

PCI Security September 2020

1. PCI Compliance Training 5.10.17





1.1 PCI DSS Compliance



1.2 Objectives

Objectives






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

 PCI -Meaning-	Know the meaning of PCI, DSS, and Security Awareness.
 PCI -Terms-	Define common PCI terms.
 PCI -Landry's-	Understand the importance of PCI compliance to Landry's, Inc.
 PCI -Training-	Understand which employees are required to have PCI compliance training and why the training is necessary.


1.3 Objectives

Objectives

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

 Credit Card -Processing-	Know the best practices for processing credit cards.
 PCI -Exceptions-	Understand how to process and handle exceptions to processing credit cards for different functions/events.
 PCI -Breaches-	Identify potential security breaches and know the corrective actions that need to be taken.
 Credit Card -Fraud-	Examine credit cards and identify potentially fraudulent cards.
 POS -Tampering-	Identify signs of POS tampering to illegally obtain PCI information and know how to respond to signs of POS tampering.

1.4 What is PCI DSS Compliance?



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.

1.5 Common Terms

Common Terms



Payment Cards

Payment cards are 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

A card present transaction occurs when a guest presents the actual card to the merchant for processing. The card is swiped into a device and a signature is obtained.



Card Not-Present (CNP) Transactions

A card not-present transaction occurs when the guest submits card information over the phone or on a designated form.

1.6 Importance of PCI DSS Compliance to Landry's

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. Information to be kept safe includes:



1.7 Who is Responsible for PCI DSS Compliance?

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 all credit card information safe. This includes:



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

1.8 Best Practices for Payment Card Processing

Best Practices for Credit Card Processing

DO NOT SEND OR ACCEPT ANY PAYMENT CARD INFORMATION BY EMAIL

 Supervisor If you receive an email with payment card information, notify a supervisor.	 No Trail DO NOT print or forward the email with payment card information.
 Delete Delete the email containing the payment card information immediately.	 Notify Let the sender know that we do not accept payment card information by email and we cannot process the payment.

1.9 Best Practices for Credit Card Processing

Best Practices for Credit Card Processing

NEVER STORE PAYMENT CARD DATA ELECTRONICALLY

 DO NOT STORE: <ul style="list-style-type: none">• 16 Digit Primary Account Number (PAN)• Expiration Date• Track Data• Security Codes• Pin Numbers	 Separation of Duties Individuals that process payment card transactions and refunds should not be involved in reconciling.
--	--

1.10 Best Practices for Credit Card Processing

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 user needs their own ID and password that is changed regularly.
- Destroy unneeded payment card numbers with a cross-cut shredder.

1.11 Exceptions

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 authorization form and stored securely, for example, in a locked safe or filing 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.

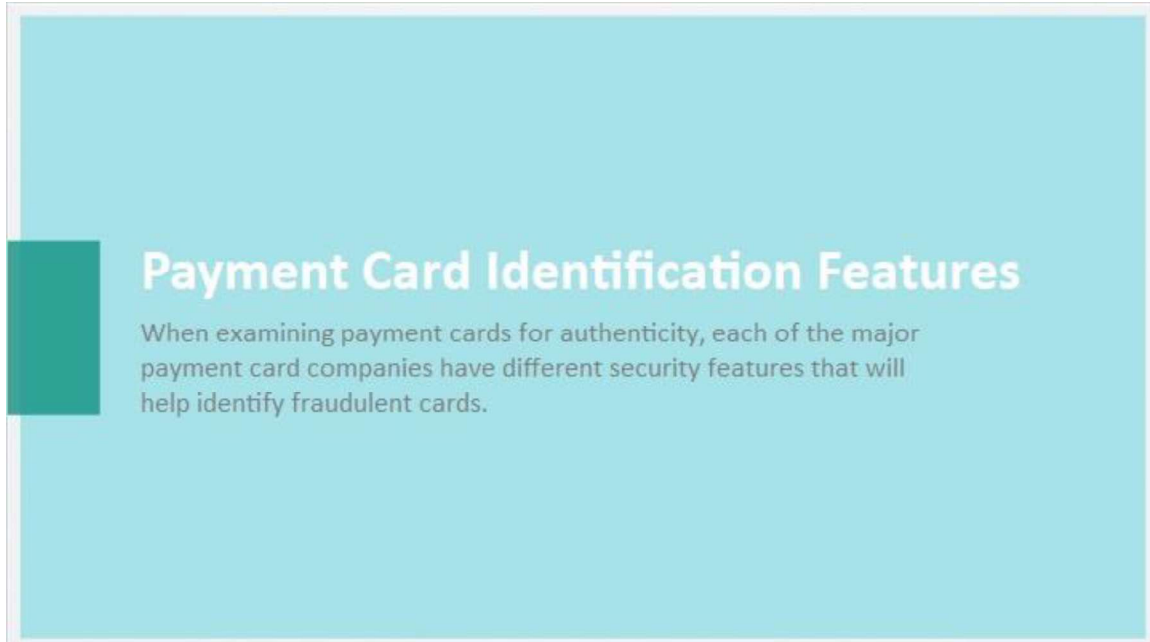
Examples of Exceptions

- Marina Boat Leases or Rentals
- Catering and Weddings
- Bulk Gift Card Purchase
- Social Booking
- Group Sales

1.12 Grid Layout



1.13 Payment Card Identification Features



1.14 American Express Card Identification Features

American Express® Card Identification Features

The letters "AMEX" and a phosphorescence in the Centurion portrait are visible under an ultraviolet light.

Pre-printed (non-embossed) Card Identification Number (CID) should always appear above the account number.

Do not accept a Card after the expiration date.

Only the person whose name is embossed on an American Express Card is entitled to use it.


All American Express account numbers start with 3. Embossing should be clear and uniform in size and spacing. The number on the front and back of the Card, plus the one printed on the sales receipt should all match.

With this statement on the Card, American Express reserves the right to "pick up" the Card at any time.

Some Cards have a hologram of the American Express image embedded into the magnetic stripe.

The signature on the back of the Card should match the customer's signature on the receipt. The signature panel is tamper-evident.

**Merchant Code 10 Authorization
1-800-528-1212
if you are suspicious of a card transaction**



1.15 Visa Card Identification Features

Visa® Card Identification Features

The Dove Hologram appears on most cards, however its location on the card may vary. It can be in its traditional location on the front of the card, or a smaller hologram may be on the card back.

All Visa account numbers start with 4. The embossed account number must match the account number printed on the sales receipt.

The pre-printed Bank Identification Number (BIN) must match the first four digits of the embossed account number.

The Visa Brand Mark appears in the lower right corner. Visa debit cards have the word "DEBIT" printed above the Visa Brand Mark.

A full or partial account number is indent-printed on the tamper-evident signature panel.

A three-digit code (CVW2) must appear in the white box to the right of the signature panel or on the signature panel.

Some cards have a holographic magnetic stripe featuring doves in flight on the back of the card. These cards do not have any other hologram or magnetic stripe.

If you are ever suspicious about a card or a transaction, call your authorization center and request a Code 10 authorization.



1.16 MasterCard Card Identification Features

MasterCard® Card Identification Features

All MasterCard account numbers start with 5. The embossing should be uniform in size and spacing, and extend into the hologram.

The pre-printed Bank Identification Number (BIN) must match the first four digits of the embossed account number.

The valid date lists the last month in which the card is valid.

Issuers have the option of placing a holographic magnetic stripe on the card back, replacing the Globe hologram or the Debit hologram.

The three-dimensional hologram, which may appear on the front OR the back should reflect light and appear to move.

All new and re-issued consumer Debit cards must display the Debit hologram.

The magnetic stripe should appear smooth, with no signs of tampering.

The last four digits of the account number appear on the signature panel in reverse indent printing.

The three-digit CVC2 appears to the right of the signature panel.

The word "MasterCard" is printed repeatedly in multicolors at an angle on a tamper-evident signature panel.

**Are you suspicious about a card?
Call for a Code 10 Authorization.**

1.17 Discover Network Card Identification Features

Discover® Network Card Identification Features

The words "DISCOVER NETWORK" will appear under an ultraviolet light.

All Discover Network account numbers start with 6. The embossing should be uniform in size and spacing, and extend into the hologram.

"Valid Thru" indicates the last month in which the card is valid.

A Business Name may be embossed below the account name.

An embossed Security Character appears as a stylized "D."

The three-dimensional hologram should reflect light and appear to move.

The magnetic stripe should appear smooth, with no signs of tampering.

The words "DISCOVER NETWORK" appear on the signature panel, and an underprint reading "VOID,"

The last four digits of the account number appear on the signature panel in reverse indent printing.

The three-digit Card Identification Data (CID) appears to the right of the signature panel.

The Discover® Network Acceptance Mark appears on both sides of the card.

**Law Enforcement Phone Line
1-800-347-3083
For Law Enforcement Officers ONLY**

**Merchant Code 10 Authorization
1-800-347-1111
for suspicious transactions**

1.18 Detecting POS Terminal Tampering

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.

1.19 Detecting POS Terminal Tampering

Detecting POS Terminal Tampering

01

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



02

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



1.20 Detecting POS Terminal Tampering

Detecting POS Terminal Tampering

03

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



04

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



1.21 Detecting POS Terminal Tampering

Detecting POS Terminal Tampering

05

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



06

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



1.22 Detecting POS Terminal Tampering

Detecting POS Terminal Tampering

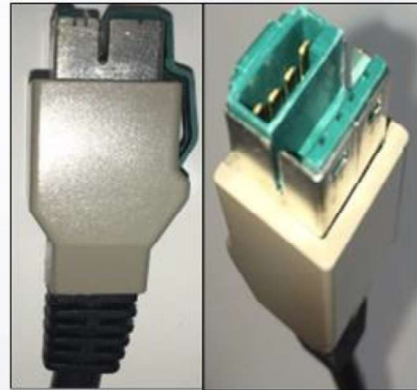
07

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



08

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



1.23 Handling Suspected POS Tampering

Handling Suspected POS Tampering

If you suspect POS terminal tampering, it is important that you notify IT Help immediately. Always be on the lookout for any suspicious or unusual behaviors.

Call
IT Help

1-800-493-1010

If a POS device appears to have been tampered with, inform your manager and contact IT Help.

Call
IT Help

1-800-493-1010

If a POS device is broken or inoperable, do not try to repair it. Contact IT Help. Broken devices will be replaced.

Suspicious
Behavior

No On-Site Repairs

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

1.24 MAIN MENU LAYOUT



1.25 Physical Security Best Practices



1.26 Summary of PCI DSS Compliance

Summary of PCI DSS Compliance

Let's review what we have learned about 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 brands to protect credit and debit card transactions and prevent the misuse of the cardholder's personal information. 	Compliance Responsibility All employees that handle anything regarding payment cards are responsible for keeping information safe. 
Landry's Role in Compliance Landry's has an obligation to keep payment card information safe. 	No Email Never accept payment card information by email. 
	No Electronic Storage Never store payment card data electronically. 

1.27 Summary of PCI DSS Compliance

Summary of PCI DSS Compliance

Let's review what we have learned about PCI DSS Compliance.

Security Breaches Do your part to prevent security breaches. Do not leave safes unlocked and do not throw payment card information in the trash. 	Payment Card Security Each brand of card has different security features to ensure authenticity. 
	POS Tampering Identify the most common forms of POS tampering. 
	POS Tampering Know what action to take if you suspect POS tampering. 

1.28 Questions about PCI DSS Compliance

Questions about PCI DSS Compliance

If you have any questions, comments, or concerns regarding PCI DSS Compliance, please contact Landry's Information Technology Department.



ITSecurity@ldry.com

Nibin Philip
Information Security Officer

 Nibin.Philip@ldry.com

1.29 PCI Security Awareness Training Acknowledgement

Read the statement below and click each box to acknowledge 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:

(Multiple Response, 10 points, 1 attempt permitted)

PCI Security Awareness Training Acknowledgement

Read the statement below and click each box to acknowledge 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 of 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, employees can write down customer credit card information.

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

1.30 Results

(Results Slide, 0 points, 1 attempt permitted)