



Critical Data Security Errors That Payment Application Companies Should Avoid

6 October 2010



Agenda

- Card Data Compromise Trends
- Level 4 Merchant Compromises
- Compliant Applications Not Enough
- Visa Top 10 Best Practices
- Questions

Card Data Compromise Trends



Hackers continue shifting their attacks to more easily accessible and unprotected environments to steal card data

Security Measure

- Large merchants adopt PCI DSS compliance
- Merchants adopt PA-DSS compliant POS software
- Entities secure payment environment from attacks



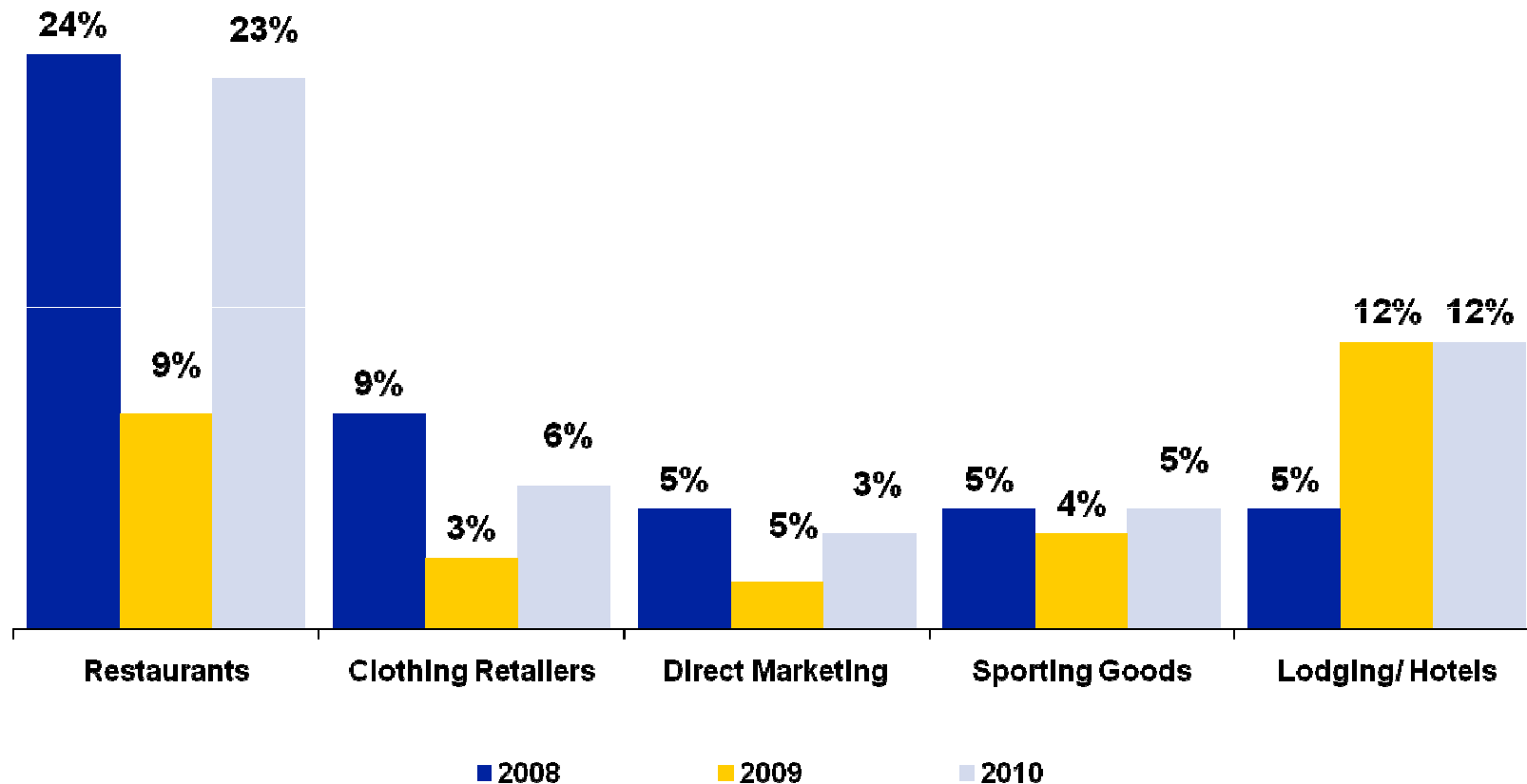
Compromise Trend

- Criminals target entities with unsecured payment environment
- Hackers utilize “sniffers” to steal cardholder data in transit
- Hackers attack corporate systems to gain access



TOP 5 MCC Growth – Global System Compromise Incidents

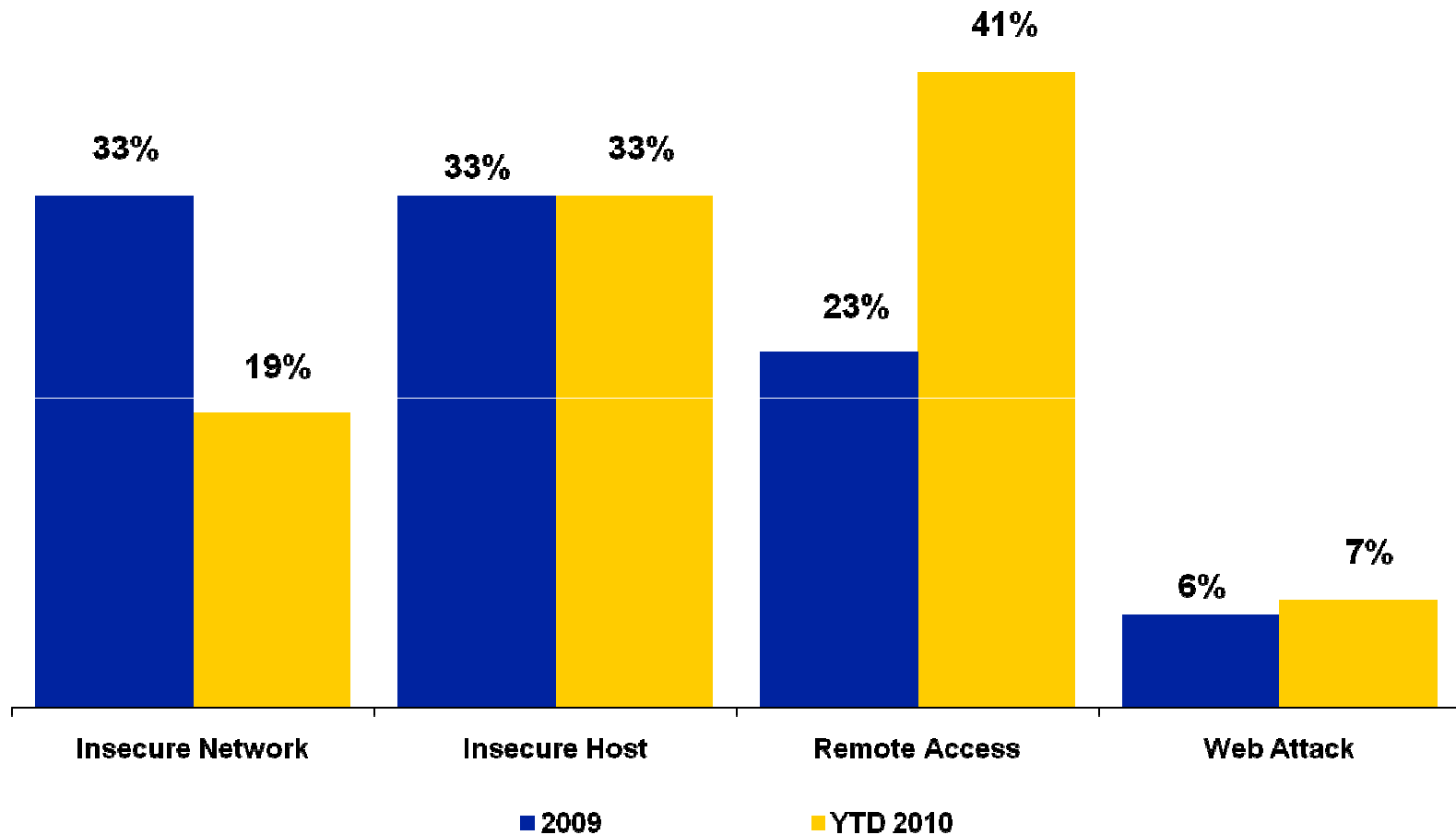
January 2008 through July 2010





Attack Vectors

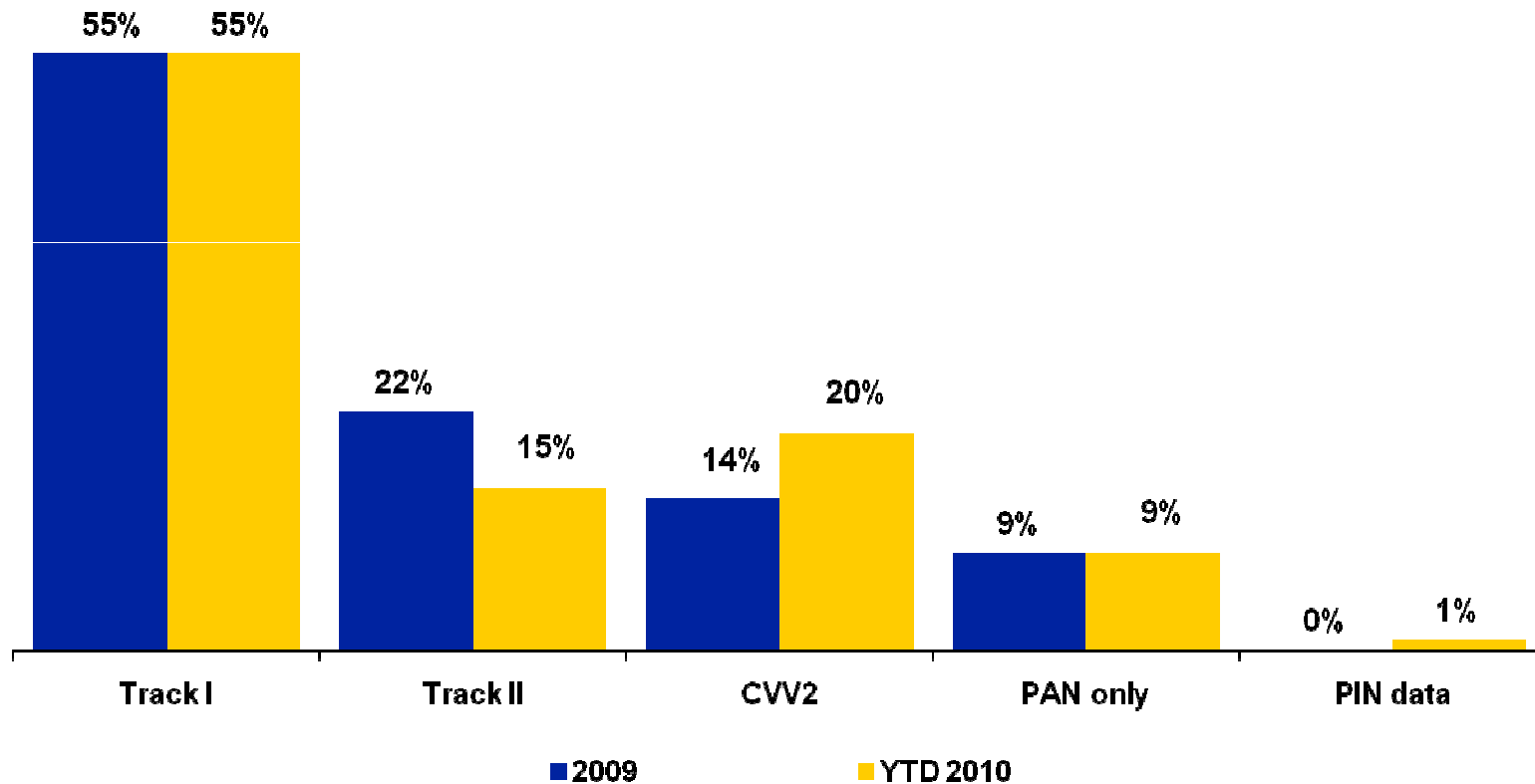
January 2009 through June 2010





Data Type At Risk

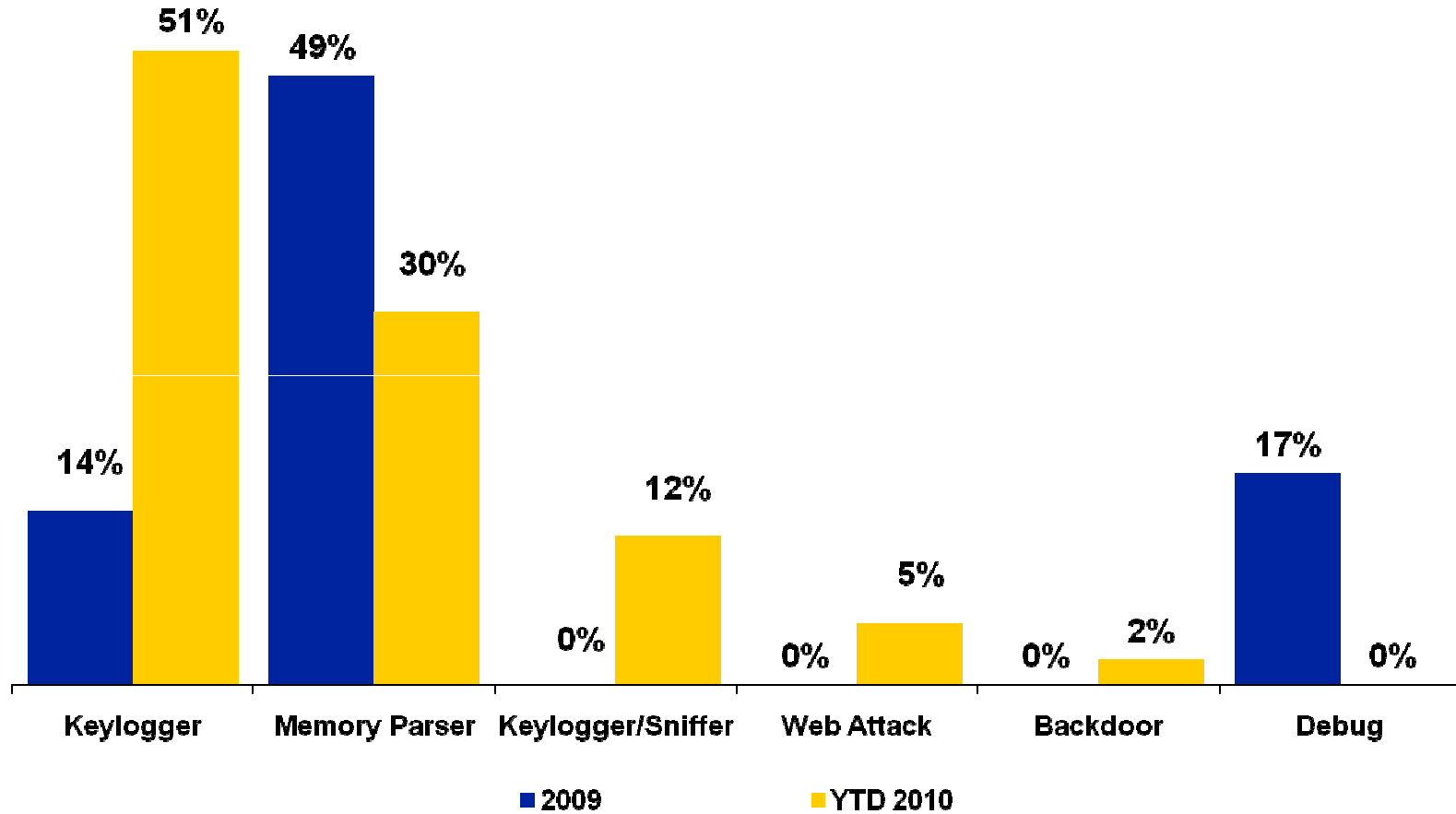
January 2009 through June 2010





Malware Types

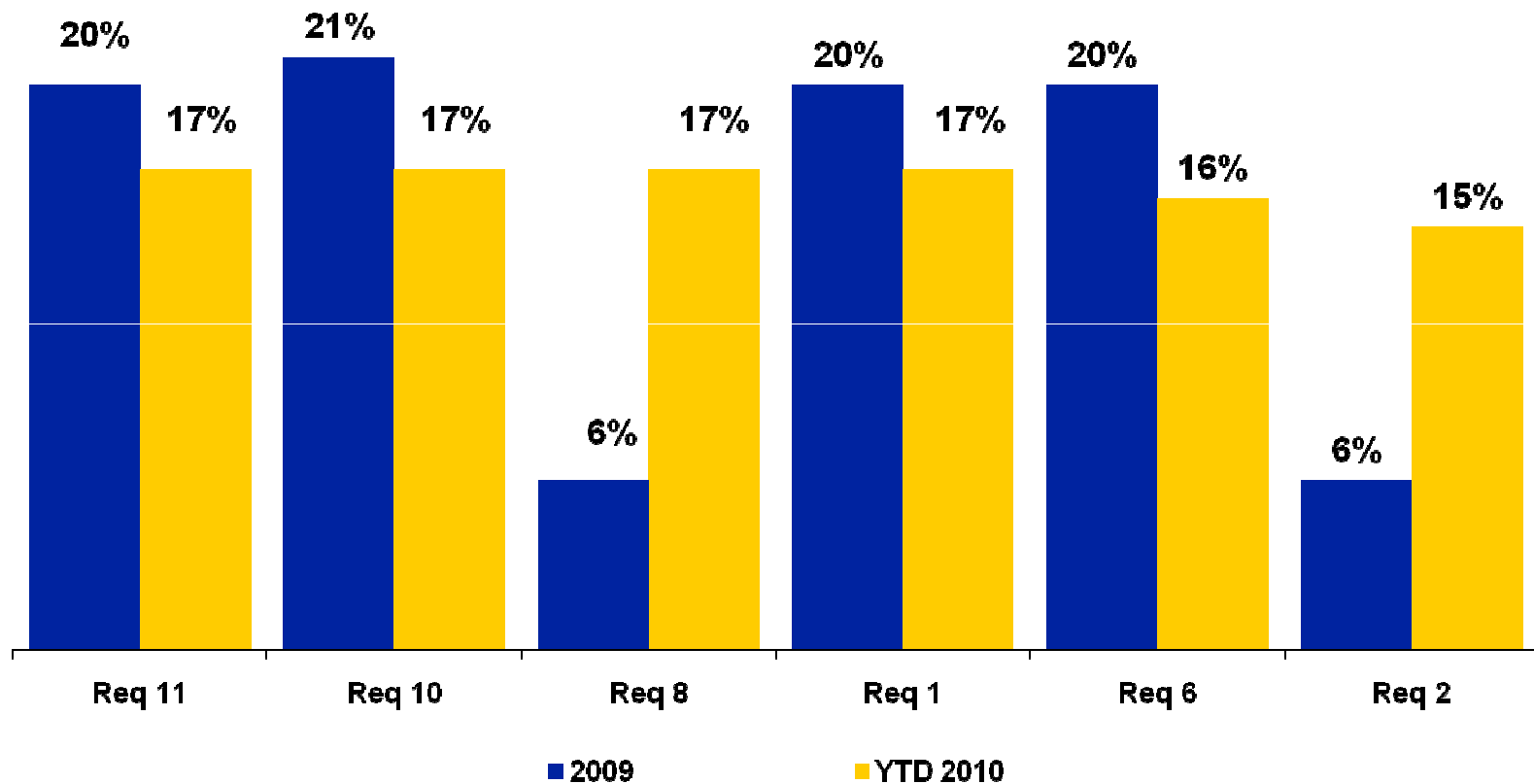
January 2009 through June 2010





Top PCI DSS Violations

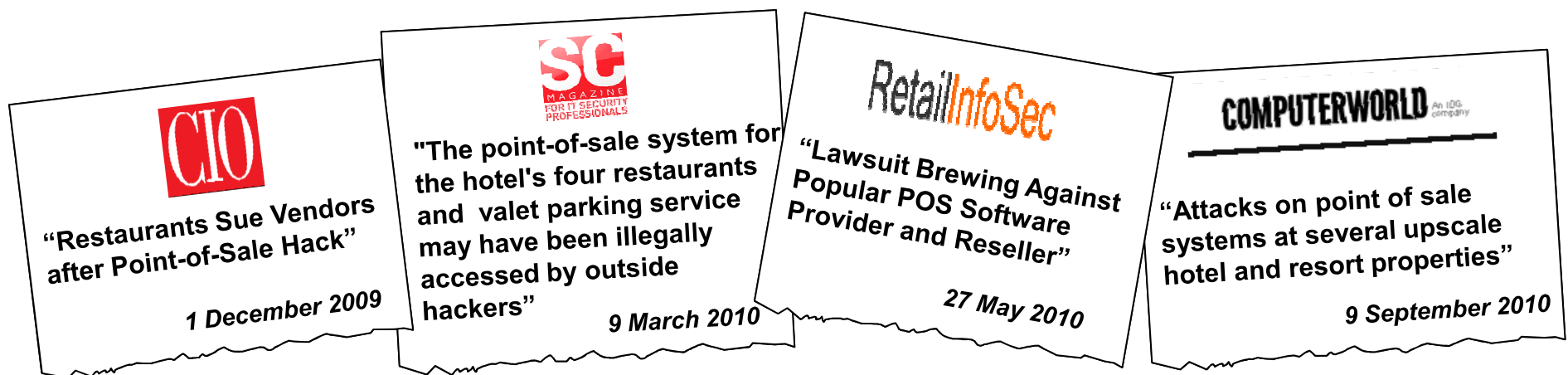
January 2009 through June 2010



Level 4 Merchant Compromises

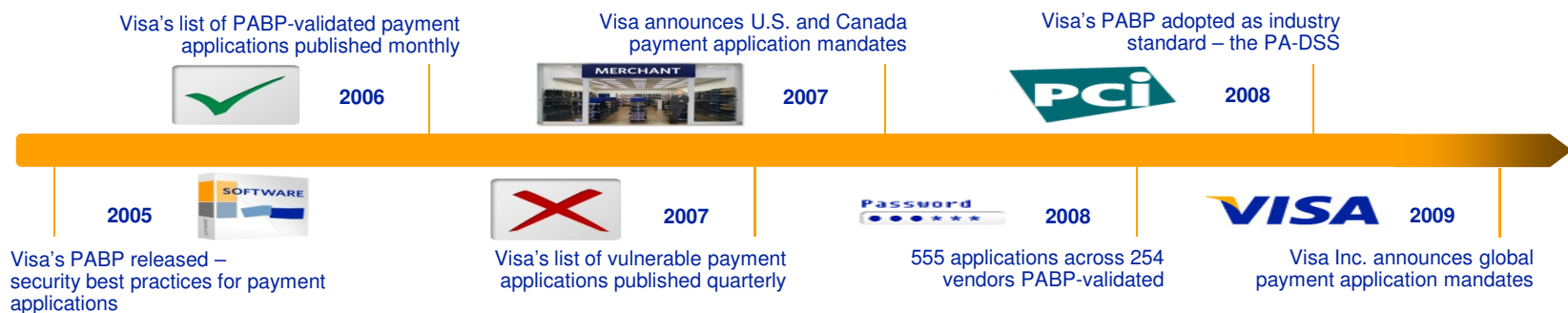


- Small merchant (Level 4) compromises are on the rise because of poor implementation of Point-of-Sale (POS) systems
- Many Level 4 merchants that use payment applications are asking their vendors for Payment Application Data Security Standard (PA-DSS) compliant software
- Level 4 merchants often rely on third parties (e.g., application vendors, resellers and integrators) to install and manage their POS software
- Unfortunately, in many compromise cases these same third parties have left their customers vulnerable to attack



Global Mandates for PA-DSS software

- In early 2007, Visa announced phased-in mandates for its U.S. and Canada markets requiring acquirers ensure their Level 3 and 4 merchants (new and existing) and their agents must use PA-DSS compliant applications or be PCI DSS compliant by **1 July 2010**
- With the successful adoption of these mandates, Visa announced similar mandates in 2009 for its remaining regions (Latin America, Central Europe and Middle East and Africa, as well as Asia Pacific markets) requiring:
 - Newly boarded merchants that use payment application software must use PA-DSS compliant applications or be PCI DSS compliant by **1 July 2010**
 - Acquirers must ensure their merchants (new and existing) and agents use PA-DSS compliant applications or be PCI DSS compliant by **1 July 2012**



Compliant Applications Not Enough



- Adopting PA-DSS compliant software is not being PCI DSS compliant, it does however:
 - Ensure software does not store sensitive cardholder data (i.e., full magnetic stripe data, CVV, CVV2 or PIN data) coveted by criminals
 - Provide protection of cardholder data (i.e., account number, cardholder name or expiry date) whenever stored by the payment application
 - Include a vendor's PA-DSS implementation guide which must include proper installation, maintenance and support procedures
- In numerous compromise events payment application vendors, resellers and integrators have left merchant systems exposed to attack
 - Deploying insecure POS builds (i.e., default and shared passwords)
 - Installing remote access software (e.g., pcAnywhere, Remote Desktop, VNC, etc.) with inadequate security
 - Upgrading to a compliant POS application, but not removing historically stored sensitive cardholder data
 - Using the same login credentials across all of their customers

Visa Top 10 Best Practices – Overview

Domain	Best Practice
Organizational Security	<ol style="list-style-type: none"> 1. Perform background checks on new employees and contractors prior to hire 2. Maintain internal and external software security training and certification curriculum
Mature Software Development	<ol style="list-style-type: none"> 3. Adhere to a common software development life cycle across payment applications 4. Ensure that newly released payment application versions are PA-DSS compliant
Product Vulnerability Management	<ol style="list-style-type: none"> 5. Conduct application vulnerability detection tests and code reviews against common vulnerabilities and weaknesses prior to sale or distribution 6. Actively identify payment application versions that store sensitive authentication data and/or retain critical security vulnerabilities, and notify affected customers
Secure Implementation	<ol style="list-style-type: none"> 7. Maintain customer service level agreements stating that only PA-DSS compliant payment application versions will be sold and supported 8. Implement an installer, integrator and reseller training and certification program that enforces adequate data security processes when supporting customers
Emerging Payment Technologies	<ol style="list-style-type: none"> 9. Adhere to industry guidelines for data field encryption and tokenization and PAN elimination across payment applications that use these technologies 10. Support capability of dynamic data solutions across payment applications

Best Practice #8



- Ensure that installers, integrators and resellers maintain adequate data security requirements in accordance with all PCI DSS and PA-DSS requirements, in addition to:
 - Ensuring that all new employees and contractors with access to customer sites pass background checks including, but not limited to, previous employment history, academic history, credit history and reference checks (within the constraints of local laws) before being offered employment
 - Ensuring that employees and contractors with access to customer sites are trained on how to adequately access, install, maintain and support payment applications (and any connected systems) in accordance with industry data security best practices and standards
 - Not selling, installing or supporting any vulnerable payment applications listed on the Visa list of Payment Applications that Store Sensitive Authentication Data (or any other known payment application that stores sensitive authentication data after authorization)

Best Practice #8 – Continued



- Ensure that installers, integrators and resellers maintain adequate data security requirements in accordance with all PCI DSS and PA-DSS requirements, in addition to:
 - Verifying at the completion of an installation that the payment application and its respective systems were correctly installed or configured; unique user IDs must be used for each customer site and for secure authentication functions
 - When upgrading the payment application, verifying that all historical sensitive authentication data, if stored by previous versions of the payment application, is securely wiped
 - When debugging or troubleshooting for customers, verifying that sensitive authentication data, if necessary to resolve a problem, is collected in limited amounts, encrypted while stored, and securely wiped immediately after use

Best Practice #8 – Continued



- Ensure that installers, integrators and resellers maintain adequate data security requirements in accordance with all PCI DSS and PA-DSS requirements, in addition to:
 - Ensuring that remote access to any customer’s site for the purposes of installation, support and maintenance is always done securely by:
 - Restricting access to customers’ sites and authentication credentials to only those personnel who need access
 - Limiting access from a limited number of trusted IP addresses and providing customers with a list of those IP addresses
 - Using strong two-factor authentication
 - Using unique, complex and secure authentication credentials for each customer
 - Ensuring that data transmissions are always encrypted
 - Advising customers to turn on remote access technologies only when necessary and needed, and to turn off access immediately thereafter
 - Instructing customers to install and properly configure a firewall, limiting remote access only to IP addresses where remote access is needed

Best Practice #8 – Continued



- Ensure that installers, integrators and resellers maintain adequate data security requirements in accordance with all PCI DSS and PA-DSS requirements, in addition to:
 - At minimum, installers, integrators and resellers must certify to these data security requirements through an internal vendor program requiring quarterly reports, which include employee training, certification and ongoing compliance to the requirements. For any installer, integrator or reseller who fails to maintain compliance and is found to have played a direct role in a customer's compromise, immediate dismissal or revocation will occur

Adopt Industry Best Practices



- Go beyond purchasing PA-DSS compliant software and focus on secure implementation by addressing common areas of compromise
- Demand your payment application company maintain due diligence of data security when installing, maintaining and supporting your systems
- Merchants should insist their payment application companies immediately adopt Visa's *Top 10 Best Practices for Payment Application Companies* located at www.visa.com/cisp under *Alerts, Bulletins & Webinars* then the *Best Practices* heading
- Visa has partnered with a highly recognized information security training leader, the SANS Institute to provide detailed training for vendors, integrators and resellers found at www.sans.org/visatop10



Questions?

