.

Chapter 4 - Card-Not-Present Fraud Prevention

Address Verification Service (AVS)

FAU Merchants may be set up to use the Address Verification Service (AVS), which is an automated fraud prevention tool that allows card-not-present merchants to check a cardholder's billing address as part of the electronic authorization process. Studies have shown that perpetrators of fraud in card-not-present transactions often do not know the correct billing address for the account they are using. Verifying the address can, therefore, provide merchants with another key indicator of whether or not a transaction is valid.

AVS Processing

To use the Address Verification Service (AVS), simply ask card-not-present customers for their billing address as it appears on their monthly statement. This information is then submitted with other transaction data for electronic authorization. Address verification and authorization occur simultaneously—in a matter of seconds—and you will receive an AVS response code with the authorization.

You should evaluate the AVS response code and take appropriate action, based on all transaction characteristics and any other verification information received with the authorization (expiration date, security code/CVV2, etc.). An authorization response always takes precedence over AVS. Do not accept any transaction that has been declined, regardless of the AVS response.

AVS Response	**What It Means**
X - Exact Match	Address and nine-digit zip code match.
Y - Match	Both street address and five-digit zip code match. Complete the transaction; you can be relatively confident it is legitimate.
A – Partial Match	Street address matches, but zip code doesn't. View as a sign of potential fraud. Depending on the transaction amount, you may decide to complete the transaction or investigate further to ensure it is valid.
Z – Partial Match	Zip code matches but the street address doesn't. View as a sign of potential fraud. Depending on the transaction amount, you may decide to complete the transaction or investigate further to ensure it is valid. Unless you sent only a zip code AVS request and it matched, you may want to follow up before shipping merchandise. Note: A zip code only request and P.O. Box address. Issuers may respond with either a "Y" (Exact Match), or a "Z" (Partial match-zip Code Matches).
N – No Match	Street address and zip code don't match. View as a sign of potential fraud and take further steps to validate the transaction.
U – Unavailable	The card issuer's system is not available, or the card issuer does not support AVS. The address cannot be verified at present. You must decide whether to accept or refuse the transaction, or investigate further.
R – Retry	The card issuer's system is not available; try again later. The card issuer's system may not be working. You should resubmit your AVS request later.

Merchant Direct Access Service

The Merchant Direct Access Service offers FAU Merchants access to the Address Verification System (AVS) by a toll-free number, using a touch-tone phone. The service is specifically targeted to small mail order, telephone order, or Internet merchants for whom AVS may not be cost-effective. Merchants using MDAS are charged on a per-transaction basis.

To use the Merchant Direct Access Service, you need a touch-tone phone with an outgoing line and a Merchant Access Code, which you get from your merchant bank. To request an address verification, call the MDAS toll-free number, 1-800-VISA-AVS (1-800-847-2287). An automated voice unit guides you through the process of submitting a customer's account number and address, and gives you the results of the verification.

Merchant Direct Access Service (MDAS) responses are similar to AVS, but do not include a single-letter response code.

MDAS Response	What It Means
Exact Match	Street address and zip code match.
Partial Match	Street address matches, but not zip code.
Partial Match	Zip code matches but not street address.
No Match	Neither street address nor zip code matches.
Retry Later	Card issuer's system is not available at present.
Global	International address; cannot be verified.

Suspicious Transactions

Card-not-present merchants should develop in-house policies and procedures for handling irregular or suspicious transactions and provide appropriate training for their sales staff. Being able to recognize suspicious orders may be particularly important for merchants involved in telephone sales, and employees should be given clear instructions on the steps to take to verify these transactions.

You should be on the lookout for any of the following signs of suspicious customer behavior:

- 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.
    1. Requests to ship merchandise to post office boxes or an office address are often associated with fraud.
    2. Keep lists of zip codes where high fraud rates are common and verify any order that has a ship-to address in these areas.
    3. 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.
    4. 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.

KEY POINTS

- Authorization is required on all card-not-present transactions.
- FAU Internet Merchants primarily use the FAU TouchNet Payment Gateway.
- The Security Code, also referred to as a Card Verification Value 2 (CVV2), is a three- or four-digit security number printed on the back of credit cards to help validate that a customer is in possession of a legitimate card at the time of an order. (This code may not be written down. It must be entered directly into an authorization terminal.)
- The Address Verification Service (AVS) is an automated fraud prevention tool that allows card-not-present merchants to check a cardholder's billing address as part of the electronic authorization process.
- The Address Verification Service can only be used to confirm addresses in the United States. If you submit an address outside the U.S., you will receive the response message "G" for "Global."
- Being able to recognize suspicious orders may be particularly important for merchants involved in telephone sales, and employees should be given clear instructions on the steps to take to verify these transactions.

Chapter 5 - What to do if Security is Compromised

If you ever feel unsure about the legitimacy of a card or the intentions of a customer, trust your instincts. No one is harmed by a false alarm – but if you ignore the warning signs of fraud, it could cost you, your store, and your customers a lot of time and money.

In this section, we will review the steps that you should take if you feel that your store's security has been compromised. You should read these steps carefully, and make sure that you are prepared to implement them in the case of a security emergency.

Security Breach

If you experience a suspected or confirmed security breach, you should:

1. Immediately contain and limit the exposure. TURN OFF the compromised machine.
2. To prevent any further loss of data, conduct a thorough investigation as soon as possible. Investigations must be conducted within 24 hours of the compromise.
3. If you suspect a compromise of data:
    - Have your Supervisor contact IRM and Cash Management (Controller's Office) to report the credit card security breach.
    - Give IRM your contact information including name, phone number and e-mail address.
    - IRM will determine the extent of the breach and notify the Police Department and the University Controller's Office to take the appropriate actions.
4. Do not access or alter compromised systems. Do not log on to the machine or change passwords.
5. Preserve logs and electronic evidence. Log all actions taken.
6. Be on HIGH alert and monitor all credit card systems.

In the event of a security breach, IRM will contact the University Controller's Office to discuss the compromise and review the actions required to demonstrate the ability to prevent future loss or theft of transaction information.

Merchant banks may be subject to fines of up to $500,000 per incident if a security breach is caused by a merchant or service provider who is not PCI compliant. Merchant banks will not be fined if the compromised merchant or service provider is PCI compliant at the time of the security breach.

Chapter 5 - What to do if Security is Compromised

FAU Merchant Preparedness

Each FAU Merchant location should maintain written procedures on the processing of credit card, debit card, and electronic payments. Those procedures should give specific instructions on how and when to conduct Code 10 Calls, and how to respond to a security breach. Written procedures should be made available to all employees.

The Best Advice of All

Trust your instincts! If a sale seems too good to be true, it probably is. We hear all too often that what a merchant thought to be a great sale, turned out to be fraud. So take the time to check out that huge order from a customer with whom you've never done business. That little bit of extra work may well prevent you from being the victim of a fraud scheme.

Case Study

ABC is a store located on-campus which sells logo items to the general public. This is a retail outlet and in addition to sales in the store, they also accept telephone orders and sell on the internet. It is the beginning of the semester and business has been very busy. Even though two cashiers called in sick this morning customers have continued to stream in all day and only three people are working.

Ken, is the store manager, he has been with the University over ten years as an employee and has a good knowledge of ABC operations and processing sales transactions. (1) - Mike is a Staff employee who has just started working today. He seems bright and eager to learn. Jennifer is an OPS student who also knows procedures and has worked for about a year now.

The store is rather small, with only two registers and a credit card terminal located next to each. The check-out counters are located in front of the door and must be passed to enter or exit. Located to the left of the cashier is the customer's service area and credit card terminal with a key pad for customers to swipe their credit cards and, if using a debit card, key in their pin number. A table is located behind the Cashier on which is placed a phone, pens, scraps of paper and a bulletin board with pins. (2) Sometimes when it gets busy and a customer calls to order merchandise the staff must write down the order, along with the credit card number, the card expiration date and the security code from the back of the card.

Because today is so busy, Ken has staggered lunch breaks between Mike and himself. Jennifer will be available from 11:00 to 2:00 – their busiest hours so neither will have to be alone in the store during this time.

Continued on next page...

Case Study continued...

At 11:30 Mike takes a break leaving Ken helping customers and Jennifer on the register. By noon Ken has to take a register along with Jennifer because customers are getting restless in line at the check-out. Ken helps several customers check out, the first pays cash, and the second uses a credit card. The phone has rung several times so Ken answers it and puts the call on hold until after completing the transaction with the customer at his register. (3) Ken doesn't have time to key in the phone order and credit card number of the caller so he writes the information on a slip of paper which is pinned to the bulletin board for safe keeping then Ken returns to checking customers out on his register. In the mean time Jennifer has a customer whose card will not swipe. The store does not have a Point of Sale system so (4) Jennifer moves the credit card terminal next to her and keys the credit card information which is accepted.

Mike returns from lunch at 12:30 but because the store is very busy with calls, customers, and questions this keeps all three staff members occupied.

It is now 2:00 PM, Jennifer is leaving and Ken has not yet taken lunch so he leaves for a quick break. Mike has been shown how to run the register and the credit card terminal and says he will be fine. Several customers come and go within the thirty minutes Ken is on break - some paying with cash, others paying with credit cards and one paying by check. Mike thinks he understands the process until a customer's credit card is declined. He doesn't know what to do and the customer is getting angry – Ken is no where to be seen so (5) Mike takes the credit card anyway and decides he will figure out what to do when Ken arrives.

When Ken returns, he notices that the (6) credit card terminal next to the register Jennifer was operating is missing. In addition, Mike tells Ken of the declined credit card and that he accepted the transaction anyway.

How could credit card security at ABC be improved?

- Mike has just started today and likely has not had a background check, adequate training and signed ethics form.
- Credit Card information (especially the CVV2) should not be written down; rather it should be keyed as received or stored on a secured server if necessary for delayed shipment.
- Posting credit card information on a bulletin board is very dangerous threat to security. It leaves the customer's personal and credit card information visible and available to everyone in the store. Additionally, there is no mention of what is done with the slips of paper after they are entered in the terminal. Note: Credit cards are not to be charged until the item is shipped.
- Credit card terminals must be kept in an area where customers do not have access to them – preferably behind a counter or in a limited access area.
- NEVER accept a credit card that has been declined.
- Now that the terminal is missing – what do staff members do? A written policy for security breaches and lost information is important. The Cash Management Department of the Controller's Office should be notified immediately.

KEY POINTS

- Merchant banks may be subject to fines of up to $500,000 per incident if a security breach is caused by a merchant or service provider who is not PCI compliant.
- Merchant banks will not be fined if the compromised merchant or service provider is PCI compliant at the time of the security breach.
- If you experience a suspected or confirmed security breach during a transaction, you should alert IRM and the Controller's Office.
- IRM and the Controller's Office will determine the extent of the breach and contact the necessary authorities including the FAU Police department.
- **Trust your instincts! If a sale seems too good to be true, it probably is.**

Course Complete

If you have any questions or concerns regarding any element of this course, contact Dianna Zaia at 561-297-1425.

Glossary

Account number

The 16-digit account number that appears in print on the front of all valid credit cards. The number is one of the card security features that should be checked by merchants to ensure that a Card-Present transaction is valid.

Address Verification Service (AVS)

AVS allows FAU Merchants that accept card-not-present transactions to compare the billing address (the address to which the card issuer sends its monthly statement for that account) given by a customer with the billing address on the card issuer's master file before shipping an order. AVS helps merchants minimize the risk of accepting fraudulent transactions in a card-not-present environment by indicating the result of the address comparison.

Authorization

The process by which a card issuer approves or declines a credit card purchase. Authorization occurs automatically when you swipe the magnetic stripe of a payment card through a card reader. See also: Voice Authorization Center.

"Call" or "Call Center" response

A response to a merchant's authorization request indicating that the card issuer needs more information about the card or cardholder before a transaction can be approved; also called a referral response.

Card acceptance procedures

The procedures FAU Merchants and Employees must follow at the point of sale to ensure a card and cardholder are valid.

Glossary

Card expiration date

See Good Thru date.

Cardholder

The person to whom a credit card is issued.

Card-Not-Present

A merchant, market, or sales environment in which transactions are completed without a valid credit card or cardholder being present. Card-not-present is used to refer to mail order, telephone order, and Internet merchants and sales environments.

Card-Present

A merchant, market or sales environment in which transactions can be completed only if both a valid credit card and cardholder are present. Card-Present transactions include traditional retail—department and grocery stores, electronics stores, boutiques, etc.—cash disbursements, and self-service situations, such as gas stations and grocery stores, where cardholders use unattended payment devices.

Card security features

The alphanumeric, pictorial, and other design elements that appear on the front and back of all valid credit card and debit cards. Card-Present merchants must check these features when processing a transaction at the point of sale to ensure that a card is valid.

Glossary

Card Verification Value 2 (CVV2)

A fraud prevention system used in card-not-present transactions to ensure that the card is valid. The CVV2 is the three-digit value that is printed on the back of credit cards. Card-not-present merchants ask the customer for the CVV2 and submit it as part of their authorization request. For information security purposes, merchants are prohibited from storing CVV2 data.

Cardholder Information Security Program (CISP)

A program that establishes data security standards, procedures, and tools for all entities—merchants, service providers, issuers, and merchant banks—that store cardholder account information. CISP compliance is mandatory.

Chargeback

A transaction that is returned as a financial liability to a merchant bank by a card issuer, usually because of a disputed transaction. The merchant bank may then return or “charge back” the transaction to the merchant.

Code 10 call

A call made to the merchant’s voice authorization center when the appearance of a card or the actions of a cardholder suggest the possibility of fraud. The term “Code 10” is used so calls can be made without arousing suspicion while the cardholder is present. Specially trained operators then provide assistance to point-of-sale staff on how to handle the transaction.

Glossary

Copy request

A request by a card issuer to a merchant bank for a copy or facsimile of a sales receipt for a disputed transaction. Depending on where sales receipts are stored, the merchant bank either fulfills the copy request itself or forwards it to the merchant for fulfillment. A copy request is also known as a retrieval request.

Credit receipt

A receipt that documents a refund or price adjustment a merchant has made or is making to a cardholder's account; also called credit voucher.

Disclosure

Merchants are required to inform cardholders about their policies for merchandise returns, service cancellations, and refunds. How this information is conveyed, or disclosed, varies for Card-Present and Card-Not-Present merchants, but in general, disclosure must occur before a cardholder signs a receipt to complete the transaction.

Firewall

A security tool that blocks access from the Internet to files on a merchant's or third-party processor's server and is used to ensure the safety of sensitive cardholder data stored on a server.

Glossary

Good Thru date

The date after which a bankcard is no longer valid, embossed on the front of all valid credit cards. The Good Thru date is one of the card security features that should be checked by merchants to ensure that a Card-Present transaction is valid. See also: Card expiration date.

High-risk merchant

A merchant that is at a high risk for chargebacks due to the nature of its business. High-risk merchants include direct marketers, travel services, outbound telemarketers, inbound teleservices, and betting establishments.

Internet Protocol address

A unique number that is used to represent individual computers in a network. All computers on the Internet have a unique IP address that is used to route messages to the correct destination.

Key-entered transaction

A transaction that is manually keyed into a point-of-sale device.

Magnetic-stripe reader

The component of a point-of-sale device that electronically reads the information on a payment card’s magnetic stripe.

Glossary

Mail order / telephone order (MO / TO)

A merchant, market, or sales environment in which mail or telephone sales are the primary or a major source of income. Such transactions are frequently charged to customers' bankcard accounts. See also: Card-not-present.

Merchant agreement

The contract between a merchant and a merchant bank under which the merchant participates in a credit card company's payment system, accepts credit cards for payment of goods and services, and agrees to abide by certain rules governing the acceptance and processing of credit card transactions. Merchant agreements may stipulate merchant liability with regard to chargebacks and may specify time frames within which merchants are to deposit transactions and respond to requests for information.

Merchant bank

A financial institution that enters into agreements with merchants to accept credit cards as payment for goods and services; also called acquirers or acquiring banks.

Merchant Chargeback Monitoring Program (MCMP)

A program that alerts merchant banks when one of their merchants has a chargeback-to-transaction rate of over one percent. Merchants then work with the bank to reduce their chargeback rates to acceptable levels. Failure to reduce chargebacks can result in fines for a merchant.

Glossary

Payment gateway

A system that provides services to Internet merchants for the authorization and clearing of online credit card transactions.

Pick-up response

This response indicates that the card issuer would like the card to be confiscated from the customer. However, FAU 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.

Point-of-sale terminal (POS terminal)

The electronic device used for authorizing and processing bankcard transactions at the point of sale.

Printed number

A four-digit number that is printed below the first four digits of the printed or embossed account number on valid credit cards. The four-digit printed number should be the same as the first four digits of the account number above it. The printed four-digit number is one of the card security features that merchants should check to ensure that a Card-Present transaction is valid.

Representment

A chargeback that is rejected and returned to a card issuer by a merchant bank on the merchant’s behalf. A chargeback may be re-presented, or redeposited, if the merchant or merchant bank can remedy the problem that led to the chargeback. To be valid, a representment must be in accordance with Payment Card Industry Operating Regulations.

Glossary

Sales receipt

The paper or electronic record of a bankcard transaction that a merchant submits to a merchant bank for processing and payment. In most cases, paper drafts are now generated by a merchant's POS terminal. When a merchant fills out a draft manually, it must include an imprint of the front of the card.

Skimming

The replication of account information encoded on the magnetic stripe of a valid card and its subsequent use for fraudulent transactions in which a valid authorization occurs. The account information is captured from a valid card and then re-encoded on a counterfeit card. The term "skimming" is also used to refer to any situation in which electronically transmitted or stored account data is replicated and then re-encoded on counterfeit cards or used in some other way for fraudulent transactions.

Split tender

The use of two forms of payment, or legal tender, for a single purchase. For example, when buying a big-ticket item, a cardholder might pay half by cash or check and then put the other half on his or her credit card. Individual merchants may set their own policies about whether or not to accept split-tender transactions.

Third-party processor

A non-member organization that performs transaction authorization and processing, account record keeping, and other day-to-day business and administrative functions for issuers and merchant banks.

Glossary

Transaction

The act between a cardholder and merchant that results in the sale of goods or services.

Unsigned card

A seemingly valid credit card that has not been duly signed by the legitimate cardholder. Merchants cannot accept an unsigned card until the cardholder has signed it, and the signature has been checked against a valid, government-issued Photo ID, such as a driver's license or passport.

Voice authorization

An authorization obtained by telephoning a voice authorization center.

Voice authorization center

An operator-staffed center that handles telephone authorization requests from merchants who do not have electronic POS terminals or whose electronic terminals are temporarily not working, or for transactions where special assistance is required. Voice authorization centers also handle manual authorization requests and Code 10 calls.

PCI Security Standards Council™