Risk Management and Compliance: Addressing Uncertainty with Integrity

Virgil Lloyd, Regional VP, Nelnet Campus Commerce
MCCBOA Summer Workshop 2018
Nelnet Campus Commerce

- Experienced
- Integrated
- Service Oriented
- Comprehensive
- Student Focused
Audience response

Web
PollEv.com/vlloyd722

Mobile
1) Text **VLLOYD722** to **22333** to join the session, then they text Choose custom keywords
2) Text a response
When you think of Risk Management and Compliance what words come to mind?
What is Risk Management?

The management and strategic process of assessment, identification, and prioritization of risks followed by a coordinated response to minimize, monitor, and control unfortunate events.
Risk Management in Higher Ed

Why it Matters

• Protecting the data of 20.4 million students (NCES, 2017)

• Multiple points of entry

• Increased scrutiny by the banks

• Staying out of the news
Who’s data is HE protecting?

- Students
- Families
- Authorized Payers
- Authorized Parties
- CC employees
Which company or institution has been compromised with a data breach?

- Target
- Yale University
- Anthem
- University of California, Berkely
- All of the above
In the news

World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated 23rd Mar 2018)
Best Practices
To avoid a data breach

- NEVER email CC info or process payments received by email
- NEVER store CC numbers in any database or spreadsheet
- Mask all but first 6 or last 4 digits
- Keep CC documentation locked in a safe and secure filing cabinet
- Oversight of the “need-to-know” players
- Don’t allow unauthorized persons access to areas where data is stored
- Destroy documentation when no longer needed
- Document departmental payment card handling procedures
What merchant level does higher education fall into?

Level 1
Level 2
Level 3
Level 4
Level 5
### Why is Risk in HE Growing?

#### Merchant Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Visa/MC Transactions/y</th>
<th>American Express Transactions/y</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>&gt; 6 million Visa/MC txns/yr</td>
<td>&gt; 2.5 million transactions/yr</td>
</tr>
<tr>
<td>2</td>
<td>1 to 6 million Visa/MC txns/yr</td>
<td>50,000 to 2.5 million txns/yr</td>
</tr>
<tr>
<td>3</td>
<td>20,000 to 1 million Visa/MC ecommerce txns/yr</td>
<td>All other Amex Merchants</td>
</tr>
<tr>
<td>4</td>
<td>All other Visa/MC merchants</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- **Level 1**: High risk, high volume businesses.
- **Level 2**: Medium risk, moderate volume businesses.
- **Level 3**: Low risk, low volume businesses, predominantly online.
- **Level 4**: All other merchants not fitting into the above categories.
# Merchant Levels and Validation

<table>
<thead>
<tr>
<th>Level</th>
<th>Visa</th>
<th>MasterCard</th>
<th>Discover</th>
<th>American Express</th>
</tr>
</thead>
</table>
| 1     | • Annual on-site assessment (QSA)  
      | • Quarterly network scan (ASV)     | • Annual on-site assessment (QSA)  
      |                                  | • Quarterly network scan (ASV)     |
| 2     | • Annual on-site assessment (QSA/ISA)  
      | • Quarterly network scan (ASV)     | • Quarterly network scan (ASV)     |
| 3     | • Annual Self-Assessment Questionnaire (SAQ)  
      | • Quarterly network scan (ASV)     | • Quarterly network scan (ASV)     |
| 4     | • At discretion of acquirer  
      | • Annual SAQ  
      | • Quarterly network scan (ASV)     | • N/A                            |
Which generation is most at risk and susceptible to cyber attacks?

- Millennials
- Gen X
- Baby Boomers
- Gen Z
- All equally susceptible
Millennial Generation
A phishing email is when cyber criminals use emails as "bait" to fish for information.
Phishing scams

- Messages contain a sense of urgency
- Look authentic
- “Verify your account information”
- Verify with a direct phone call
- Do not click on links
- Always report to IT department
Multiple Points of Entry
What Higher Ed looks like…
Also known as...
Compliance

We suffered a data breach but we were fully validated as PCI compliant!

24/7/365 – it’s an ongoing process
- Not just a yearly assessment
- Assessment measure a snapshot in time

PCI compliance is business as usual everyday
- 130+ criteria must be met
Who is HE accountable to?

- Federal Agencies
  - U.S. Department of Education (ED)
  - Federal Trade Commission (FTC)
  - Consumer Financial Protection Bureau (CFPB)

- State Agencies

- Private/Trade Associations

- Credit card associations
Rules and Regulations in HE

• PCI-DSS and PA-DSS
• Family Educational Rights to Privacy Act (FERPA)
• Telephone Consumer Protection Act (TCPA)
• Gramm/Leach/Bliley Act (GLBA)
• Truth-in-Lending Act (TILA)
• Fair Credit Reporting Act (FCRA)
• Title IV Cash Management regulations
• State-based service charge limitations
What has Nelnet learned?

How do we respond?

Team of 30+ security professionals
  • Partnership with CampusGuard

Security Response Plan
  • Determine and identify incident
  • Containment
  • Eradication
  • Recover
  • Lessons learned

Client communication—3 T’s
  • Transparency
  • Timely response
  • Team coordination
Nelnet Campus Commerce
Your trusted partner

- 25+ years in Higher Ed
- Fully PCI-DSS, FERPA, GLB, NACHA compliant
- P2PE with Bluefin Payment Systems
  - Reduces PCI scope
  - Seamless integration
  - Increased security
  - Simplifies compliance
- Ingenico ePayments
  - Remote, tents sale
Websites of interest

Millennials vs. Boomers cybersecurity:
http://www.uzado.com/blog/millennials-are-the-biggest-targets-for-cyber-attacks

This is also related and interesting:

“Krebs on Security”, easy reading that gives a lot of information on some of the latest security news.  https://krebsonsecurity.com/

DataBreach Today:  https://www.databreachtoday.com
Educause Cybersecurity:  https://library.educause.edu/topics/cybersecurity

World’s Biggest Data Breaches:
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Let’s connect

Virgil Lloyd
Regional Vice President
Midwest Region
773-656-2781
Virgil.Lloyd@Nelnet.net

Sandy Gjermstad
Customer Relations Manager
Midwest Region
224-623-2223
Sandy.Gjermstad@Nelnet.net