PCI DSS Compliance
Security Awareness Training

Payment Card Industry (PCI)
Data Security Standards (DSS)

What are the Objectives?

At the Conclusion of this training, the learner will be able to:

- Know the meaning of PCI, DSS, and Security Awareness.
- Define common PCI terms.
- Understand the Importance of PCI compliance to Landry's Inc and why training is necessary.
- Know the best practices for processing credit cards.
- Understand how to process and handle exceptions to processing credit cards for different functions/events.
- Identify potential security breaches and know the corrective actions that need to be taken
- Examine credit cards and identify potentially fraudulent cards.
- Identify signs of POS tampering to illegally obtain PCI information and know how to respond to signs of POS tampering.

What is PCI DSS Compliance?

Payment Card Industry Data Security Standard (PCI DSS) compliance is the adherence to policies and procedures set forth by all credit card brands to protect credit and debit card transactions and prevent the misuse of the cardholder's personal information.

What are Common Terms?

Payment Cards

Any brand of credit or debit cards that are presented by a guest as the form of payment for any transaction.

Card Present (CP) Transactions

Occurs when a guest presents the actual card to the merchant for processing. The card is swiped, inserted, or tapped into a device and a signature is obtained.

Card Not-Present (CNP) Transactions

Occurs when the guest submits card information over the phone or on a designated form.

What is the Importance of PCI DSS Compliance to Landry's?

Landry's has an obligation to all guests, vendors, employees, and others to keep all account information safe when processing payment cards.

- Primary Account Information (PAN)
- Expiration Dates

- Card Security Codes (CVV)
- PIN Codes
- Magnetic Stripes

Who is Responsible for PCI DSS Compliance?

All employees of Landry's that have any kind of contact with payment card processing or payment card information are responsible for keeping credit card information safe.

- All employees that process payments or issue refunds.
- All managers with employees that have direct contact with credit card processing data.
- All employees that oversee, manage, or work with credit card processing software or hardware.

Best Practices for Credit Card Processing

Never send or accept any payment card information by email.

If you receive an email with payment card information, notify a supervisor.

Never print or forward the email with payment card information.

Delete the email containing the payment card information immediately.

Let the sender know that we do not accept payment card information by email and we cannot process the payment.

Best Practices for Credit Card Processing

Never Write down or Store Payment Card Data Electronically

- 16 Digit Primary Account Number (PAN)
- Expiration Date
- Track Data
- Security Codes
- PIN Numbers

Handling Credit and Debit Cards

Handle Credit/Debit cards safely and securely outside of public view.

If you see Credit/Debit cards or banking information lying around in plain sight, hand it immediately to your supervisor.

Separation of Duties

Individuals that process payment card transactions and refunds should not be involved in reconciling.

Best Practices for Credit Card Processing

Other Guidelines to Follow

- Never store more than the last 4 digits of the Primary Account Number (PAN)
- Restrict employee access to cardholder information.
- Restrict physical access to areas where card information is handled and stored.
- Store card receipts for the current fiscal year and the 3 prior years in a secure location.
- Each terminal needs their own ID and password that is changed regularly
- Destroy unneeded payment card numbers with a cross-cut shredder.

Exceptions

There may be instances that require paper-based storage of payment card information.

In these examples, payment card information may be handwritten in a ledger or on an approved form and stored securely, for example, in a locked safe or file cabinet.

Once the cardholder cancels the services or the services are rendered and the financial obligation is met, the payment card information must be destroyed in a cross-cut shredder.

Best Practice:
If payment information is taken over the phone, do it quietly and discreetly to prevent eavesdropping.

Potential for Security Breaches

It is very important that we do our part to help prevent payment card data from being stolen. The following are common instances where the potential for a security breach can occur.

- Leaving filing cabinets and safes unlocked.
- Lost or stolen keys.
- Computer breaches, compromises, or infections.
- Skimming devices placed in the POS area.
- Shared or stolen User IDs and Passwords.
- Unusual or unexplained payment card transactions.
- Payment Card information thrown in the trash or the dumpster.

Payment Card Identification Features

When examining payment cards for authenticity, each of the 4 major payment card companies have different security features that will help identify fraudulent cards.

American Express

1. All American Express account numbers are embossed and starts with “37” or “34”.
2. Account numbers are embossed (15 digits), with no alterations and spaced in 4, 6 and 5 digits.
3. The 4 digit Card Identification Number (CID) is printed above the embossed account number on the right or left of the card and cannot be scratched off.
4. Compare the name embossed on the card with your customer. Cards are not transferable.
5. The “member since” date is embossed — compare the age of your customer.
6. The expiry date is embossed and it shows the time period during which the card is valid.

7. The clarity of the Centurion is similar to U.S. currency. The Centurion portrait is phosphores and the words “AMEX” are visible under UV light.
8. Some cards have a hologram of the American Express image embedded into the magnetic stripe.
9. The printed account number must match the embossed number on the front of the card and the sales receipt.
10. Compare the signature with the one on the sales receipt. If the presented card is unsigned, request a photo ID with signature and request your customer to sign the card and sales receipt while you hold the ID.

VISA CARD
SECURITY FEATURES

The **Signature Panel** must appear on the back of the card. The words "Authorized Signature" and "Not Valid Unless Signed" must appear near the signature panel. If tampered with, the word "VOID" will be displayed.

The **Mini-Dove Design Hologram** may appear on the back on either side of the signature panel or on the front of the card above the Visa brand mark.

Card Verification Value 2 (CVV2) is a three-digit code that appears either on or in a white box to the right of the signature panel. Portions of the account number may also be present on the signature panel.

Account Number on valid cards begins with "4." All digits must be even, straight, and the same size.

Visa Brand Mark must appear in blue and gold on a white background in either the bottom right, top left, or top right corner.

Visa Chip cards are embedded with a chip. At this time, chip cards are primarily issued outside the U.S.

Expiration or "Good Thru" date should appear below the account number.

Four-Digit Bank Identification Number (BIN) must be printed directly below the account number and must match exactly with the first four digits of the account number.

MasterCard® Card Security Features and Optional Card Features

Card Front

1. The first 4 digits of the account number must match the 4 digit preprinted BIN. Remember, all MasterCard account numbers start with the number 5.

2. The last 4 digits of the account number must match the 4 digits that appear on the cardholder receipt.

3. The global hologram is three dimensional with a repeat "MasterCard" printed in the background. When rotated, the hologram will reflect light and appear to move.

4. The stylized "MC" security feature has been discontinued, but may continue to appear on cards through June 01, 2010.

Card Back

5. The signature panel is tamper evident with the word "MasterCard" printed in multiple colors at a 45° angle. For magnetic swiped transactions, remember to compare the signature on the back of the card with the cardholder's signature on the receipt.

6. The 4 digits printed on the signature panel must match the last 4 digits of the account number, followed by the 3 digit indent printed CVC2 number.

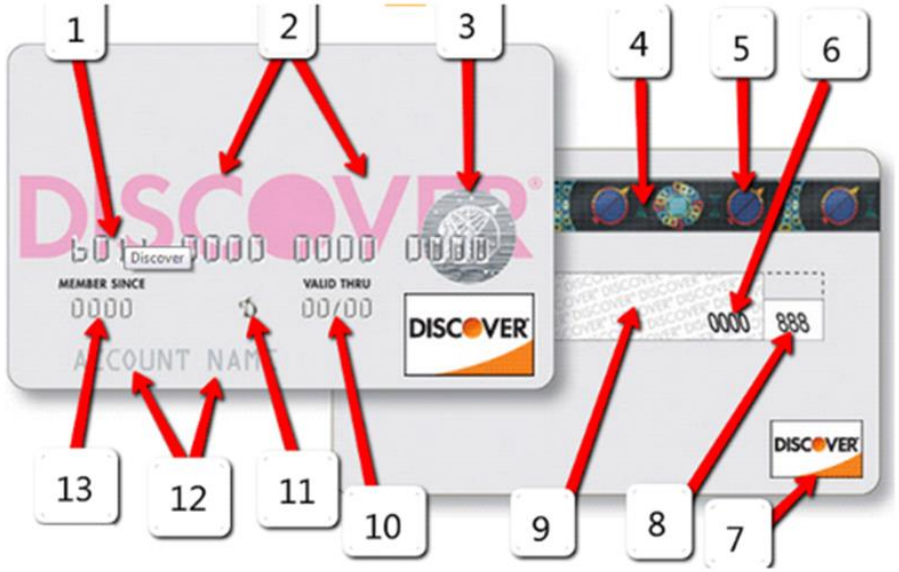
Optional Card Feature (see Card Front).

7. A Chip may be present on the card. The cardholder will be prompted to enter a unique personal identification number or PIN when the card is inserted into a chip capable payment terminal.

8. PayPass® contactless payment technology may be present on card. A signature is not required for PayPass® "tapped" transactions below a specified limit.

cirrus. maestro.

(Affiliates of MasterCard)



1. **Account number.** All Discover account numbers begin with "6" and are 16-digit long. Embossed numbers should be uniform in size and spacing, and extend into the hologram. Unembossed cards may display the account number and expiration date printed flat on the front.
2. **Discover Network.** The words "Discover" or "DISCOVER NETWORK" will appear under an ultraviolet light.
3. **Hologram.** Some Discover cards may display a hologram on the front of the card with a globe pierced by an arrow. However, if the back of the card displays a holographic magnetic stripe, there is no hologram on the front.
4. **Magnetic stripe.** Discover's magnetic stripe should look smooth, with no signs of tampering.
5. **Blue circles.** Some Discover cards display a holographic magnetic stripe with blue circles.
6. **Last four digits.** The last four digits of Discover's card number are also displayed within the signature panel, in reverse indent printing.
7. **Discover brand mark.** Discover's Network Acceptance Mark will appear on the front and / or back of the card.
8. **Card Identification Number (CID).** The three-digit CID is printed in a separate box, immediately to the right of the signature panel on the back of the card.
9. **Discover Network on the back.** The words "DISCOVER NETWORK" appear repeatedly within the signature panel on the back of the card.
10. **Expiration date.** As with the other brands, the "Valid Thru" date, which indicates the last month in which the card is valid, is placed underneath the account number and to the right of the "Member Since" date.
11. **Stylized "D".** An embossed security character appears as a stylized "D". However, no such symbol is present on unembossed cards.
12. **Cardholder name.** In some cards, a "Business Name" may be embossed below the account name.
13. **Member since date.** Located to the left of the expiration date, it indicates the month and year in which the account was open.

Detecting POS Terminal Tampering

Modified POS terminals are used to copy and store magnetic stripe card data and confidential PIN codes. Modified terminals can be difficult to detect, but these are the most common.

Look for additional cables, an antenna, or a card skimmer that was not present before.

Look for new payment card processing terminals that are not the same as other terminals in your store.

Look for thicker cables that conceal additional wires to capture payment card data.

Look for new or different buttons on the payment card terminals; it could be a false number pad overlay.

Look for unusual gaps, discoloration or loose swipe card slots on the payment card terminals.

Look for glue, tape, uneven gaps, holes, or cracks on the payment card terminals.

On the back check for extruding parts, missing/wrong screws, screws not flush, missing paint, and missing labels.

Examine the data connector and determine if it is different/wrong type, if it has an adaptor/extender, or if it has tape.

Handling Suspected POS/Payment Device Tampering

If you suspect POS/Payment Device terminal tampering, it is important that you notify your Supervisor immediately.

Always be on the lookout for any suspicious or unusual behaviors.

Inform your Supervisor

If a POS or Payment Device device appears to have been tampered with, or broken and inoperable, do not attempt to repair it, inform your manager.

No On-Site Repairs

There will never be on-site POS or Payment Device repairs from 3rd parties. Watch out for suspicious behavior around POS or Payment Device repairs.

Summary of PCI DSS Compliance

PCI DSS Compliance

Payment Card Industry Data Security Standard (PCI DSS) compliance is the adherence to policies and procedures set forth by all credit card companies to protect credit and debit card transactions and prevent the misuse of the cardholder's personal information.

Landry's Role in Compliance

Landry's has an obligation to keep payment card information safe.

Compliance Responsibility

All employees that handle anything regarding payment cards are responsible for keeping information safe.

No Email

Never accept payment card information by email.

No Electronic Storage

Never store payment card data electronically.

PCI Security Awareness Training Acknowledgement

Read the statement below acknowledge each box to confirm your PCI understanding.

I have been provided with Landry's PCI Security Awareness Training information, and after reviewing, I understand the following Information and Directives:

- ❑ Cardholder data consists of all the following components:
Primary Account Number (PAN), Card Verification Code (CVC), and Expiration Date
- ❑ I should never share my login information with a co-worker.
- ❑ The primary goal of PCI DSS is to protect cardholder data.
- ❑ PCI Security Awareness training is mandatory.
- ❑ A primary benefit of PCI compliancy is protection against fraud.
- ❑ Under specific situations/conditions mentioned in this module, employees can write down customer credit card information on approved ledgers.

Security Awareness Training

Physical Security

Social Engineering

Reporting

Physical Security Awareness

It is important to protect your property and premises against, theft, crime, and unauthorized personnel attacks.

- Always secure your belongings and valuables.
- If you see anyone Loitering/trespassing or attempting to access an unauthorized area, alert your supervisor immediately.
- If you encounter a situation that poses a threat to anyone's life or safety, immediately dial 911 and follow up with your supervisor afterward as soon as possible.
- Always shred and securely dispose of any sensitive information once it is no-longer needed.

Social Engineering Awareness

Social engineering is any attempt by phone, email, or in person, to deceive, manipulate, or even blackmail or threaten you into doing or sharing something you shouldn't.

Recognizing Signs of Social Engineering:

- Message arrives unexpectedly
- Sender asks something out of the ordinary
- Requested action is potentially harmful to safety or security
- Attacker attaches an unusual file or URL
- Attacker Includes a sense of urgency

Types of Social Engineering Attacks:

- Phishing- The use of shortened links to redirect users to obtain personal information
- Pretexting-The attacker fabricates a scenario to steal personal information
- Vishing- Phishing attacks over the phone to retrieve personal or confidential information
- Quid Pro Quo- Attackers promise a form of service in an attempt to steal information
- Tailgating- Attackers follow employees into restricted areas

Conclusion

Report inappropriate, illegal, and suspicious conduct immediately to your supervisor.