PCI DSS Annual Training

Best Practices for Payment Card Acceptance

Please read though this guide to gain an understanding of the Payment Card Data Security Standard. After completion, you will be responsible for completing the PCI DSS Annual Confidentiality Agreement.

Key Terms

Payment Cards
Credit Cards, Debit Cards, or Purchasing Cards issued by a financial instituition.

Merchant Account
An account set up through a bank, which provides the alibity to process Payment Cards as payment for goods or services rendered by the account holder (The University of Utah).

Card Present Transactions
Transactions in which the cardholder presents the acutal card to the merchant for processing.

Card Not-present Transactions
Transactions in which the cardholder gives their credit card information to the merchant over the phone or sends through mail on a designated form. A form may include a signature. Generally, a signature is not obtained in this type of transaction.

E-Commerce
The ability to process payment cards as payment for goods or services through a merchant account, using the Internet. The cardholder initiates the transactions from their own computers. The merchant does not handle the cardholder data at any time during the transaction.

Redaction
The process of removing sensitive data from printed or written documents by making it illegible. Redaction may also include removing the sensitive information completely from the document. Redaction is a manual process.

Truncation
The process of removing the majority of the sensitive data. For cardholder data, Truncation means leaving only the last four digits of the card number on the receipt. Truncation is done by the payment processing device or program.

The Payment Card Industry Data Security Standard

University of Utah departments that accept Payment Cards become custodians of their students/customers information. This is nothing new. Practically everything that is stored electronically on campus is someone's sensitive information.

As custodians of sensitive data, if that data is compromised, the owner of the information will face the consequences, whether they be financially or by reputation. The University will ultimately face the same consequences.

It is imperative to use both standard security procedures and technologies to thwart theft of sensitive data. As an example we will look at Cardholder Data.

The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of comprehensive requirements for enhancing payment card data security. Compliance with the PCI DSS helps to mitigate vulnerabilities that put cardholder data at risk.

PCI Data Fields

Cardholder Data:

- Primary Accont Number (PAN)
- Cardholder Name when associated with the PAN
- The Security Code when associated with the PAN
- Expiration Date when associated with the PAN

Sensitive Authentication Data:

- Full Magnetic Stripe Data (can never be stored)
- CAV2/CVC2/CVV2/CID (can never be stored)
- PIN or PIN Block (can never be stored)

Six Main Goals of PCI DSS

1. Build and maintain a secure network
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

Each goal has detailed requirements, listed below are ways to adhere to them:

Strong Passwords

- DO NOT use vendor-supplied default passwords or share your passwords with others.
- Follow the University's password guidelines by using a password phrase, or upper & lowercase letters, combined with numbers and special characters.
- Change your password every 90 days.
- DO NOT store your passwords in a notebook, on post-it notes, or any other accessible means.

Protect Cardholder Data

- Never store cardholder authentication data after authorization. This includes the full card number, the expiration date, and the 3 digit security code.
- Written card numbers should only be kept until authorization, and for no more than one business day for authorization to be completed. During that business day, keep the information in a secure area in your desk or office.
- Any document or scratch paper with cardholder authentication data, such as payment card numbers, expiration dates, and security codes must be cross-cut shredded immediately after authorization.
- Make sure all receipts and reports (both yours and the cardholders) have truncated card numbers. Only the last 4 digits.
- **Redacting** Payment Card data on written documents is acceptable if done in the following manner:
    - Card number, expiration date, and security code are cut off of the form and immediately cross-cut shredded
    - **Or**, using a sharpie or white out, get rid of the sensitive card data, **copy the document**, shred the original document and keep the copy.
- Receipt storage/retention time may be whatever time is required by business, legal, and/or regulatory purposes – as long as the cardholder data is appropriately truncated or redacted.
- Keep payment card machines out of site and reach of customers. When applicable, keep your computer screen out of the line of sight of customers so they cannot see card numbers as you enter them.

Restrict Access to Cardholder Data by Business - "Need to Know"

- "Need to Know" means that access rights are granted to only the least amount of data and privilages needed to perform a job.
- Limit access to payment card processing equipment and cardholder data to only those individuals whose jobs require such access.
- Your duties as department staff accepting payment cards, requires you to follow your department's payment card procedures regarding the proper storing, protection, and disposal of cardholder data.

Maintain An Information Security Policy

- A strong security policy sets the tone for the whole company and informs employees (and all relevant system users) what is expected of them.
- All system users should be made aware of the sensitivity of data and their responsibilities of protecting it.
- An incident response plan should be implemented and practiced.
- The University has a standard payment card acceptance procedure – please contact your department merchant contact to review the procedure.

Card Present Transactions

- If the imprinted name on the card does not match the signature on the back of the card or signed receipt, do not accept the card. Void the transaction.
- If you receive a declined response, you may run the card one more time as a customer service gesture. **Stop** after 2 attempts. Continually running the transaction will not change the declined response.
- If the customer insists on contacting their card issuer, they may do so on their own to have their funds made available. **Do Not do it for them**. An authorization must be received through your department's processing method.
- Swiping the card is the most secure method of accepting payment cards.
- Hold onto the card while the card is authorized and the receipt is signed.
- Compare signatures on the receipt and on the back of the card. Make sure the embossed name matches the signed name.
- If the signature panel on the card says, "Please see ID" the card is not valid. Ask for the ID and ask the cardholder to sign the card in front of you. Check the signatures and pictures.
- All receipts must be kept, for dispute purposes, for one year. Receipts older than one year can be shredded.
- **Do Not call the phone number on the back of the card for authorization**. An authorization is only valid if it is obtained through the merchant services help desk or your payment processing device.
- If you suspect fraud, call the merchant services help desk for a voice authorization and tell them you have a "**Code 10**". They will ask specific questions and give you direction on how to proceed.
- Only retain the card when instructed to do so, if you feel **safe** to do so.
- Euro Mastercard and Visa Cards (aka EMV or Chip and Pin cards) are now being used more for card present transactions.
- The benefit to these cards is that the chip that is inside the card is constantly changing how it matches the card number with the PIN number. Both the chip and the PIN must be validated during authorization, making duplication of these cards extremely difficult.
- EMV cards only protect against fraud when the card is present at the time of the transaction. It does not reduce fraud for online or phone order transactions.
- Visa and Mastercard have mandated that when an EMV/Chip and Pin card is presented for payment, it must be processed as a Chip and Pin card. If there is a fraudulent transaction on a Chip and Pin card and you did not process as a Chip and Pin card, you will lose the funds on that transaction if it is disputed. If the fraudulent transaction is disputed and you processed the card as a Chip and Pin card, then you keep the money from that transaction.
- The FD-130 is the terminal that will process these cards. If the majority of your transactions are card present and you want to upgrade your terminal to this model, please contact Income Accounting for more information.

Card Not-Present Transactions

Phone/Mail Order:

- Enter all of the information you are prompted for. By doing so, you will be using security prompts to make sure the person using the card is the cardholder.
- It is best to keep the customer on the phone while you run the transaction. If that is not possible, you should get the customer's phone number in case the card is declined.
- Shred any paper that has card information on it – especially the CVV/CVV2 code and full card number. It is University policy to never physically store full credit card numbers, expiration dates, or security codes. You may redact the cardholder data as previously mentioned if your document must be kept.

Refunds

- Refunds must be issued to the **same** card used in the original transaction.
- Refunds must be issued using the **same mode** of processing that was used for the original transaction.
    - For example, if the original transaction was processed on your terminal, the refund must be issued using the terminal, not through e-commerce, any other software, or a check request.
- The refund amount may only be up to the amount of the original transaction.
- All refunds should be dual controlled, or in other words, approved by a supervisor.
- There are very few exceptions to the refund rules. Here are two examples that may apply to you:
    - Your processing system may not allow you to process refunds without the card present and/or without a previous transaction.
    - The refund request is older than 6 months. Some systems cannot perform refunds after certain time frame.
- If either of these exceptions apply to your department, you may send a check request. Please add this exception as an addendum to your PCI department procedure document.

Avoiding Fraud

- Despite our best efforts, it is still possible for our payment card systems to be breached or compromised. Watch out for the following:
    - Multiple completed transactions or multiple attempts to complete transactions by the **same** cardholder.
    - Cardholders asking for refunds to be posted to a different payment card.
    - Your day-to-day card swiping equipment looks different than usual, and cannot be confirmed as replacement equipment from your verified vendor.
    - Cardholder documents displaying card numbers, such as written phone orders, are not stored securely or disposed of correctly.
- Be sure that your credit card processing devices are out of reach and sight of your customers.
- All devices capable of swiping a payment card must be checked for tampering on a monthly basis. The payment card contact for your department will be responsible for keeping a log of the device inspection.
- A copy of the payment card device inspection form is available on the Payment Card Acceptance website.

- A common way criminals are able to obtain cardholder data is through Skimming.
    - Skimming is a device that logs the card numbers as they are swiped through the payment card device, or key entered. Skimmers are more common on ATMs and gas pumps, but they can be inserted onto any card terminal.
    - Cameras are often used to capture cardholders entering PIN numbers in association with the cards being swiped through the skimming devices.
    - As mentioned above, inspect your devices regularly in order to avoid things such as Skimming.

- The keys to avoiding payment card fraud are:
    - Know your customers. If you have repeating customers, be aware of their behaviors and the cards they use.
    - Know your card processing devices and check then regularly for tampering.
    - Be vigilant! Taking the few extra seconds to match signatures and look at the card you are accepting can save you time and money later on.
    - Train all staff that handle payment cards on "Acceptance Best Practices" and your department procedures. Repeat training often.

- Social Engineering is the manipulation of people in order to get them to perform actions or divulge confidential information .
    - Social engineering is one of the easiest routes to sensitive data, especially when staff have not been trained on how to recognize and combat it. **Everyone** is a potential target, from the receptionist to management.
    - Social engineers are confident, friendly, and usually in a hurry. They look and/or act like they belong and use pressure to rush employees into giving them the information they desire.
- Social Engineering examples:
    - You enter a secure/key access office and someone tries to follow you in, but you don't recognize them – **what do you do?** Dont hold the door for them – ask them to use their key for security purposes.
    - You have been to a website and your computer starts to make a horrible noise. You get a pop-up from Microsoft support with a phone number to call for assistance – **what do you do?** Call your University IT support instead.
    - You receive an email with an attachment from someone you do not recognize – **what do you do?** Delete the email. If it's legitimate, the person will eventually contact you another way.
    - You receive a call from someone who says they are from Merchant Services and your equipment needs updating. You have not been previously notified by the proper channels (Income Accounting to each department contact) – **what do you do?** Kindly ask the person to remove your number from their list and hang up.
    - You find a USB drive in the parking lot or restroom – what do you do? Leave it there, or throw it away. **Do Not put it in your computer for any reason**, as it could be infected with malware or another type of computer virus.

- You have a co-worker who can't remember their password. They ask you if you can login for them – **what do you do?** You help them contact the appropriate person for a password reset.
- You get an email from University IT services about an expired password. You are asked to click on the attached link to reset your password – **what do you do?** Think about how you are normally notified about an expiring password, then contact UIT or your department IT support to verify.

Better safe than sorry!

- When dealing with sensitive information, always question activity that seems to be outside your normal business practices.

Incident Response

- Incident Response Plan
  - If you suspect a data breach, contact the Information Security Office (ISO) and Income Accounting & Student Loan Services **immediately. Do Not** disable or turn off your system, unless directed to do so by ISO.
  - Your department will be restored with the ability to accept payment cards as soon as possible.

Summary

- Properly securing cardholder data is the responsibility of **every** University of Utah employee. It only takes few extra seconds to make a big difference.

- Lack of compliance to the PCI DSS, in a single area of the University, could jeopardize the University's ability to accept payment cards. (Policy 3-070)

- Your support and cooperation is essential to the University's compliance.

- Completing the PCI DSS Annual Confidentiality Agreement is required after the reading and understanding this guide. The Agreement is in the form of a quiz. Click here to access the quiz.