

# Accepting Payments Securely - Online and off

Presented by Bryan Boutz  
October 2009 IT Security Training

- The problem – collecting payments, especially electronically
- Credit Cards and PCI-DSS
  - What is it?
  - Why bother?
  - Where do we start?
- Other payment methods
- Solutions and examples
- Discussion

## Agenda

- Rules for securing cardholder data that is stored, processed, and/or transmitted by merchants and other organizations.
- Apply to EVERYONE that touches the data.
- Set by the Payment Card Industry Security Standards Council, which represents major credit card networks.  
<https://www.pcisecuritystandards.org>

**What is PCI-DSS?**

- 12 requirements in 6 sections

Build and Maintain a Secure Network	<ul style="list-style-type: none"><li>• Install and maintain a firewall configuration to protect cardholder data</li><li>• Do not use vendor-supplied defaults for system passwords and other security parameters</li></ul>
Protect Cardholder Data	<ul style="list-style-type: none"><li>• Protect stored cardholder data</li><li>• Encrypt transmission of cardholder data across open, public networks</li></ul>
Maintain a Vulnerability Management Program	<ul style="list-style-type: none"><li>• Use and regularly update anti-virus software</li><li>• Develop and maintain secure systems and applications</li></ul>
Implement Strong Access Control Measures	<ul style="list-style-type: none"><li>• Restrict access to cardholder data by business need-to-know</li><li>• Assign a unique ID to each person with computer access</li><li>• Restrict physical access to cardholder data</li></ul>
Regularly Monitor and Test Networks	<ul style="list-style-type: none"><li>• Track and monitor all access to network resources and cardholder data</li><li>• Regularly test security systems and processes</li></ul>
Maintain an Information Security Policy	<ul style="list-style-type: none"><li>• Maintain a policy that addresses information security</li></ul>

The standards

- 4 levels of certification

1	<p>Any merchant-regardless of acceptance channel-processing over 6,000,000 transactions per year.</p> <p>Any merchant that has suffered a hack or an attack that resulted in an account data compromise.</p> <p>Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.</p>
2	<p>Any merchant-regardless of acceptance channel-processing 1,000,000 to 6,000,000 transactions per year.</p>
3	<p>Any merchant processing 20,000 to 1,000,000 e-commerce transactions per year.</p>
4	<p>Any merchant processing fewer than 20,000 e-commerce transactions per year, and all other merchants-regardless of acceptance channel-processing up to 1,000,000 Visa transactions per year.</p>

## Merchant certification

In the event of the a breach, the acquirer CAN make the merchant responsible for:

- Fines of up to \$500,000 per incident
- Cost to notify victims
- Cost to replace cards (about \$10/card)
- Cost for any fraudulent transactions
- Forensics from a Qualified Security Assessor
- Level 1 certification from a QSA

**Cost of non-compliance**

- Large, complex networks with many devices and interconnections with other networks
- Large community with complicated mix of backgrounds, skills, and requirements
- Extremely “open” by tradition and culture
- Departments control local technology and act independently
- Understaffed IT departments

## Challenges in Higher Education

- Training
- Qualified Security Assessor
- Make a plan and prioritize

**Where do we start?**

- Cash and physical checks
  - Keep it secure
  - Good accounting practices and controls
- E-Checks, direct payments, etc
  - Generally lower cost but higher risk
  - Rules set by National Automated Clearinghouse (NACHA) now Electronic Payments Association
  - Work with your bank
  - Build a relationship with the customer

**Other payment methods**

- Do it yourself
  - PCI requirements are available and QSA are willing to help.
  - Works best if highly centralized or already fairly secure.
- Contract with a service provider
  - Examples include PayPal, Google Checkout, Authorize.net, and Cashnet.

**Solutions and examples**

- Requirements and features
  - API or website
  - Recurring payments
  - Integration with existing applications
- Costs
  - Setup costs
  - Transaction fees
  - Support

**Selecting a provider**

- Level 1 PCI-DSS compliant
- Integrates with student and financials systems
- E-Commerce module has 3 modes
  - Storefront – [Testing Center](#)
  - Checkout – [Admissions](#)
  - Gateway – [Continuing Education](#)

**Cashnet at K-State**

- What are you doing to secure payments now?
- What problems have you had?
- What is your biggest concern?
- Anything else?

## Discussion

- <https://www.pcisecuritystandards.org>
- Dennis Reedy, Walter Conway. Cards at School. *AFP Exchange*, March 2007
- [USF / FAU PCI Training Guide, April 2008](#)
- [VISA risk Management](#)
- Bob Gentile, David King. 2007 CACUBO presentation: [“PCI Compliance/The Gateway to Paradise”](#)

**Sources and more information**