PCI DSS Compliance & Security Awareness Program at UST
# PCI DSS in a Nutshell

<table>
<thead>
<tr>
<th><strong>Who?</strong></th>
<th>Applicable to all UST employees that are exposed to any cardholder data while performing their job responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What?</strong></td>
<td>Regulations created by card associations for merchants to follow in order to minimize risk and maximize protection of cardholder data</td>
</tr>
<tr>
<td><strong>Where?</strong></td>
<td>Everywhere UST is handling (transmitting, storing, or processing) credit/debit card data</td>
</tr>
<tr>
<td><strong>When?</strong></td>
<td>Supposed to be compliant a few years ago the day before yesterday…</td>
</tr>
<tr>
<td><strong>Why?</strong></td>
<td>Criminals are sneaky. Anyway, it’s our duty to think critically, act wisely, and work skillfully to advance the common good…this qualifies!</td>
</tr>
</tbody>
</table>
Stephen Watt, 26, wrote a custom packet-sniffing program dubbed “blabla” - the code was used to siphon more than 100 million credit- and debit-card numbers from TJX’s corporate network. When he’s released from jail, he’ll have a $171.5 million restitution order waiting for him – to repay financial losses claimed by TJX in the hack attack.

Albert Gonzalez is a computer hacker and convicted criminal for masterminding the combined credit card theft and subsequent reselling of more than 170 million card and ATM numbers from TJ Maxx, Dave and Busters, and Heartland.
Higher Ed Is In The Crosshairs

Data Security Challenges in HE

- Commitment to open networks
- Payment processes spread over large geographical areas/multiple campuses
- Multiple merchants on one campus
- Multiple third-party systems for merchant transactions
- House data such as names, social security numbers, addresses, phone, etc...

Taking into consideration that:

- There are vastly fewer education institutions than there are businesses (over 14 million) in the U.S.
- The share of total payment card transactions processed in the U.S. attributable to Higher Ed is relatively small

Conclusion - Higher Ed has a disproportionately high percentage of data security incidents...it’s not a matter of “if”, but rather “when.”
Categorizing Incidents

• **Security breach** – an incident where an attacker is able to circumvent the security of a system but does not imply a violation of the data

• **Data compromise** – an incident where an attacker breaches a security system and gains access to data

• **Exposed data** – Halfway between a breach and a compromise, when a known breach has occurred, but uncertain when and what data may have been compromised

For example - You arrive home from work and find your front door broken down (breach). After entering your home, you realize your computer is gone (compromised). You keep track of your finances on that computer without any password protection (exposed data).
The Dangers of Noncompliance with PCI DSS

- Compromised data negatively affects customers, merchants, and financial institutions
- **Just one incident can severely damage the reputation of UST**
- Fines of up to $500,000 per card association per incident
- Additional related expenses of a breach:
  - Forensic investigation fees
  - Lawsuits
  - Insurance claims
  - Cancelled accounts
  - Government fines
  - Replacement cards
  - Credit monitoring fees
  - Reimbursement of losses
- Immediate level 1 merchant status and corresponding security measures (UST is currently level 4; level 1 is much more costly and burdensome to maintain)
- Lose the ability all together to accept payment cards
Alphabet Soup

Before delving too much farther into the wondrous world of PCI DSS compliance, note the following acronyms and what they stand for:

✓ PCI DSS – Payment Card Industry Data Security Standards
✓ PCI SSC – Payment Card Industry Security Standards Council
✓ PA-DSS – Payment Application Data Security Standards
✓ QSA – Qualified Security Assessor
✓ ASV – Approved Scanning Vendor
✓ SAQ – Self Assessment Questionnaire
✓ ROC – Report On Compliance
✓ CHD – Cardholder Data
✓ CDE – Cardholder Data Environment
✓ PAN – Primary Account Number
PCI Players

PCI SSC

ASV/QSA (“auditors”)
Approved Scanning Vendor/
Qualified Security Assessor

Card Associations

Acquiring Bank

Merchant
PCI Players

PCI Security Standards Council

- aka the “Council” – was founded in 2006 by the five major Card Associations (Visa, MasterCard, Discover, American Express, and JCB) in an effort to standardize regulatory compliance requirements for payment card processing
- The 12 fruits of their labor are the PCI DSS
PCI Players

Merchant

• Point of initiation for a payment card transaction
• Accepts payment cards (debit/credit) via one of several acceptance channels (card present/card not present)
• Subject to PCI DSS if process, store, or transmit sensitive cardholder data

• You! (As an agent of St. Thomas)
PCI Players

Approved Scanning Vendor (ASV)
• Organizations approved by the PCI SSC to perform quarterly Internet vulnerability scans as required by PCI DSS 11.2

Qualified Security Assessor (QSA)
• A company and employed individual that is trained and approved by the PCI SSC to perform PCI compliance assessments
PCI Players

Acquiring Bank

• aka the “merchant bank” – the organization that sponsors the merchant to the card associations and enables the merchant to accept payment cards via the use of a merchant ID

• Majority of PCI DSS enforcement is accomplished through fines, fees, and other requirements issued by the acquiring bank to the merchant
PCI DSS Compliance vs. Validation

Compliance – state of being
• 24/7/365
• Continual maintenance of baseline security requirements
• Merchants must be compliant with PCI DSS requirements at ALL times

Validation – point in time
• Periodic
• Annual or quarterly verification of compliance with PCI DSS
• Even if compliance is validated at some point during the year it does not mean UST is safe from attack
Merchant Categorization

PCI DSS compliance validation standards may vary for merchants depending upon the volume of transactions processed and the acceptance channels used to process them. Merchants are segregated into levels (1 – 4) by their acquiring bank. Level 1 has the most stringent validation requirements, while level 4 allows for more self-reporting.

*Generally speaking, UST merchants are level 4.*
The Self Assessment Questionnaire (SAQ) is a report completed by the merchant to assist with validating their PCI DSS compliance. There are several versions of the SAQ; selection of the appropriate SAQ is based upon payment acceptance methods.
## PCI DSS – The Digital Dozen

| 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 data  
4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | 5. Use and regularly update anti-virus software  
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 |
UST Compliance

PCI Group
• Representatives from IRT and Finance have been working on PCI DSS compliance for years
• Much effort has been expended toward creating a “PCI Island” - segmenting connected systems to keep them out of the PCI scope
• Created campus wide policy regarding payment card processing
• Updated Web Apps to bring them into compliance
• Responsible for developing and maintaining PCI DSS compliance program
Things You Must Do To Help Maintain Compliance

• Never store, process, or transmit card data outside of the approved systems
• Never transmit payment card data via email, text, IM, etc...
• Do not use Wi-Fi for processing payment cards
• Contact the Business Office if you have any questions/concerns about payment card processing
Things You Must Do To Help Maintain Compliance

• Limit access to and lock down machines used to process payment card transactions
• Use only PA-DSS certified vendors (Put it in the contract!)
• Adhere to all UST payment card and data security policies
• Contact the Business Office if you have any questions/concerns about payment card processing
Things You Must Do To Help Maintain Compliance

• Shred any paper with payment card data immediately after processing using a cross-cut shredder

• Contact the Business Office if you have any questions/concerns about payment card processing
For more information...

Visit the following websites to learn more about PCI DSS and related issues:

- https://www.pcisecuritystandards.org/
- http://www.adamdodge.com/esi/
- http://www.treasuryinstitute.org/pages/PCI%7B47%7DSS-Information.html
- http://www.youtube.com/watch?v=OceYWri86Ts