Payment Card Industry Training 2014

Phone Line Terminal &
Hosted Order Page/Secure Acceptance Redirect Merchants

Contact * Carole Fallon * 614-292-7792 * fallon.82@osu.edu

Updated May 2014
AGENDA

A. Payment Card Industry, PCI, Security Awareness Training
B. PCI Incident Response Training
C. PCI & Incident Response Training Certification Form
D. Credit Card Processor Best Practices & Manager Finance Facts
Who needs PCI training?
How often?

All personnel who manage and all personnel who “transmit, process or store cardholder data.”
Upon hire and annually.
Purpose of Training

1. Awareness to prevent a breach of cardholder data.
2. Protect customers’ cardholder data.
3. PCI Regulation 12.6 - Implement a formal security awareness program to inform personnel of the importance of cardholder data security.
4. PCI Regulation 12.9 - Implement an incident response plan. Be prepared to respond immediately to a system breach incident.
What is PCI DSS?

Payment Card Industry Data Security Standards
Why was it developed?

1. Protect the card brands’ reputation as a secure method of payment.
2. Protect customers’ cardholder data
3. Establish Data Security Standards for any entity accepting credit and debit cards.
Who developed the Data Security Standards?

The PCI Council

The Council includes the major card brands - Visa, MasterCard, Discover, and American Express.

Established in 2006 to develop one set of security standards for all card brands.
What organizations must comply with PCI?

Any entity that accepts Visa, MasterCard, Discover, or American Express credit or debit cards.
How are Data Security Standards enforced?

Credit Card Processor (First Data) enforces by:
Self Assessment Questionnaire by merchant or QSA, Qualified Security Assessor, onsite visit.
Are all organizations audited annually by a PCI assessor? 

A merchant with over 1,000,000 Visa or Master Card transactions annually must have a QSA, Qualified Security Assessor, or a certified ISA, Internal Security Assessor, complete an annual RoC, Report of Compliance. OSU is audited and submits a RoC.
What is a RoC, Report of Compliance?

The RoC is a 600+ page document prepared by a PCI QSA, Qualified Security Assessor, listing each merchant’s compliance data. This report is submitted to our merchant processor to verify OSU’s compliance. July/August 2014 QSAs will be onsite to visit OSU merchants to validate compliance with the DSS, Data Security Standards, that apply to each merchant’s method of accepting credit and debit cards. Each merchant must pass the audit. If any merchant fails the audit, the merchant must remediate immediately.

If one merchant fails the audit, OSU as an organization is not compliant.
THE OHIO STATE UNIVERSITY

Data Breach

What are the consequences?

Got Hacked?
$5,404,000 – Estimated cost of an organization’s data breach.

(Ponemon Institute & Symantec 2013 report based on 2012 breaches)

Costs of a breach included in our Merchant Processing Contract:
- Fines and penalties levied by each of the card brands.
- Cost to hire forensic experts.
- Cost to reissue customers’ credit cards.

Additional Costs:
- Free Credit Monitoring (avoid identity theft following breach).
- Reputational risk for OSU.
What are the Data Security Standards and do all the standards apply to my merchant account?
The Ohio State University
12 Standards & 226 Regulations

The PCI Data Security Standard

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data. It consists of common sense steps that mirror security best practices.

<table>
<thead>
<tr>
<th>Goals</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
</table>
| **Build and Maintain a Secure Network** | 1. Install and maintain a firewall configuration to protect cardholder 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 or programs  
6. Develop and maintain secure systems and applications                                |
| **Implement Strong Access Control Measures** | 7. Restrict access to cardholder 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 for all personnel            |
Terminal Merchants – 32 regulations
Hosted Order Page or Secure Acceptance Web Mobile Pay Redirect merchants – 13 regulations.
Internet Merchants – 226 regulations.
Cardholder Data & Sensitive Authentication Data

What are they?

Cardholder Data – Store Securely
1. PAN, primary account number – 16 digit number on cards
2. Cardholder’s name
3. Expiration date
Sensitive Authentication Data – DO NOT STORE

1. CVV, Card Verification Value – 3 or 4 digit number on cards
2. Magnetic Stripe Data
3. PIN, Personal Identification number
CVV code - Sensitive Data cannot be stored
Terminal Merchants

Best Practices

1. Terminal – does not print full PAN, 16 digit number, on any receipt or report.
2. Forms – do not have forms on file with PAN.
3. Transmission – do not send a PAN by e-mail, fax, OSU mail or other messaging technology.
4. Terminal location
   - terminal is located in an environment where other personnel can view the processing of credit cards.
   - terminal is in a protected location not accessible to the public or to others not processing credit cards.
Terminal Merchants – DSS Requirements

Regulation 3 – Protect Cardholder Data

a. Do not store or record on any media, paper or electronic device, customers’ CVV code (3 or 4 digit code on front or back of card).

b. Do not store or record on any media, paper or electronic device, customers’ PIN # (Personal Identification number.)

c. The terminal display and receipts must mask the cardholder 16 digit number except the last 4 digits.

d. Do not acquire or disclose cardholder data without customer’s consent.
Terminal Merchants DSS Requirements

Regulation 4 – Encrypt transmission of cardholder data on public networks. The PAN (16 digit number) cannot be scanned or sent by e-mail, fax, or other messaging technology.

Regulation 7 – Restrict access to cardholder data by business “need to know”. Do not allow public access.
Terminal Merchants DSS Requirements

Regulation 9 – Restrict physical access to cardholder data.

a. All media, electronic or paper, that contains cardholder data is physically secured and locked.
b. All media that contains cardholder data is sent by secure courier or US mail and is accurately tracked. (It cannot be sent by OSU mail.)
c. All media that contains cardholder data is destroyed when it is no longer needed. (Retention is 2 years.)
d. All media that contains cardholder data is destroyed using a cross cut shredder.
e. Escort and supervise all visitors and OSU personnel not responsible for processing cardholder data in areas where cardholder data and terminals are maintained.
Terminal Merchants DSS Requirements

Regulation 12 – Maintain a Security Policy

a. PCI Policy 5.15 is disseminated to all relevant personnel.
b. Policy is reviewed annually. (Treasurer’s Office reviews.)
c. List of terminal devices is maintained.
d. Formal “Security Awareness Training” is available to all personnel who “transmit, process, or store” cardholder data.
e. Distribute “Security Incident Response Procedures.”
f. Background Check – required if access to more than “one card number at a time.” Does not apply to cashiers.
Annual Audit by External Auditors – July/August 2014

1. PCI and Incident Response Training - Complete Training for all personnel who process cards.
2. PCI Training and Sign Certification – After completing training, all personnel who process credit cards must sign the “PCI Training and Incident Response Training Certification Form.” Managers keep forms on file for internal or external audit.
3. Disseminate PCI Policy 5.15 to all personnel who process credit cards.
4. Insure terminals are not printing 16 digit card number or the expiration date on receipts or reports.
5. No personnel may store the CVV code, 3 or 4 digits, or a customer’s PIN number.
6. Insure terminals are not accessible to personnel not processing cards. Escort and supervise visitors and OSU personnel not responsible for processing cards.
7. The PAN, primary 16 digit account number, may not be sent by scan, e-mail, fax or any messaging technology.
8. Destroy cardholder data when no longer needed. (2 year retention. Full 16 digit number does not need to be retained; only the transaction record.)
9. Background Check for personnel with access to more than one card number at a time.
10. Refunds and Safety- Check with merchant processor regarding a password on your terminal to insure no changes can be made to tamper with the terminal. Refunds should only be made with manager approval.
DSS Requirement 8 - Passwords

This requirement applies to merchants using the Internet and does not impact merchants processing using a phone line terminal. It is important to be aware of the following password standards.

1. Do not use group, shared, or vendor supplied passwords.
2. Immediately change the password initially issued.
3. Change password every 90 days.

Strong password – Use the initials of a sentence.

“I travel every year to the Grand Canyon with a friend named Kim!”

IteyttGCwafnK!
Incident Response Procedure

"Report immediately a credit or debit card security incident to my supervisor, the Office of Financial Services, and the Office of the CIO if I know or suspect card information has been exposed, stolen, or misused.

1. Notify supervisor in writing.
2. Office of Financial Services by fax 282-7568.
3. Office of the CIO by e-mail security@osu.edu.
HOP or SA Web Mobile Pay
Redirect Merchants

What is a Hosted Order Page
Secure Acceptance Web Mobile Pay
Redirect Merchant?
HOP/SA Web Mobile Pay Redirect Merchant is…

an OSU merchant that redirects the customer to a third party PCI approved service provider to transmit, process, and store the credit or debit card payment on the third party’s site. An example of an approved third party provider is Cybersource and Authorize.net.
HOP/SA Web Mobile Pay Redirect
Merchant reduces your PCI “Scope”. This means only 13 of 226 regulations must be met.
PCI Approved Third Party Service Providers are listed on the Visa Global Registry.
Regulation 9 – Restrict Physical Access to Cardholder Data

OSU personnel should not have access to cardholder data. The customer will enter their card number online on their personal computer. OSU personnel should not enter customers’ cardholder data.
HOP/SA Redirect Merchants

Regulation 12 – Maintain a Security Policy

a. PCI Policy is disseminated to all relevant personnel.

b. Policy is reviewed annually. (Treasurer’s Office reviews.)

c. Formal “Security Awareness Training and Incident Response Training” is available to all personnel who set up and maintain the HOP/SA and personnel responsible for assisting in processing or reconciling.

d. Distribute “Security Incident Response Procedures”

e. Regulation 12.8 – a written agreement that the third party acknowledges responsibility for the security of cardholder data. (See sample in Policy 5.15.)
HOP/SA Manager Responsibility Checklist.

Annual Audit by External Auditors – July/August 2014

1. PCI and Incident Response Training - Complete training for all personnel involved in setting up and maintaining the website, personnel responsible for reconciliation, and personnel with access to cardholder data.

2. All personnel who complete training must sign the “PCI and Incident Response Training Certification Form” after completing training. Managers keep forms on file for internal or external audit.

3. Disseminate PCI Policy 5.15 to all personnel who are trained.

4. Do not process payment for customers. Only customers may enter their credit or debit card number. Customers are not permitted to enter their cardholder number from an OSU computer as this would put the OSU network “in scope” for PCI and 226 PCI regulations must be met.

5. Use a Level 1 approved third service provider listed on the Visa Global Registry.

6. Maintain copy of Third Party Service Provider’s agreement stating the service provider is responsible for credit card data security.
Incident Response Procedure

“Report immediately a credit or debit card security incident to my supervisor, the Office of Financial Services, and the Office of the CIO if I know or suspect card information has been exposed, stolen, or misused.

1. Notify supervisor in writing.
2. Office of Financial Services by fax 282-7568.
3. Office of the CIO by e-mail security@osu.edu.
Reference Links

Service Provider Registry – http://visa.com/spllisting/search_Grsp.do
OSU Policy – www.busfin.ohio-state.edu/FileStore/PDFs/515_CreditCard.pdf
PCI Council Website – https://www.pcisecuritystandards.org
My Client Line online reporting – www.myclientline.net

Select orange “Enroll” tab and enter merchant number (219#), OSU Tax ID, OSU Bank account number and Contact information. HELP DESK 800-984-6305
PCI and Incident Response Training Certification Form

• I have completed the PCI, Payment Card Industry, Training and Incident Response Training.
• I have read OSU Policy 5.15.
• I understand the University will take appropriate corrective action up to and including termination and/or criminal action against employees who violate the OSU Credit Card PCI Policy. I understand compliance with the Policy is to protect the University from onerous fines and penalties levied by the card companies in the event of a credit card breach.
• I understand it is my responsibility to report immediately a credit or debit card security incident to my supervisor, the Office of Financial Services, and the Office of the CIO if I know or suspect card information has been exposed, stolen, or misused.
  a. Report to my supervisor in writing.
  b. Report to the Office of Financial Services by fax 292-7568.
  c. Report to the Office of the CCIO by email to security@osu.edu and by phone to 688-5650.

____________________________________   ____________________________________
Print Name        Date

____________________________________   ____________________________________
Signature       Merchant Name/Department
Credit Card Processor - Best Practices

Credit Card Processor - Best Practices
a. Card Present
b. Card Not Present
c. Authorization and Settlement
d. Credit and Debit Card Fees - Ways to reduce credit and debit card fees
e. Terminal Controls
f. New Terminals – EMV, Euro MasterCard Visa, Chip and Pin

Manager - Finance Facts

Manager - Finance Facts
a. Terminal Controls
b. Auto Journal in PeopleSoft
c. Reconciliation
d. Sales Tax
e. Debit and Credit Card Fees
f. Debit Card and Durbin
g. Conference Registrations
CARD PRESENT TRANSACTION (CP)

Check list when processing a credit card:

1. Expiration date – check to be sure the card has not expired.
2. Card signature on back of card matches the signature of signer.
3. Card may only be used by the owner of the card.

Swipe Card – the fees are cheaper to process a card that is swiped.

Key Enter – this is more costly to process.

CODE 10 Suspicious Transaction – call the Voice Authorization Center and ask for Code 10
CARD NOT PRESENT (CNP)

Internet, Telephone orders and Mail in Orders are examples.

CNP transactions are riskier transactions.

Checklist

1. If possible, obtain the customer’s signature.

2. Internet transactions – use AVS, Address Verification Service. (This will check the zip code and address against the card owner’s address.)

3. Internet transactions – list OSU’s Privacy Policy
Credit Card Processor
Authorization and Settlement

Credit Card Process – two steps

1. Authorization of Cards – indicates availability of credit on a customer’s account at the time the authorization is requested.

2. Settlement of Funds with the Bank – The transfer of a customer’s funds from their credit card issuer’s account to our JP Morgan Chase account.
Credit Card Processor - Authorization

CREDIT CARD TRANSACTION FLOW

Cardholder → Merchant → Acquiring Bank → Credit Card Issuer
Credit Card Processor - Settlement

FUNDS are not sent to our Bank account until the transactions are SETTLED.

Settlement Bank and Acquiring Bank/Processor
JP Morgan Chase – settlement bank
Huntington First Data - acquiring bank/processor

Settlement of funds
Terminals - Determined by time the terminal is “batched out.”
HOP/SA – Determined by the third party’s settlement process.

General Settlement Time between OSU’s Bank and Acquiring Bank
Visa/MC – two business days (Monday settlement deposited Wednesday)
Discover – two business days.
American Express – three business days.

PeopleSoft /eReports – add additional day for bank file to be loaded into PeopleSoft.
Ways to Reduce costs:

1. MCC Codes – Merchant Category Code (Treasurer’s office)

2. Swipe card vs. Key Enter – avoids “downgrade” or increase in fees.

3. Settle or “batch out” same day.

4. Use new terminal that sends “Level 2” data.

5. IT configures software to send “Level 2” data.

6. AVS – Address Verification Service.

Type of Card Presented - Cannot control type of card presented. Merchant pays higher fee for Platinum, World Points and other premium cards.
Credit Card Processor  
Terminal Controls

1. Be familiar with your terminal. Notice if there is a change or device added to your terminal.

2. Skimming – hacker device installed on a terminal that records cardholder information. Notify supervisor if you notice changes.

3. Notify supervisor if the terminal has been replaced.

4. Notify supervisor if you receive a call to make program changes to your terminal.
EMV – Euro MasterCard Visa
Chip and Pin Card

New Terminals – Fall 2015
If not using EMV terminal, the chargeback/dispute process for merchants will be more difficult.

Fall 2015 - Liability for fraud shifts from the card issuers to the merchant for fraud losses in Card-Present sales.
Manager Finance Facts

Terminal Controls

1. Auto Settle – Manager should program the terminal to automatically settle transactions at the end of the business day. (9 pm suggested time.)

2. Terminal Passwords and Codes

   Refunds – Contact Credit Card Processing Company or Treasurer’s Office to program terminal to set up password for administrator only to enter Refunds.

   Terminal Code – Terminals have a code that can be assigned to each processor. Each processor can log in to identify the person processing the transactions.
Manager Finance Facts
Auto Journal

Auto Journal

OSU “Intellimatch” Auto Journal Process

1. When the merchant account is set up, the chartfield information provided is recorded in OSU’s new software Intellimatch.

2. When deposits are received or fees charged for credit card processing, an automated journal is recorded in PeopleSoft. The transactions can be viewed and researched in eReports.
1. Reconcile Card Transactions to BANK transactions recorded in PeopleSoft/eReports. (Bank transactions are JP Morgan Chase transactions uploaded to PeopleSoft and available on eReports).

2. Merchants must reconcile the credit card transactions daily from their terminal report, First Data report, or online report to the bank transactions.

3. Credit card statements are provided by First Data via mailed monthly statements or an online service, “My Client Line”.

4. MY CLIENT LINE – online reporting (See Reference Links in this PowerPoint.)
OSU Merchants must charge sales tax where applicable.

Tax rate in Franklin County is 7.5%

Contact: Scott Gill 2-7540; gill.414@osu.edu

Taxable items:
1. Most tangible goods – food (exceptions apply), clothing, publications, band CDs, chemicals, computer hardware, software, flowers, art, etc.
2. Services – sports memberships

Non-taxable
1. Ticketing events
2. Donations
3. Tuition

Sales tax reports are due on the 15th of the following month.
Manager Finance Facts
Credit & Debit Card Fees

Basic Fees – average cost 2% - 2.5%
1. Processor transaction – First Data
2. Card Brand fees
   Visa/MC – “Interchange” fee varies
   Discover – flat fee
   AmEx - flat fee

Additional Fees
1. Online fee – if using a gateway such as Cybersource.
2. Software – may have additional transaction fees.
Manager Finance Facts
Debit & Durbin

Debit Card and Durbin Amendment

Regulated Banks > $10B
Limited to charging 22 cents + .05%

Now more costly for merchants to process small $5.00 debit card purchase = 4.4% rate

Unregulated Banks can charge higher debit card fees.
Manager Finance Facts
Conference Registrations

REG ONLINE – Conference Registration Company

Contract: Contract pre-signed by OSU and Medical Center legal department.

Contact: Michael Cimperman
michael.cimperman@lanyon.com
303-465-7460