PCI COMPLIANCE 2013

MERCHANT ACCOUNT USERS

PRESENTATION BY: Dawn MacAdams-Mull
Contact Info: 215-746-6369
dawnmac@upenn.edu
Purpose of PCI Compliance

• The Payment Card Industry has established important and stringent security requirements to protect credit card data. These are called PCI Data Security Standards or “PCI-DSS”.
  – Protects against:
    • Identity theft
    • Fraudulent activity

• The PCI-DSS policy defines the way in which credit card merchant accounts must protect cardholder data and achieve PCI compliance based on the method that credit cards are processed.
  – Various processing methods include:
    • Phone processing
    • Terminals
    • Internet
Risk of Non-Compliance

• Without adherence to the PCI-DSS standards, the University would be in a position of unnecessary reputational risk and financial liability.

• Merchant account holders who fail to comply are subject to:
  – Any fines imposed by the payment card industry.
  – Any additional monetary costs associated with remediation, assessment, forensic analysis or legal fees.
  – Suspension of the merchant accounts for the whole University.
  – Schools and Centers who are found to fail PCI compliance will be held liable and any fees or fines will be imposed against them NOT the University.
Responsibility of the Treasurer’s Office

• The Treasurer’s Office is responsible for issuing credit card merchant accounts and for overseeing policies and procedures regarding payment processing.

• Responsibility and authority to ensure that all merchant accounts and any related third party payment processors adhere to the PCI requirements to protect cardholder data throughout the University.

• Responsible for submitting the annual Report On Compliance (ROC) to our acquiring bank.
Responsibility of the Senior Business Officers

• Responsible for ensuring that a PCI self assessment is completed each year for every merchant account user.
  – Can be found through Knowledge Link.

• Must certify that their organization is PCI compliant by signing off on the PCI Compliance questionnaire.
  – Questionnaire will be sent in an email
  – Non-Compliance will lead to remediation. The Audit and Compliance team will work with your department to help you achieve PCI Compliance
Merchant Account Owners

• Maintaining PCI compliance.
• Responsible for identifying possible merchant account handlers (anyone who takes credit card numbers, cards or information regarding merchant accounts) throughout the department.
• Holding all confidentiality forms for all merchant account handlers in the department.
  – This form will be available at the end of the “Payment Card Industry - Data Security Standards Workforce Education – Penn” test, available through Knowledge Link. If you completed Penn Profiler, this will be a required course, otherwise you can find it listed in the course catalog.
Time Line of Events

– June-July: I will be reviewing merchant account feeder files and reaching out to account owners for feeder account verification.

– August-September: Once all feeder accounts are verified, I will reach out to each school and center to make sure addresses, account owners and merchant accounts are updated. I will also be requesting a list of all merchant account users.

– October: Scheduled release of the PCI Compliance Questionnaire 2.0. All questionnaires must be finished and sent back to the Treasurer’s office no later than October 31, 2013

– November: Knowledge link course will be completed by all merchant account users within your department by November 30, 2013

– December: Certification is due. Next year’s kick off for PCI compliance will begin. This is a calendar year requirement.
Questions