National Cyber Security Awareness Month

NFIB The Voice of Small Business.

VISA

Secure Commerce:
Data Security Essentials Every Small Business Should Know

November 16, 2012

Disclaimer

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Agenda

- Global Compromise Trends
- Common Network Vulnerabilities
- What To Do If Compromised
- Data Security Best Practices
- Visa's Authentication Vision
- Reducing The Battlefield

National Cyber Security Awareness Month

NFIB The Voice of Small Business.

VISA

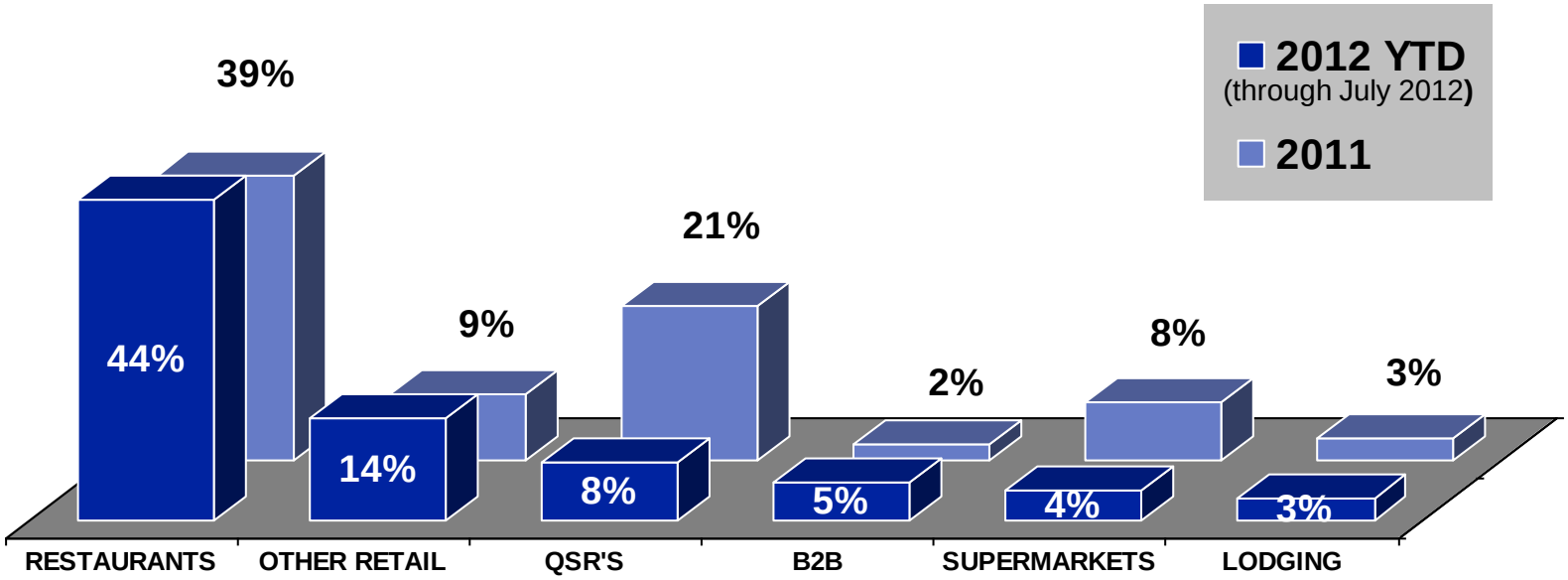
Global Compromise Trends

Justina Jow
Senior Investigator

Visa Inc. CAMS Compromise Events: Top Market Segment* (MCC)

NFIB The Voice of Small Business. VISA

Restaurant merchants and franchises continue to be targeted



*** Market Segment based on Acceptance Solutions MCC "Market Segment" category**

Source: Compromised Account Management System (CAMS) – Original "IC" and "PA" Alerts

Data Breach Reporting

- Types of incidents Visa investigates:
  - Network intrusions
  - Skimming / PIN Entry Device (PED) tampering

- How Visa is notified:
  - Issuer notification through Common-Point-Purchase (CPP) analysis
  - Acquirer notification
  - Compromised entity notification (self-reported)
  - Visa internal analysis
  - Law Enforcement notification
  - Media reports

Common Network Security Deficiencies

- Remote access management
- Default usernames and common passwords
- Deficiencies introduced by third-parties hired to install and manage Point of Sale (POS) systems
  - It is up to the business owner to ensure the payment environment is secure
  - If using an outside vendor, take steps to ensure they have set up your systems properly and securely
- Firewalls are not properly configured

Indicators of a Compromise

- Customer complaints
- Law Enforcement
- Bank complaints
- Abnormal activity on Point of Sale (POS) system
  - Constant reboot on POS system
  - Unexpected pop-up windows

- "What To Do If Compromised" manual available on **www.visa.com/cisp**

Source: Visa's "What To Do If Compromised"

What To Do If Compromised

Requirements for Compromised Entities

- Merchants are responsible for notifying their bank if a compromise is suspected
- If you detect a suspected or confirmed breach, you must:
  - Immediately contain and limit the exposure
  - Preserve evidence and facilitate the investigation
  - Contact your merchant bank and provide documentation
  - If you do not know your merchant bank, contact US Fraud Control at (650) 432-2978 (option 4) or usfraudcontrol@visa.com
- Consider contacting law enforcement
- It is critical to work with your merchant bank and Visa to assist with containment

National Cyber Security Awareness Month

NFIB The Voice of Small Business.

VISA

Data Security Best Practices

Stanley Hui
Program Manager

PCI Data Security Standard

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

Source: PCI Security Standards Council

Cardholder Data Security:
Key Security Tips

Payment Application Data Security Standard (PA-DSS)

- Merchants must use secure payment applications that do not retain sensitive authentication data
- PA-DSS helps payment application vendors develop secure payment applications that support compliance with the PCI DSS

Network Security

- Insecure or vulnerable networks accessible via the Internet are prime candidates for attack
- To mitigate the risk of network intrusions entities should implement appropriate POS perimeter controls

Remote Management Application (RMA)

- Many small businesses use RMAs with their service providers to facilitate application / software upgrades, business downloads, or manage inventory
- Improperly configured RMAs create a potential attack vector for hackers leaving small businesses vulnerable to data compromise

Use Unique and Secure Passwords

- Change all vendor provided usernames and passwords
- Implement a strong password creation policy for all users for systems within the cardholder data environment

Data Security Communication and Training

- Employees can be the weakest link in an organization
- Establish data security policies and procedures and ensure that you provide training at least annually

Dealing with Third Party Agents or Vendors

- What data does your software automatically store?
- Does my network have a firewall installed to protect my Point-of-Sale system from unauthorized access?
- Can you confirm that you do not use common or default passwords for my system?
- Have all unnecessary and insecure services been removed from the systems and databases that are part of my system?
- Do you deliver updates via a secure method?

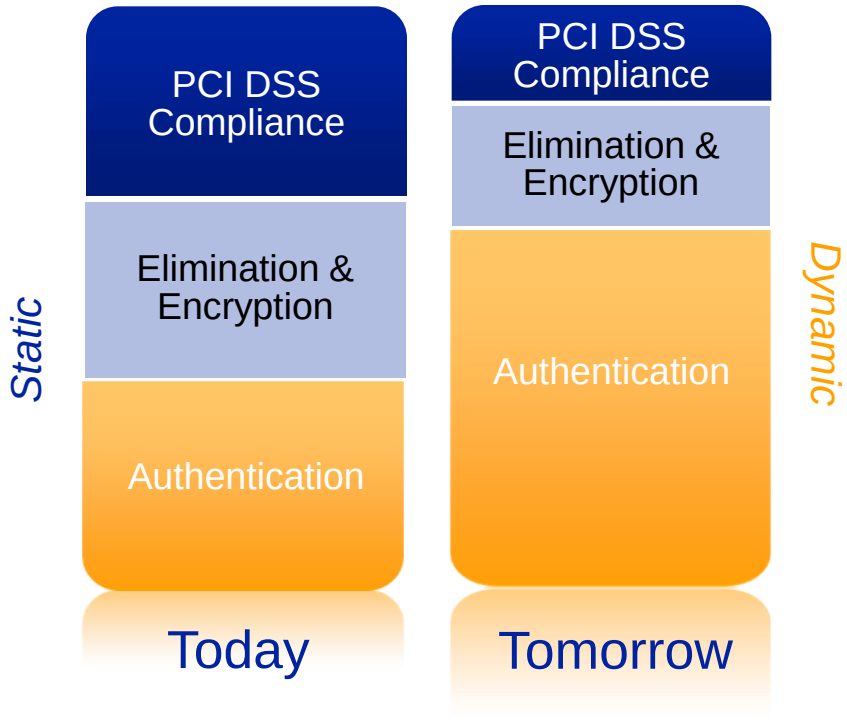
Merchant Actions to Protect Online Data

Merchants should consider the various options and associated risks when building an e-commerce business

- Lower risk
  - Fully managed hosted solution with a PCI DSS compliant service provider
- Medium risk
  - Multiple providers and custom-designed or “off the shelf” applications
- Higher risk
  - Card data is captured on merchant’s website

Visa Authentication Vision

Maintain trust in the Visa payments system by deploying dynamic data solutions across all markets and channels



Smart Network

1. Eliminate vulnerable data where possible
2. Maintain effective security where vulnerable data remains
3. Devalue transaction data by moving to dynamic data

"Dynamic" authentication methods, such as chip, contactless, mobile NFC, or one-time-passwords, utilize unique data elements and render stolen data useless

Visa's U.S. Chip Announcement

August 9, 2011

Laying the Groundwork for Dynamic Authentication in the U.S.

1	**Technology Innovation Program**	Starting October 2012, Visa will eliminate the need for eligible merchants to annually validate compliance with PCI DSS for any year in which > 75% of transactions originate from chip-enabled terminals
2	**Develop Chip Processing Infrastructure**	By April 2013 Visa will require processors to support acceptance of EMV chip transactions
3	**Establish Liability Shift**	By October 2015* acquirers/merchants who do not support dynamic data (chip) may be liable for counterfeit fraud

* 2017 for unattended gas pumps

Summary

Visa U.S. EMV roadmap provides three primary benefits

1. Build framework for mobile payments and future innovation leveraging EMV infrastructure for both contact and contactless payments
2. Support interoperability as EMV issuance and acceptance continues to grow worldwide
3. Reduce reliance on static cardholder data and incidence of counterfeit fraud

To accelerate adoption, Visa's recommended practices for chip implementation in the U.S. utilize only the essential chip functionality needed in an online infrastructure

Shrinking the Battlefield:
Reduce Value of Data to Thieves

- EMV dual-interface terminals (contact and contactless)
  - Dynamic authentication values
  - Future proof by preparing for mobile payments
- Point-to-Point Encryption
  - Protects against malware that sniffs data in transit
  - Simplifies merchant compliance by reducing the systems in the cardholder data environment
- Tokenization
  - Designed to work together with encryption to eliminate storage of cardholder data

Key Takeaways

- Don’t store any cardholder data that is not needed to run your business
- Use a PA-DSS compliant payment application
- Restrict the use of remote access to your systems
- Don’t use generic or default passwords
- Train employees on security basics
- Ensure that you only use service providers that validate compliance with PCI DSS

Resources

www.visa.com/cisp

- Data Security Alerts & Bulletins
- Best Practices
- Webinar Presentations
- Global Registry of Service Providers

www.pcisecuritystandards.org

- Data Security Standards (PCI DSS, PA-DSS, PCI PTS, P2PE)
- Validated Payment Applications
- Qualified Security Assessors, Approved Scan Vendors listings
- Merchant Resources