Company Overview

PRIORITY PAYMENTS EAST COAST®

- ✓ Incorporated May 2005, Alpharetta, GA
- ✓ Servicing 42,000 merchants/1,500 boarded monthly
- ✓ Dedicated staff of 280 employees supporting multiple divisions
- ✓ Top 40 processor in US
- ✓ Approx. $9.2 billion annual bankcard volume
- ✓ Priority supports over 1,000 financial institution locations
- ✓ Winner of the 2013 Electronic Transaction Association ISO of the year Award

PCI-DSS

PRIORITY
PAYMENTS EAST COAST®

Did You Know…

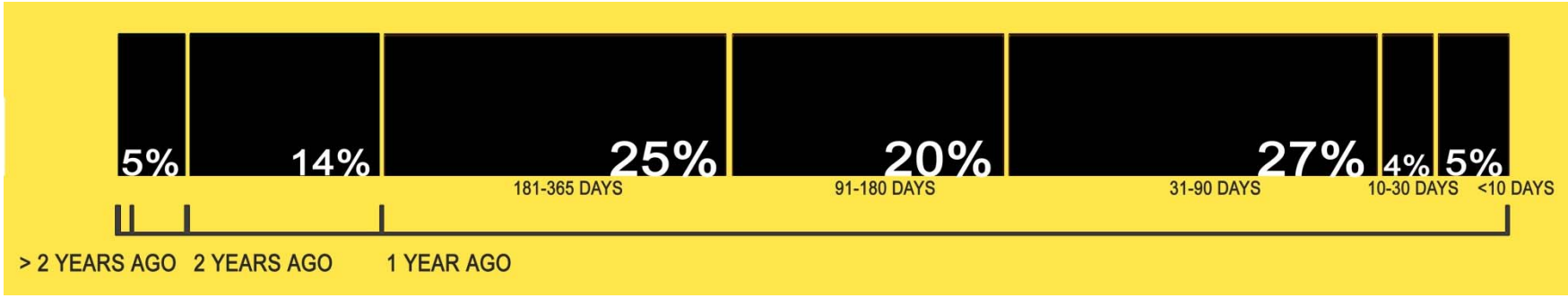
PRIORITY PAYMENTS EAST COAST®

The **primary targets** of cybercriminals in 2012 were **Retail** (45%), **Food & Beverage** (24%) and **Hospitality** (9%).

Operators that go through a breach will pay roughly **$25,000 to $250,000** depending on the amount of credit cards that were potentially stolen

Expect that **20%** of the customers affected by the breach **will not return** to your business

Timeline: Intrusion to Containment



Source: Trustwave 2013 Global Security Report

But first, the facts…

How did we get here?

PRIORITY PAYMENTS EAST COAST®

Attacker Targets

- Level 1 Merchants (larger merchants processing over 6 millions Visa transactions annually) have become "hardened targets"
- Independent merchants have become a favorite target for cybercriminals. There credit velocity is relatively high, security measures are relatively low

Attacker Methods

- Old approach was to go after unencrypted, archived data (pre-CISP software)
- Payment Applications (POS) have since been required to update their software to encrypt all credit card data
- Attackers are now using "in-line" intercept techniques to collect card data
- This method attacks the memory (memory scraping) of a PC and records sensitive data before it has a chance of being encrypted
- They are now being used against single-location businesses
- This method is effective against all POS applications, including PA-DSS validated ones

Attacker Intrusion Enablers

- Over-reliance on anti-malware – 60%+ of crimeware is invisible to AV applications
- Misunderstanding that computer security is the responsibility of the POS vendor
- Insecure remote access applications – pcAnywhere, VNC, RDP, etc.
- Soft or no perimeter – no hardware firewall or weak, unmanaged firewall
- No log monitoring – customer has no visibility to suspicious patterns

Protect Your Network

The Dangers of Malware and Crimeware

PRIORITY PAYMENTS EAST COAST®

MALWARE

Software which has a perceived intent to harm a network or system without the knowledge of that system's operator.

.

CRIMEWARE

A type of Software that through forensic audits, has been determined by Card Brands to have aided past cybercrimes.

Security vs. Compliance

PRIORITY PAYMENTS EAST COAST®

Compliance is mandatory, but achieving PCI Compliance does not ensure you are safe from a security compromise.

DAY 1 you may be compliant, but by DAY 2, changes to configurations, or not maintaining systems could result in No longer being compliant.

Security is implementing a strategy that results in lessened risk, and adapts to security weaknesses on an everyday basis.

Compliance
Satisfying regulation

Security
Preventing an incident from happening

PCI Data Security Standard

High Level Overview

PRIORITY PAYMENTS EAST COAST®

An Outline for Over 200 Requirements to meet Compliant Standards for PCI-DSS.

Build and Maintain a Secure Network	**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data
	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**Requirement 3:** Protect stored cardholder data
	Requirement 4: Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**Requirement 5:** Use and regularly update anti-virus software
	Requirement 6: Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**Requirement 7:** Restrict access to cardholder data by business need-to-know
	Requirement 8: Assign a unique ID to each person with computer access
	Requirement 9: Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**Requirement 10:** Track and monitor all access to network resources and cardholder data
	Requirement 11: Regularly test security systems and processes
Maintain an Information Security Policy	**Requirement 12:** Maintain a policy that addresses information security

How to Keep Your System Safe

What you can do today

PRIORITY PAYMENTS EAST COAST®

- **Use strong passwords** for your Windows and POS login, and be sure to change them often.
  - At least eight characters long.
  - Does not contain your user name, real name, or company name.
  - Does not contain a complete dictionary word.
  - Is significantly different from previous passwords. Passwords that change just slightly—such as Password1, Password2, Password3—are not strong.
  - Contains characters from each of the following groups:
    - Uppercase and/or lowercase letters.
    - Numbeers
    - Symbols (!,@,#,$,%, etc.)
- **Use password protection on your screensaver**. Sometimes you're away from your desk for longer than you unexpected. Plan for those situations by setting up your computer so that it locks itself after a specified amount of time.
- **Install and maintain** antivirus on ALL of your machines. Always be sure to keep your antivirus definitions up-to-date.
- **Keep your Windows, Adobe, and Java up to date**. Cybercriminals have found holes in these systems which are constantly being patched by the vendors.
- **NEVER keep remote access tools running on your machine**. This has become a favorite form of access for criminals. Be sure that vendors walk you through disabling remote access anytime their support session has ended or when your accountant is done accessing reports.
- **Segment your networks and end all internet surfing on your POS network**. It is wise to invest in a network specialist to segment your POS network from your personal network. By installing a commercial grade firewall, you can also block any and all incoming communication.
- **Train your staff**. Hold annual meetings to go over keeping data safe.
  - No Internet surfing
  - No writing down customer credit card numbers
  - Keep the office door locked when not in use
  - No checking emails and downloading questionable documents

Along with the above ideas, it is also important to complete the Self-Assessment Questionnaire (SAQ) on an annual basis. Doing so will not only keep you compliant, it will also help you avoid fees set forth by the PCI-SSC's five founding global payment brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.).

Thank You

PRIORITY PAYMENTS EAST COAST®

Thank you for your time.

Questions?

Please ask us for a complete printout of the PCI-DSS

Gary Liu
1-877-515-VISA (8472) Option #1
gliu@prioritypaymentsec.com