

# **Credit Card Policy & PCI Security Training for U of I Merchants**

Processing and Handling Procedures

# Agenda

- Policy
- Terminology
- Security
- Roles and Responsibilities
- Reconciliation
- Best Practices
- Contact Info

# Policy

- The University of Iowa's Credit Card Handling Policy was established to communicate to all U of I merchants:
  - Requirements of PCI Data Security Standards
  - The rules and regulations all University of Iowa credit card merchants are expected to follow

## TERMINOLOGY

Term	Definition
PCI	Payment Card Industry
PCI DSS	<p>Payment Card Industry Data Security Standards</p> <ul style="list-style-type: none"> <li>• PCI DSS was the result of the alignment of the data security standards included in the VISA International and MasterCard Worldwide data security programs in 2001</li> <li>• In 2004 PCI DSS was endorsed by American Express, Discover Financial Services and JCB</li> <li>• PCI DSS was created to ensure the protection of cardholder data</li> </ul>
PCI SAQ	PCI Self Assessment Questionnaire
Merchant	The department, unit, division or college, that has been authorized to accept credit cards from its customers for payment of donations, goods or services.
Processor	Moneris Solutions is the organization the University has contracted with to process all merchant credit card transactions
Card Association	The organization “brand” of credit card; i.e. MasterCard, Visa, American Express, Discover
PAN	Primary Account Number; the credit card number

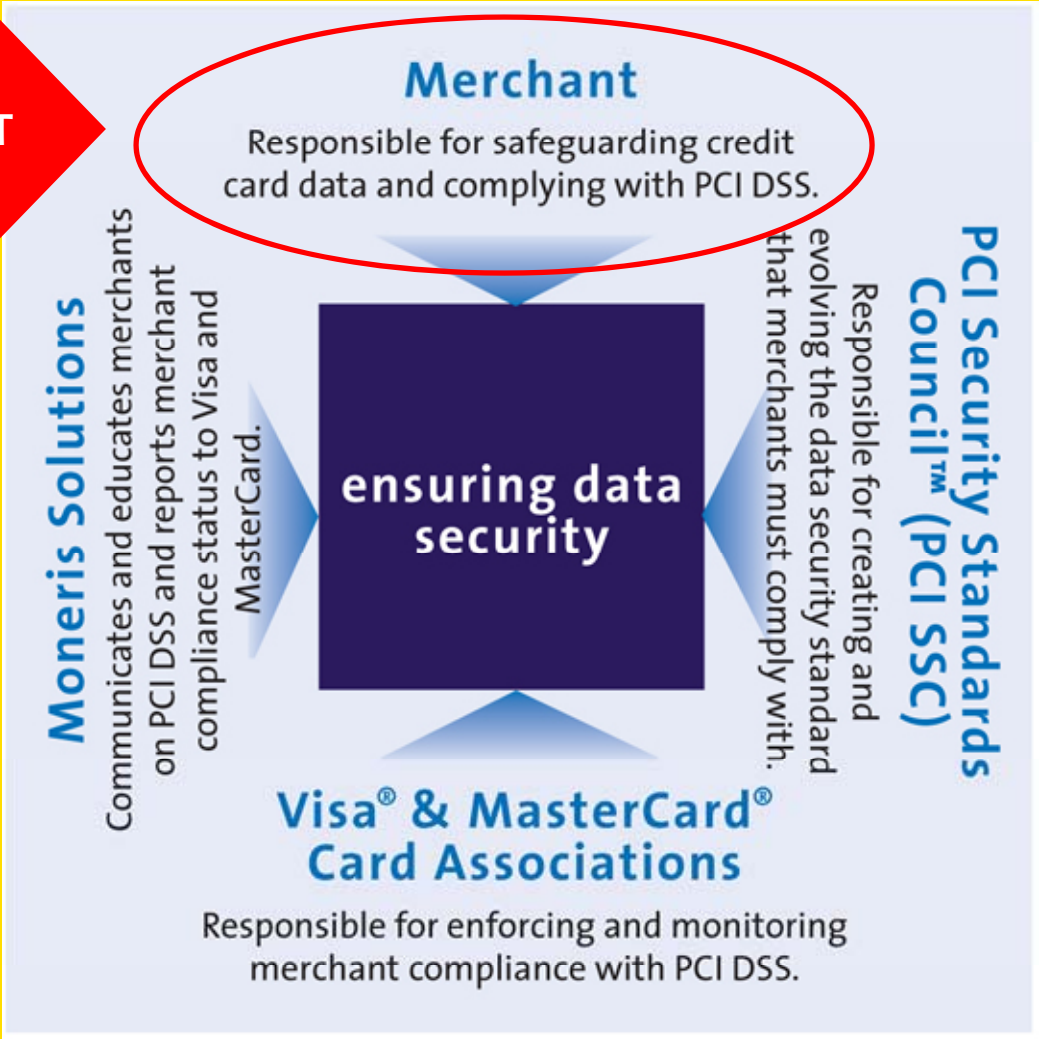
# Security

- Who are we protecting?
  - Cardholder – Fraudulent use of credit
  - University – Reputation
  - Your Unit – Reputation and financial costs
  - YOU! – Accusations of wrong doing

**Our #1 GOAL is**

**Protect Cardholder Information**

**YOU & YOUR UNIT**



# Security

- How do we protect credit card information?
  - Treat documents with credit card numbers just like cash
  - Segregation of Duties
    - Cashier function (front-line staff)
    - Accounting function (eDeposit entries)
    - Supervisory function (back office support)

# Security

- How do we protect credit card information?
  - Cardholder information should be secured and kept confidential.
  - Restrict access to credit card data to only those individuals whose job requires such access.

# Do you...

- Store, process or transmit cardholder data?
  - Point-of-Sale (POS)
  - Mail Order/Telephone Order (MOTO)
  - FAX
  - E-Commerce (website where customer can input their credit card information to complete a transaction)
- Use a system that processes or stores credit card data?
  - And are other systems connected to them?

**IF YOU ANSWER YES TO ANY OF THE ABOVE QUESTIONS THEN PCI-DSS APPLIES TO YOU!**

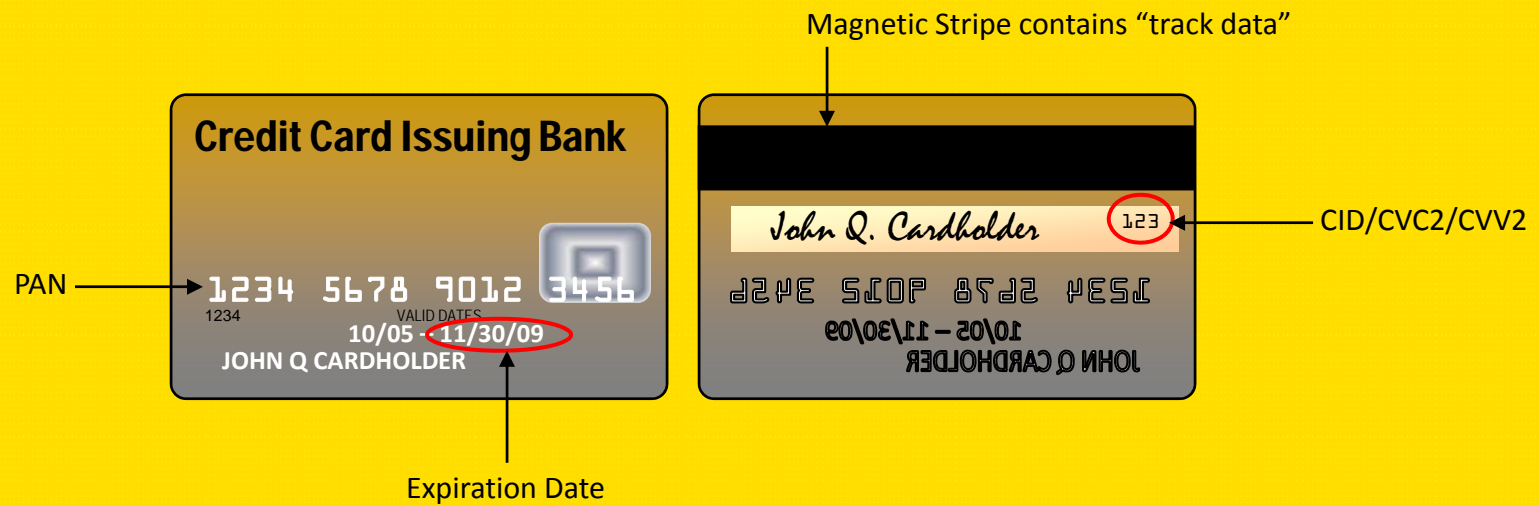
# PCI Data Security Standards

Control Objectives	Requirements
Build and maintain a secure network	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect cardholder data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>
Protect cardholder data	<ol style="list-style-type: none"> <li>3. Protect stored cardholder data</li> <li>4. Encrypt transmission of cardholder data across open, public networks</li> </ol>
Maintain a vulnerability management program	<ol style="list-style-type: none"> <li>5. Use and regularly update anti-virus software</li> <li>6. Develop and maintain secure systems and applications</li> </ol>
Implement strong access control measures	<ol style="list-style-type: none"> <li>7. Restrict access to cardholder data by business need-to-know</li> <li>8. Assign a unique ID to each person with computer access</li> <li>9. Restrict physical access to cardholder data</li> </ol>
Regularly monitor and test networks	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes</li> </ol>
Maintain an information security policy	<ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security</li> </ol>

Source: PCI SSC



# Cardholder Data



# Data Element Storage Guidelines

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
<b>Cardholder Data</b>	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date	YES	YES*	NO
<b>Sensitive Authentication Data**</b>	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

\*These data elements must be protected if stored in conjunction with the PAN

\*\*Sensitive authentication data must not be stored subsequent to authorization (even if encrypted)

# Costs of Non-Compliance

- Large fines and other costs
  - Financial liability for losses
  - Cost of forensic analysis
  - Cost of notification
  - Cost for credit watch services
  - Money held in escrow against future incursions
- Damage to the reputation of the University and the merchant unit
  - Loss of customer confidence
  - “Brand’ damage
- Loss of merchant status for the merchant unit and possibly the University

# Roles and Responsibilities

- Credit Card Transaction Processor (cashier)
- Credit Card Supervisor
- Reconciler

# Credit Card Transaction Processor

- Receives cardholder information via fax, mail, phone or in person
- Must agree not to disclose or acquire any credit card account information without the cardholder's consent
- Must follow procedures in accordance with Credit Card handling policy
  - Treating credit card receipts as cash equivalent
  - Protecting cardholder information

# Credit Card Supervisor

- Approves any refund requests
  - Refunds must be credited to the same credit card that was charged in the original transaction
- Receives daily batch information
- Prepares and submits e-deposit
- Delivers copy of each e-deposit form and supporting documentation to the Reconciler

# Credit Card Supervisor

- Enforce secure controls over all cardholder numbers and information
- Manage access to credit card data and processing to appropriate and authorized personnel
- Establish departmental segregation of duties

# Credit Card Supervisor

- Perform an annual self assessment to ensure compliance with Credit Card policy and PCI Data Security Standards

Payment Card Industry (PCI) Self-Assessment:

<https://www.pcisecuritystandards.org/tech/instructions.htm>

PCI Data Security Standards:

[https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf)

# Enforce Secure Controls Over All Cardholder Numbers And Information

- Cardholder data cannot be stored in any fashion on computers or networks.



## Especially spreadsheets!

PAN (credit card number)

Expiration date

Full Magnetic Stripe—AKA Track data  
(this is the most egregious violation of PCI-DSS!!)

CVC2/CVV2/CID

PIN



# Enforce Secure Controls Over All Cardholder Numbers And Information

- Credit card numbers must not be transmitted in an insecure manner



E-mail  
Text message  
Instant messaging  
Unsecured fax  
Campus mail



**Sealed envelopes are permitted**

# Enforce Secure Controls Over All Cardholder Numbers And Information

- All documentation containing card account numbers must be stored in a secure location.
- Access to credit card documentation should be given only to individuals who have a legitimate business “need-to-know”

# Enforce Secure Controls Over All Cardholder Numbers And Information

- Credit card documentation must be securely stored no longer than 18 months.
- 18 months after the transaction date credit card documentation must be destroyed.
- Method for destruction of data must be such that the account information is unreadable and cannot be reconstructed.

**TIP**

We recommend the use of a cross-cut paper shredder or lockable bin serviced by document destruction services.

# Limit Personnel Access to Restricted Data

- Background checks must be performed prior to hiring for any positions with unrestricted access to cardholder information (not necessary for cashier level personnel with access to only one card at a time)
- **All** personnel involved in credit card transactions must attend security training annually

# Segregation of Duties

- Establish and document departmental segregation of duties
  - Credit card transaction processing
  - Processing of refunds
  - Reconciliation



**Supervisory approval of all credit card refunds is mandatory**

# Annual PCI Self-Assessment

- Measure compliance with Credit Card Handling Policy and Procedures & PCI Data Security Standards
- Reports are submitted to Treasury Operations and kept on file
- PCI SAQ is mandatory for all merchants

# Technology Changes

- All changes in credit card processing technology must be reported to the IT Security Office and Treasury Operations **prior to purchase** and implementation

# Reconciler

- Verifies that the Credit Card Supervisor has recorded all credit card batches in e-deposits.
- Files supporting documentation and e-deposit information in a locked safe or filing cabinet.
- Reconciles credit card control account (IAcct 1100) to the supporting documentation and to the monthly statement from Moneris no less than monthly.
- Proof of reconciliation must be indicated by the Reconciler initialing and dating the hardcopy of the form being reconciled or another piece of supporting documentation.
- Reports of any unresolved reconciliation attempts must be reported to the departmental director on a monthly basis.

# Accounting (eDeposits & Reconciling)

The individual responsible for reconciliation of credit card transactions should not be involved in processing credit card sales or refunds.

# Accounting (eDeposits & Reconciling)

- The daily net sales (sales minus refunds) electronically settle into the University's bank account approximately two business days after the batch settlement
- Funding information from credit card sales is automatically loaded into the E-deposit system daily

## Credit Card Accounting Process

[http://www.uiowa.edu/~cashier/policies\\_procedures/DeptCreditCard](http://www.uiowa.edu/~cashier/policies_procedures/DeptCreditCard)

# Accounting (eDeposits & Reconciling)

- It is the responsibility of the credit card merchant unit to submit credit card e-deposits within three working days of the batch settlement

# Accounting (eDeposits & Reconciling)

- It is the responsibility of the credit card merchant to reconcile the settlement amount in the general ledger (inst acct 1100) to the credit card receipts on a regular basis, no less than monthly



The Accounts Receivable control account should not have a negative balance if all e-deposit entries are recorded in a timely basis.

# Accounting (eDeposits & Reconciling)

- Online reporting is accessible through <http://www.myclientline.net> for reconciliation purposes
- Users must enroll\* for access to MyClientLine and it may take several business days for your enrollment request to be processed and your login ID assigned

\*Check with Laurie Lentz to find out what merchant account number to use when enrolling for MyClientLine access.

# Best Practices

- NEVER e-mail credit card information
- NEVER store credit card numbers in any database or spreadsheet
- Truncate all but the last four digits of credit card numbers on any document where the complete number is visible (after the transaction has been successfully processed)

# Best Practices

- Keep credit card documentation locked in a safe or filing cabinet
- Permit only employees who have a legitimate business “need-to-know” access to cardholder information
- Don’t allow unauthorized persons access to areas where credit card data is stored

# Best Practices

- Credit card transaction records must be kept a minimum of 18 months
- Destroy documentation containing credit card information when it is no longer needed for business or legal reasons  
(cross-cut paper shredder or document destruction lockable bin)

# Best Practices

## Recommendation:

Document departmental desktop procedures addressing requirements as listed within this presentation and update cash handling procedures to include the acceptance of credit cards

# Best Practices

- Settle credit card sales at the end of each day
- Record daily credit card sales in E-deposits
- Balance credit card control account no less than monthly
- Segregate duties; the individual performing reconciliation should not be involved in processing credit card sales or refunds

# Security Incidents

- Reporting of suspected or known security breaches is **MANDATORY**
- Contact the following for investigation:
  - Supervisor or DEO
  - IT Security Office
    - 335-6332 or [security@uiowa.edu](mailto:security@uiowa.edu)  
[Security Incident Online Reporting Form](#)

# Security Incidents

- Examples:
  - Secure files/cabinets appear tampered with
  - Lost/stolen keys
  - Computer workstation breach/infection/compromise
  - ID & password stolen/known
  - Unusual/unexplained credit transactions in your account

# Important Links

## Credit Card Policy:

[Link to U of I Credit Card Handling Policy](#)

## PCI Data Security Standards:

[Link to PCI Data Security Standards v1.1](#)

## Payment Card Industry (PCI) Self-Assessment:

[Link to PCI Data Security Standards Self-Assessment Questionnaires v1.1](#)

## Credit Card Accounting Process:

[Link to Credit Card Accounting Instructions](#)



# Contact Info

- *Treasury Operations*
  - Laurie Lentz, 5-1398, [laurie-lentz@uiowa.edu](mailto:laurie-lentz@uiowa.edu)
- *Accounting Services*
  - Contact your Org Contact
- *IT Security Office*
  - Jane Drews, 5-5537, [jane-drews@uiowa.edu](mailto:jane-drews@uiowa.edu)