



 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

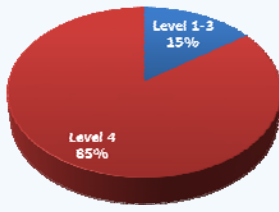
PCI , Security, and You....

Mike Petitti
 – Chief Marketing Officer Trustwave
Ken Musante
 – President, Humbolt Merchant Services
Victoria Strayer
 – Senior Director, TSYS Enterprise Business Compliance


 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

Merchant Level


While larger merchants represent greater transaction volume, smaller merchants have greater risk due to many factors discussed in this presentation.



Merchant Level	Percentage
Level 1-3	15%
Level 4	85%

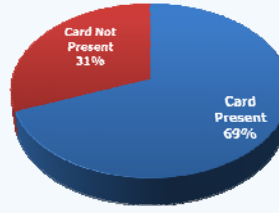
Trustwave's analysis is derived from more than 350 cardholder data compromise investigations performed in over 14 different countries.

2


 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

Acceptance Type

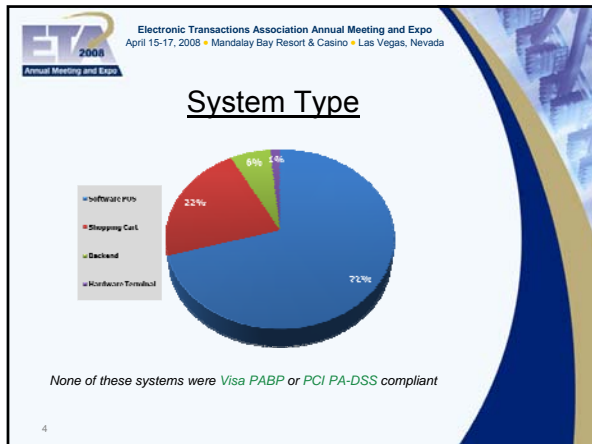
In contrast to common knowledge, Card Present merchants are 3 times as likely to be compromised than Card Not Present merchants.

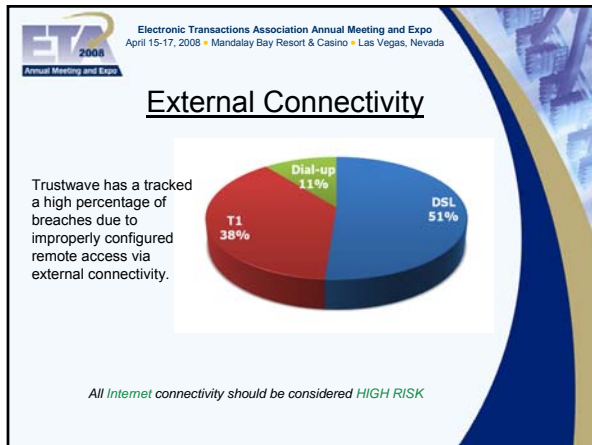


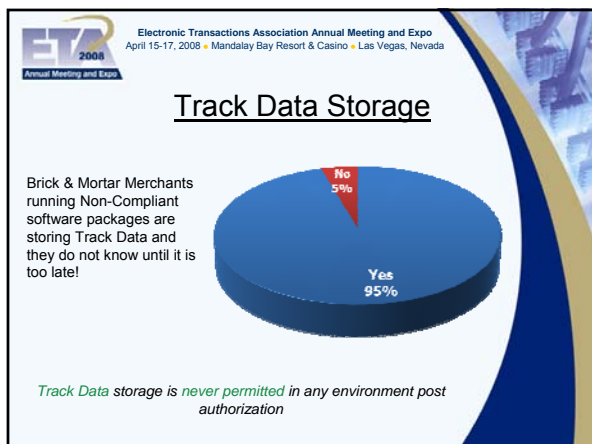
Acceptance Type	Percentage
Card Not Present	31%
Card Present	69%

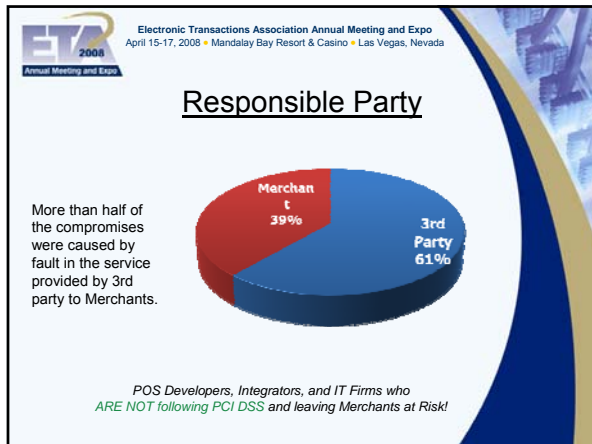
Consumer are more likely to have your credit card stolen making a face-to-face transaction, than when shopping online.

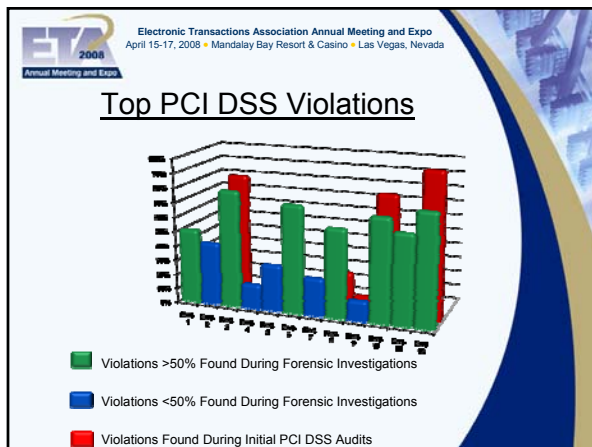
3












- ETA 2008
Annual Meeting and Expo
- Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada
- ## PCI DSS & Small Merchants
- **Lack of awareness of PCI DSS!**
- "I have never heard of PCI"
 - **No resources to attain and manage compliance**
- "I do not have people to handle this"
- "Time away from my [operations] costs me money"
 - **Most don't believe they are at risk**
- "[Data breach] happens to the bigger merchants"
- "I have been using the same equipment for years"
 - **Those who do know don't believe they need to act**
- "My payment processor is PCI compliant"
- "I can't pay for this service"



Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

Payment Security Standards Understand, Embrace, Integrate

Victoria Strayer – Senior Director, TSYS Enterprise Business Compliance



Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

- Does PCI Apply to Me?
- The Many Flavors....and some review
- Know Your Processing Partners
- Integrate Your Security Approach
- There is a "Value Add"
- Who Can Help?



Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

Does PCI Apply to Me?

⇒ Yes, the PCI Security Standards apply to you and your merchants!

⇒ Your entire processing lifecycle must be PCI compliant

- Your own tools that process or store sensitive data
- ALL aggregators and payment gateways along the path that process or store sensitive data
- Your processor and their products and services that store sensitive data
- Downstream tools that support back-office processes such as risk management, etc. if they store sensitive data

ETA 2008 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada
 Annual Meeting and Expo

The Many Flavors.....

⇒ **PCI-SSC**

- Owns and Manages PCI Data Security Standards and related documents
- Provides interpretations of the standards
- Defines the common audit requirements to validate compliance
- Manages the certification processes for security assessors (QSA) and scanning vendors (ASV)

⇒ **PCI-DSS**

- Applies to any entity's internal hardware and/or software systems that store, process, or transmit cardholder data
- Internally-developed payment applications (not sold to outside entities) **do not have to comply with PA-DSS; however, are required to comply with PCI data security standards**

ETA 2008 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada
 Annual Meeting and Expo

A little Bit More....

⇒ **PA-DSS**

- **Payment Application-DSS** applies to payment applications that store, process or transmit sensitive data (typically vendor created)
- Designed as guidance so software vendors will not develop payment apps which prevent compliance with PCI data security standards
- Using PA-DSS software does not, by itself, ensure an entity will comply with PCI-DSS
- Ensure vendors provide products that support PCI DSS compliance
- Minimize vulnerabilities caused by insecure payment applications
- Eliminate storage of prohibited data (CVV, mag stripe data, etc.)
- PCI-DSS applications can be found at: www.visa.com/pabb

ETA 2008 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada
 Annual Meeting and Expo

What is a Merchant Level?

Visa Merchant Levels (effective 06/2006)

Merchant Level	Criteria	Required Actions
Level 1	Merchant processing over 6 million Visa transactions per year, regardless of channel.	Annual onsite audit and quarterly scans required.
Level 2	Merchant processing 1 to 6 million Visa transactions per year, regardless of channel.	Annual self-assessment and quarterly scans required.
Level 3	Merchant processing 20,000 to 1 million Visa eCommerce transactions per year.	Annual self-assessment and quarterly scans required.
Level 4	Merchant processing less than 20,000 eCommerce transactions and all other merchants processing up to 1 million Visa transactions per year.	Acquirer's discretion, but annual self-assessment and quarterly scans recommended.



Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

What is a Merchant Level?

MasterCard Merchant Levels (effective 05/2007)

Merchant Level	Criteria	Required Actions
Level 1	Merchant processing over 6 million MasterCard transactions per year, regardless of channel.	Annual onsite audit and quarterly scans required.
Level 2	Merchant processing 1 to 6 million MasterCard transactions per year, regardless of channel.	Annual self-assessment and quarterly scans required.
Level 3	Merchant processing more than 20,000 eCommerce transactions but less than 1 million total MasterCard transactions per year.	Annual self-assessment and quarterly scans required.
Level 4	Merchant processing less than 20,000 eCommerce transactions and all other merchants processing up to 1 million MasterCard transactions per year.	Acquirer's discretion.



Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

PABP Important Dates


Phase	Visa PABP Mandate	Date
I	Newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (VNPs) and agents must not certify new payment applications to their platforms that are known vulnerable payment applications	January 1, 2008
II	VNPs and agents must only certify new payment applications to their platforms that are PABP-compliant	July 1, 2008
III	Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or use PABP-compliant applications	October 1, 2008
IV	VNPs and agents must decertify all vulnerable payment applications	October 1, 2009
V	Members must ensure their merchants, VNPs and agents use only PABP-compliant applications	July 1, 2010



Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


Know Your Processing Partners

- Validate PCI compliance on the Visa website
 - www.visa.com/cisp
- Periodically review the PCI Standards website
 - www.pcisecuritystandards.org
- Register your third party providers following guidelines established by the card brands and your financial institution
- Incorporate PCI compliance status into your due diligence process for new partners/service providers and include in your sales cycle for new merchants


 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

Integrate your Security Approach

- ⇒ Include PCI as an integral component of your Security program; not a separate work stream
- ⇒ Consider incorporating the Self-Assessment Questionnaire within your merchant boarding or merchant servicing processes
- ⇒ Educate your staff on the “value add” of these programs


 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


Yes...There is a “Value Add”

- ⇒ **Take Control**
Develop your own PCI strategy and this will save you time, money, and avoid the “firedrill”
- ⇒ **Stay informed**
Know the status of your processing lifecycle and periodically validate
Know what changes may be coming – Be Proactive
- ⇒ **Know what to do**
Have a policy that outlines what to do if one of your merchants reports a breach...Put the right people on the job
- ⇒ **Results**
A well managed program that can be used as a market differentiator and selling point...one that has you in control


 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


Who Can Help?

- ⇒ Stakeholders in the Payments industry
 - PCI-SSC, Card Brands, special focus groups
- ⇒ Your BIN sponsor
 - Provides you information, guidance, Industry representation
 - May also provide you programs and tools to aide in working with your merchant
- ⇒ Your processor
 - Compliant platform and Industry representation
- ⇒ The vendors who develop your payment applications
 - Following PA-DSS


 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

**However, accountability for your portfolio is YOURS....
 Embrace it and you will be more successful**


- ↳ Ask Questions
- ↳ Evaluate your portfolio, integrate your security approach...and take action
- ↳ Engage with an ASV (Authorized Scanning Vendor) and a QSA (Qualified Security Assessor), if applicable
- ↳ Avoid Financial Loss *and* Reputational Damage
 - Educate your sales team on incidents in the news and ensure your sales staff has a common response to questions!
- ↳ Get Involved



 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

**SELLING
 PCI
 COMPLIANCE**


April 16, 2008

Presented by
 Ken Musante, President





 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

- I. Motivate
- II. Introduce
- III. Educate
- IV. Close

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


MOTIVATE

- Carry articles from local and national publications regarding data breaches
 - ▶ National stories to draw attention
 - ▶ Local stories to personalize

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

MOTIVATE

- Provide anecdotal stories regarding:
 - ▶ Employee theft
 - ▶ Carelessly installed wireless networks
 - ▶ Accidentally discarded material

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

MOTIVATE

- Explain difference between hacks of online merchants vs. retail merchants
 - ▶ IPOS or LAN
 - ▶ Hacker techniques and methods for committing fraud once sensitive data is obtained

ETA 2008
Annual Meeting and Expo

Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

MOTIVATE

- Estimate expense of a breach
 - ▶ Association fines
 - ▶ Loss of customer confidence and business
 - ▶ Notification requirement and cost
 - ▶ Possible required forensic analysis
 - ▶ Possible lawsuit
 - ▶ Time

ETA 2008
Annual Meeting and Expo

Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

INTRODUCE


- PCI for Dummies

ETA 2008
Annual Meeting and Expo

Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


INTRODUCE

- Just focus on the rules for the particular channel of merchants you are presenting to


 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


INTRODUCE

- SAQ A / Validation Type 1
- 11 questions
- Merchant Type:
 - ▶ Accepts card-not-present transactions only
 - ▶ Outsources all functions involving cardholder data to a PCI-DSS compliant service provider
 - ▶ No electronic storage of cardholder data


 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


INTRODUCE

- SAQ B / Validation Level 2
- 21 questions
- Merchant Type:
 - ▶ Accepts transactions through an imprint machine only
 - ▶ Does not transmit data over a phone line or the Internet
 - ▶ No electronic storage of cardholder data


 Electronic Transactions Association Annual Meeting and Expo
 April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


INTRODUCE

- SAQ B / Validation Level 3
- 21 questions
- Merchant Type:
 - ▶ Accepts transactions using a stand-alone, dial-out terminal connected to a phone line only
 - ▶ No electronic storage of cardholder data

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

INTRODUCE

- SAQ C / Validation Level 4
- 38 questions
- Merchant Type:
 - ▶ Payment application is connected directly to the Internet
 - ▶ No WAN or LAN configuration
 - ▶ No electronic storage of cardholder data
 - ▶ Payment application vendor may provide remote support, but only in compliance with best practices

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


INTRODUCE

- SAQ D / Validation Level 5
- 226 questions
- Merchant Type:
 - ▶ Does not fit into any of the previous categories

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

INTRODUCE

- Explain that stored data must be secured
 - ▶ Hard copies
 - ▶ Online files
 - ▶ Temporary files

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


EDUCATE

- Provide one set of guidelines in a useable instrument
 - ▶ Bring printouts of the self-assessment questionnaire and attestation statement

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

EDUCATE

- Explain ways in which data can be compromised:
 - ▶ Hard copies
 - ▶ Employees
 - ▶ Data intrusion
 - ▶ Accidentally
- Share the perspective of the merchant's customers

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


EDUCATE

- Explain "validation" vs. "compliance"

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


EDUCATE

- Explain prohibited data
 - ▶ CVV2/CVC2/CID
 - ▶ Mag stripe data

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


EDUCATE

- Explain that 80% of compromised merchants are within Level 4
 - ▶ Evenly split between card-present and card-not-present merchants
 - ▶ Restaurants, universities, and retailers are targets

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

CLOSE

- Explain costs of compliance vs. costs of a compromise

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada


CLOSE

- Liken cost to insurance

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

CLOSE

- Integrate solution into process

 Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

CLOSE


- Provide alternatives to storing data
 - ▶ Use PCI-compliant service providers to handle critical data

ETA
2008
Annual Meeting and Expo

Electronic Transactions Association Annual Meeting and Expo
April 15-17, 2008 • Mandalay Bay Resort & Casino • Las Vegas, Nevada

QUESTIONS?

Ken Musante, President



707.269.3200
kmusante@hbms.com
