Don’t be tomorrow’s headline: Protect and secure customer payment information

Jonathan Stout
Vice President
eReceivables Consultant

May 2014

Poll question: Are you familiar with PCI (Payment Card Industry)?

A) Yes

B) No

Agenda

- What is PCI-DSS & PA-DSS?
- Common causes of data breaches
- Tactics to help mitigate these risks
- Best practices for retail and card not present
- Q&A

What is PCI-DSS?

- **P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandards
- Industry tools and measurements to ensure the safe handling of sensitive information
- Applies to all merchants and third party service providers

What is PA-DSS?

- **P**ayment **A**pplication **D**ata **S**ecurity **S**tandard
- Applies to all vendors that develop payment applications and gateways

When does PCI & PA-DSS apply?

Processing

Storing

Transmitting

PCI DSS validation requirements

Compliance Classification Level	Annual submission of compliant PCI DSS Report on Compliance (ROC)	Annual submission of compliant Self Assessment Questionnaire (SAQ)	Quarterly Network Scan
Level 1 >6 MM annual transactions (Any payment network)	✓		✓
Level 2* 1 MM to 6 MM annual transactions (Any payment network) Merchant can do either ROC or SAQ	✓	✓	✓
Level 3 20K to 1 MM annual transactions (Any payment network) ecommerce only		✓	✓
Level 4 (recommended) < 20K e-commerce < 1MM annual transactions		✓	✓

*Level 2 merchant Self Assessment Questionnaire (SAQ) must be completed by an ISA (Internal Security Assessor)

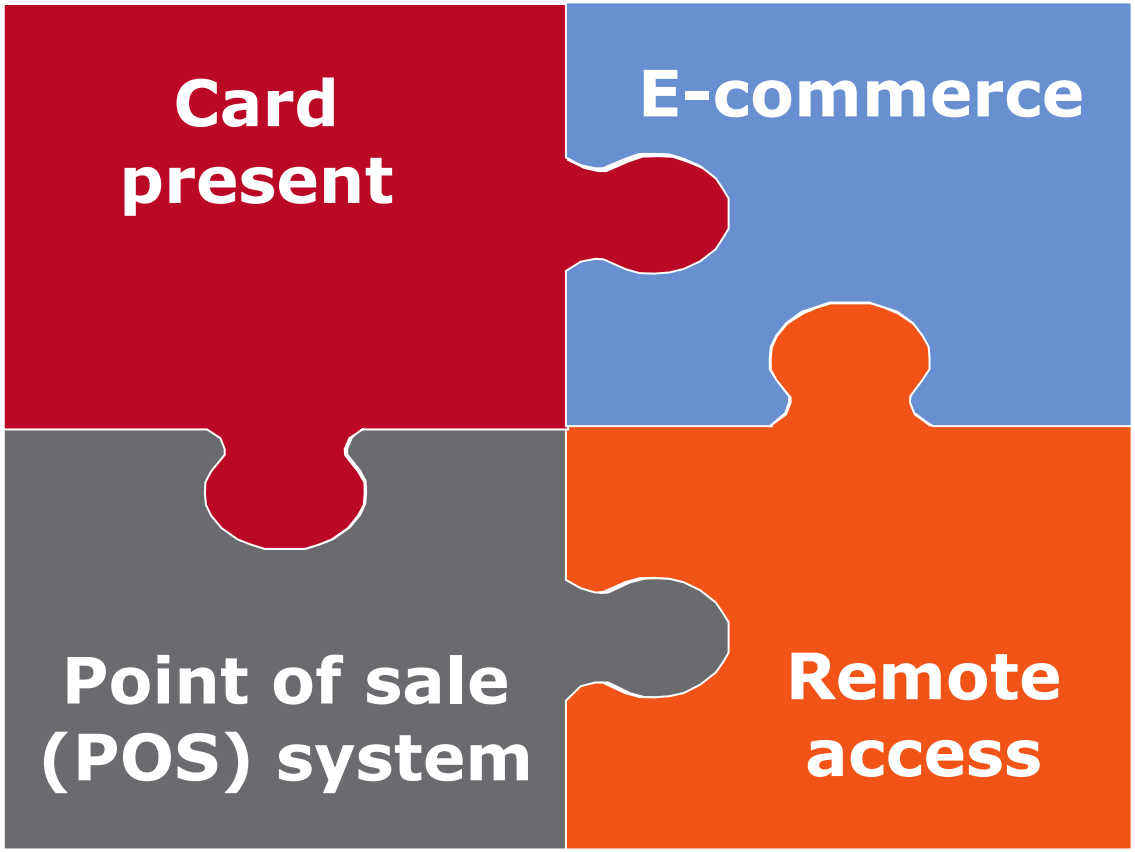
66% Breaches identified by external parties*

64% Breaches that go undetected for months*

63% Data breaches that involved a third Party responsible for system support*

*Verizon 2013 Data Breach investigations report

Tactics to minimize data breach risk



PCI: Validation versus compliance

Validation		Compliance
	Strategy	(BAU)
	Data security	
Reactive	Monitoring security controls	Proactive

Protective measures: Evolving requirements

- ✓ Monitor changes
- ✓ Monitor activities
- ✓ Test protection measures
- ✓ Rigorous penetration testing
- ✓ Staff responsibilities
- ✓ Work with your service providers

Goal is to protect your infrastructure

Poll question: How are most breaches identified?

A) By the merchant

B) By the customer

C) By the card processor

D) By the issuing bank

E) B,C,D

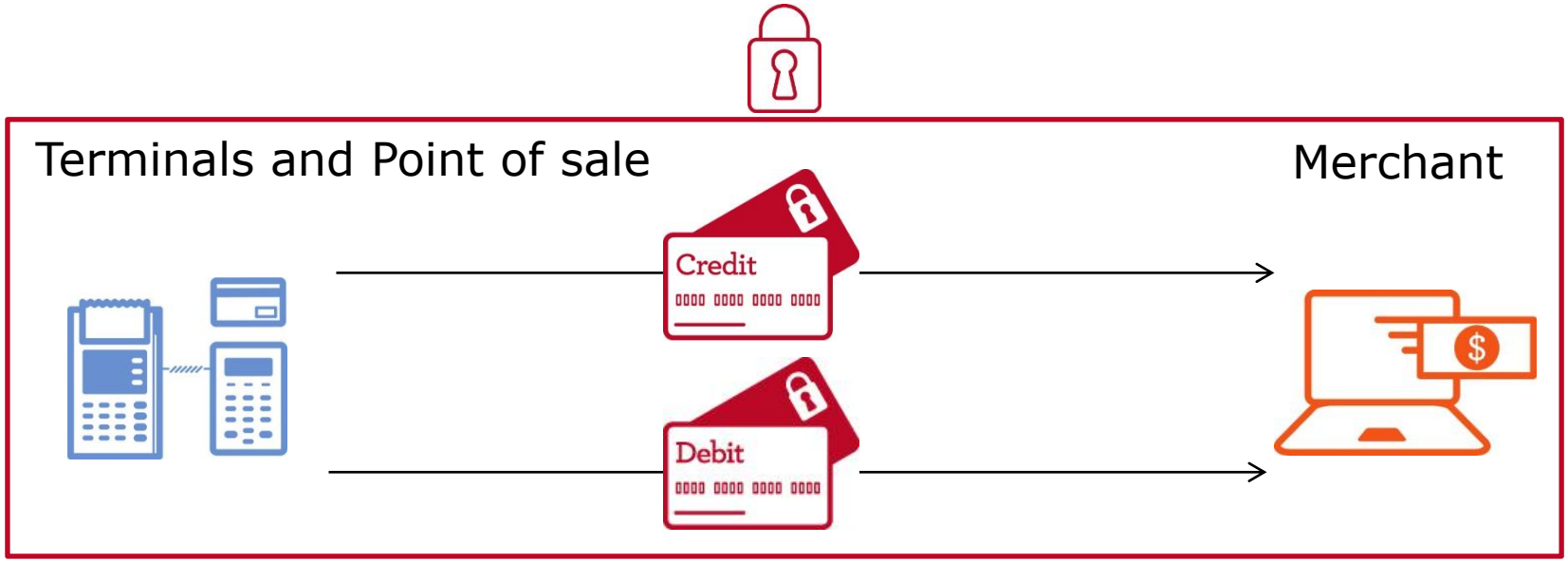
Answer: B,C,D

Best practices

End-to-end encryption

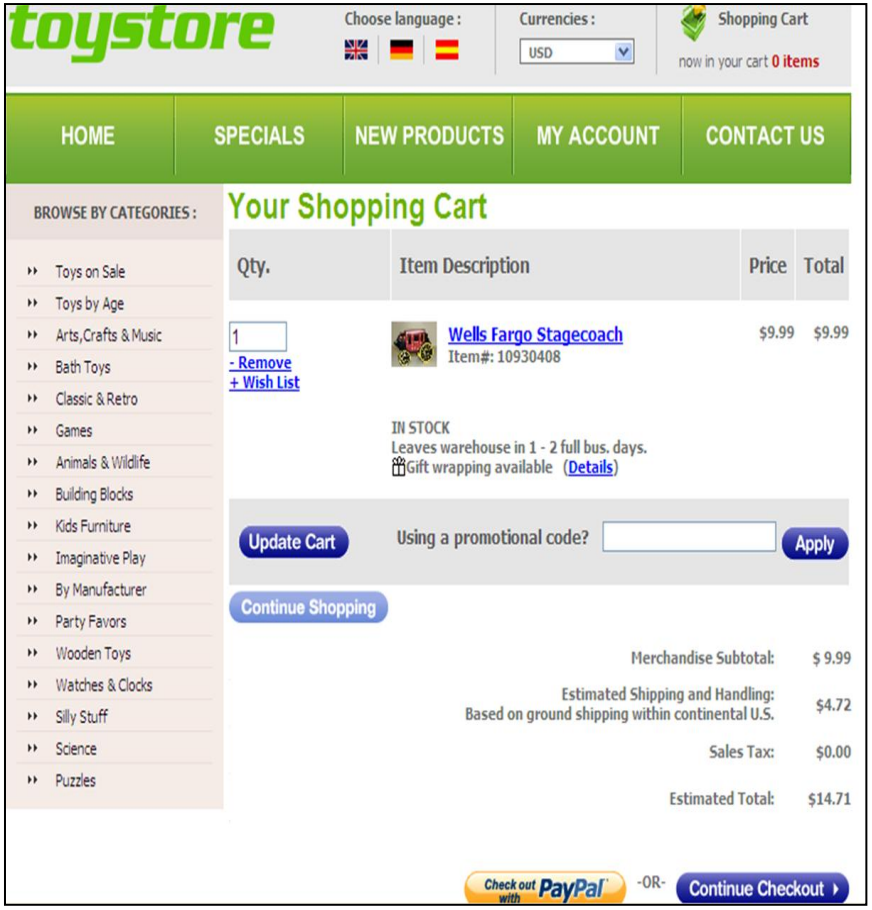
Card present transactions

- Includes tokenization



Tokenization

Card not present transactions



Card number:
3456 7890 1112 1314

Tokenized Number:
0176 2190 3475 1314

Poll question: The average cost of a data breach to an organization is $7.2 million?

A) True

B) False

Answer: True

* Network World March 8, 2011 news article

Poll question: Do you know if your company is PCI Compliant today?

A) Yes

B) No

"PCI is an industry-enforced regulation but it might as well be in the law. You can't do business without it."

- *Brian Krebs*
  Journalist

Questions?

Thank You!