WHAT LEADERS NEED TO KNOW ABOUT TAKING CREDIT CARDS

Business Practices Seminar

April 3, 2014

OVERVIEW

- Departmental Operations
- Review of Payment Card Industry Standard
- Assessment Process Overview
- Review of University Policy No. 3610

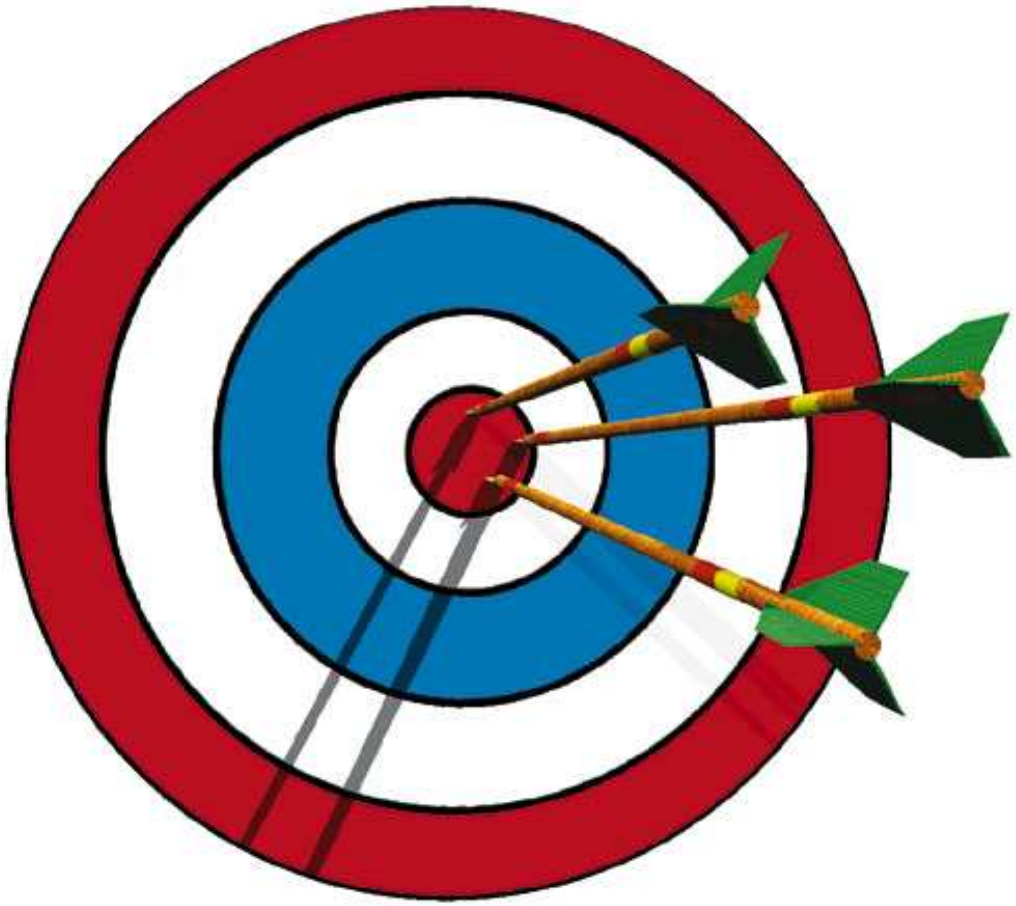
CHALLENGE ---

57.7

467

200+

TARGET



WHAT'S BEST FOR MY DEPARTMENT?

Scott Weimer
Director of Continuing and Professional Education

Elizabeth Scharman
Center for the Arts at Virginia Tech,
Director of Administration

Melinda West
University Bursar

CHOOSING "THE" SOLUTION:

- Volume?
- Total sales? Added costs?
- Retail? Internet? MOTO? Brick-n-Mortar?
- Equipment requirements?
- Mobility?
- System integration?
- Competition (Peer) practices?
- Customer/Retailer convenience? i.e. 24/hr availability
- Inventory management?
- IT expertise?
- Outsource?

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

Reflects industry best practices

WHAT IS PCI-DSS?

- Payment Card Industry Data Security Standards (PCI DSS)
  - The 5 members of the payment card industry banded together to develop
  - 12 overarching security requirements
  - to protect cardholder data and
  - to reduce losses from fraud

ELEMENTS OF A PAYMENT CARD

- Cardholder data
  - PAN (Primary Account Number)
  - Expiration Date
  - Cardholder Name

ELEMENTS OF A PAYMENT CARD

- Sensitive Authentication Data
  - CVC or CVV (Card Verification Code) – 3 or 4 digit code used in card-not-present transactions
  - Full Magnetic Stripe – data encoded in the magnetic stripe for authorization during transactions when the card is swiped

PCI STANDARDS FOR STORED CARDHOLDER DATA

		Data Element	Storage Permitted	Render Stored Account Data Unreadable
Account Data	Cardholder Data	Primary Account Number (PAN)	YES	YES
		Cardholder Name	YES	NO
		Service Code	YES	NO
		Expiration Date	YES	NO
	Sensitive Authentication Data	Full Magnetic Stripe Data	NO	CANNOT STORE
		CAV2/CVC2/CVV2/CID	NO	CANNOT STORE
		PIN/PIN Block	NO	CANNOT STORE

Per University Policy 3610, cardholder data may NOT be stored

WHAT IS PCI-DSS NOT?

- PCI Compliant does NOT equal Secure and vice versa
- One-size fits all
- One-time effort
- Low-effort or Low-cost

WHY FOLLOW PCI STANDARDS?

- Protect customers against fraud and identity theft
- For the university's protection to avoid potential financial liabilities, loss of reputation and customers, as well as litigation.
- Contractually mandatory
  - Under PCI DSS rules, acquiring banks are contractually responsible for ensuring that any merchants they authorize for payment card transactions are fully compliant with PCI DSS requirements. They can be fined if one of their merchants gets breached as a result of a failure to comply with PCI. Acquiring banks typically pay the fines to the credit card companies, and later recover it from the merchant that suffered the breach.

WHY FOLLOW PCI STANDARDS?

- Applies to any operation processing or transacting business, including those using a third party, which touches credit cards
- Potential for substantial penalties for compliance failure
  - penalty of $5,000 - $100,000 per month, per brand for noncompliance
  - fine/penalty of up to $500,000 per brand per data security incident
  - liability for all fraud losses incurred from compromised account numbers
  - liability for the costs of investigation
  - liability for the costs of re-issuing cards associated with the compromise

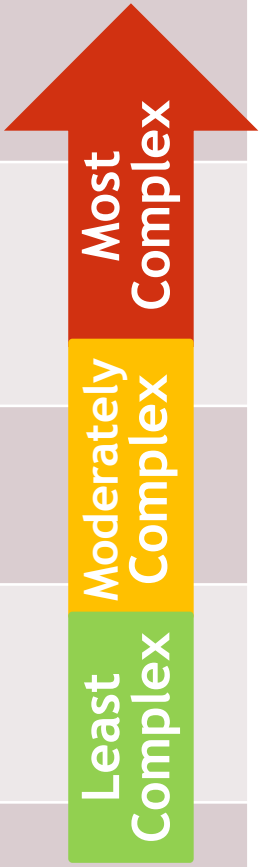
CHALLENGES WE FACE:

- Identifying affordable and compliant solutions that meet operational and service needs of campus operations
- Mobile payments/Secure mobile payments
- EMV capable readers beginning in October 2015
- Evolving requirements as the Council refines approach
- Changes in scope for e-commerce
  - E-commerce merchants specifically excluded from validating with all SAQs except SAQ A, SAQ A-EP or SAQ D

SELF ASSESSMENT QUESTIONNAIRE - V2.0

GENERALLY VALID THROUGH DECEMBER 31, 2014 FOR CONTINUING MERCHANT ASSESSMENTS

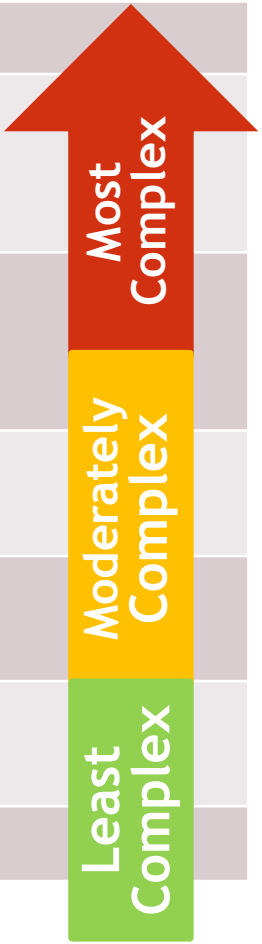
SAQ	Method of Acceptance	Requirements	Complexity of Transaction Process
D	All other SAQ eligible service providers for all merchants not meeting the descriptions of SAQ A – C	289	
C	Those who process cardholder data via payment applications connected to the internet but who do not store cardholder data on any computer system	80	
C-VT	Those who process cardholder data only via isolated virtual terminals on personal computers connected to the internet	51	
B	Those who process cardholder data only via imprint machines or via standalone, dial out terminals	29	
A	Third party hosted	13	



SELF ASSESSMENT QUESTIONNAIRE - V3.0

EFFECTIVE JANUARY 1, 2014; MANDATORY FOR ALL BEGINNING JANUARY 1, 2015

SAQ	Method of Acceptance	Requirements	Complexity of Transaction Process
D	All other SAQ eligible service providers	326 (+37)	
C	Process via payment applications connected to the internet but do not store cardholder data on any computer system	139 (+59)	
A-EP	Partially outsourced e-commerce merchants using third party website for payment processing	139 (+126)	
B-IP	Process through stand alone IP-connected terminals	83 (+54)	
C-VT	Process cardholder data **only** via isolated virtual terminals on pc connected to the internet	73 (+22)	
B	Process cardholder data **only** via imprint machines or via standalone, dial out terminals	41 (+12)	
A	Fully outsourced e-commerce merchant	14 (+1)	



E-COMMERCE

V2.0

- Integrated hosting/shopping on department website with preferred third-party vendor handling payments
- Payment page/order without integration
- Analog swipe terminals

V3.0

SIGNIFICANT CHANGES IN V3.0

- SAQ A-EP
  - Changes determination of in-scope machines with additional measures to counter known hacker exploit in the merchant hosted web-pages redirecting to a hosted, compliant service provider
  - Requires external scanning quarterly, internal scanning quarterly and after any significant changes in the network environment, and external penetration test annually

SIGNIFICANT CHANGES IN V3.0

- Physical Protection of POS Terminals and Systems
- Cardholder Data Flow Diagrams Required for All
- In-scope Systems

QUESTIONS?