



Franchise Data Compromise Trends and Cardholder Security Best Practices

December, 2010





Franchise Data Security – Agenda

- Cardholder Data Compromise Overview
- Breach Commonalities
- Hacking Techniques
- Franchisee Security Practices, Training and Education
- Prevention Methods and Practical Security Guidance
- What to Do if Compromised Guidelines
- Questions?

2010: The Security Challenge



➤ **Fraudsters have evolved their business models and migrated between channels, products and geographies**

➤ **Criminals continue to adapt and challenge the system**

- The number of compromise incidents involving cardholder information has grown globally
- Stakeholder costs are increasing
- Security tops consumer concerns
- Regulatory attention and intervention on the rise

THE WALL STREET JOURNAL

**The Menace in the Machines --
Cyber-Scams On the Uptick
In Downturn**

M.P. McQueen
29 January 2009

**Consumer
Reports**

**Falling economy
pushing cybercrimes up**
21 May 2009

**PC
MAGAZINE**

22 April 2010

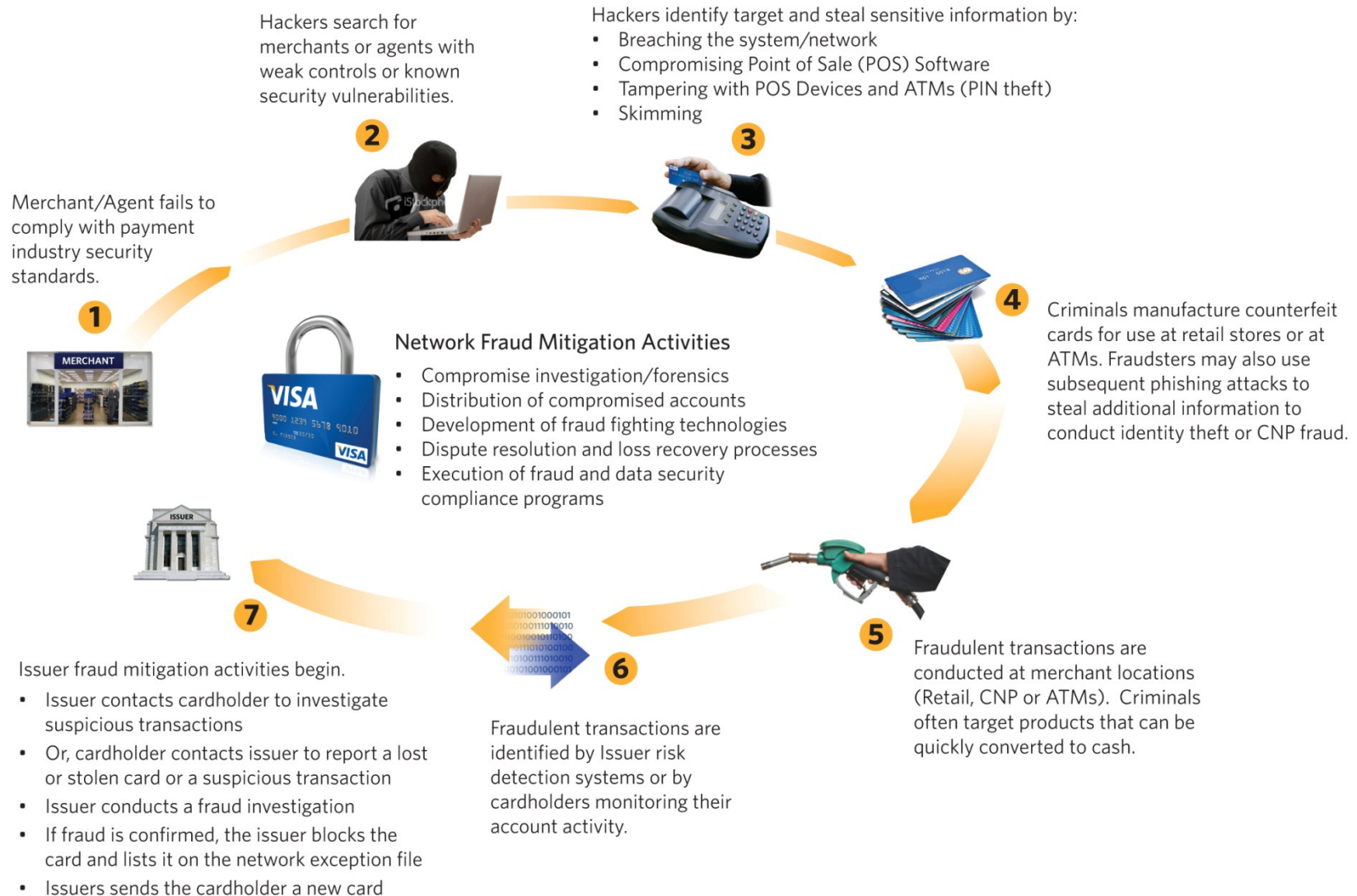
**Cybercrime Moving
to Emerging Countries
-- Since the Internet is
global, it doesn't really
matter where attacks
come from.**

REUTERS

**U.S. struggles to ward
off evolving cyber threat --
Spies, criminals, terrorists
eye U.S. networks**

12 May 2010

Typical Data Breach / Fraud Cycle





Hacking Methods

- Brute Force on Weak Log in Credentials
 - Point-of-Sale (POS)
 - Remote Desktop
 - Local/Domain Administrative Accounts
- Using selected internal computers as malware repositories
- Sending traffic in some cases over legitimate ports using traffic converters
- Taking advantage of 'Trusted' networks
 - Infiltrate one network and freely move about an additional network
- Use malware to steal cardholder data

Common Network Security Deficiencies

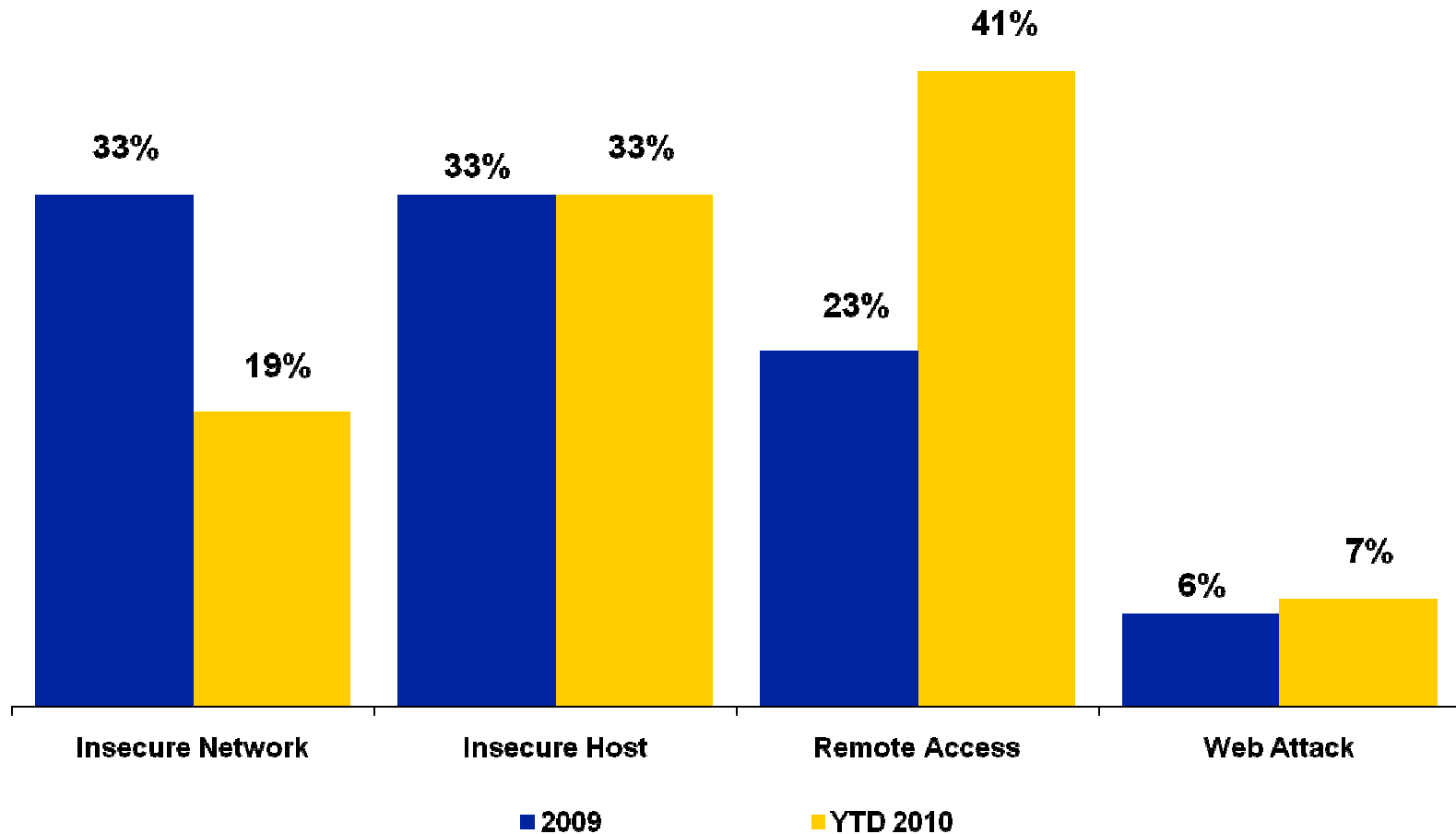


- Remote Management Access
- Trivial and Common Passwords
- Limited Access Control List (ACL) and segmentation
- Reliance on third-parties to install and manage Point of Sale (POS) systems
 - Many third-parties disregard security when implementing POS systems
- Attacks can easily propagate to other locations via:
 - **Limited ACLs on Wide Area Network**
 - **Insecure Remote Access (i.e., no two-factor authentication)**
 - **Common or “Dictionary” credentials**



Attack Vectors

January 2009 through June 2010

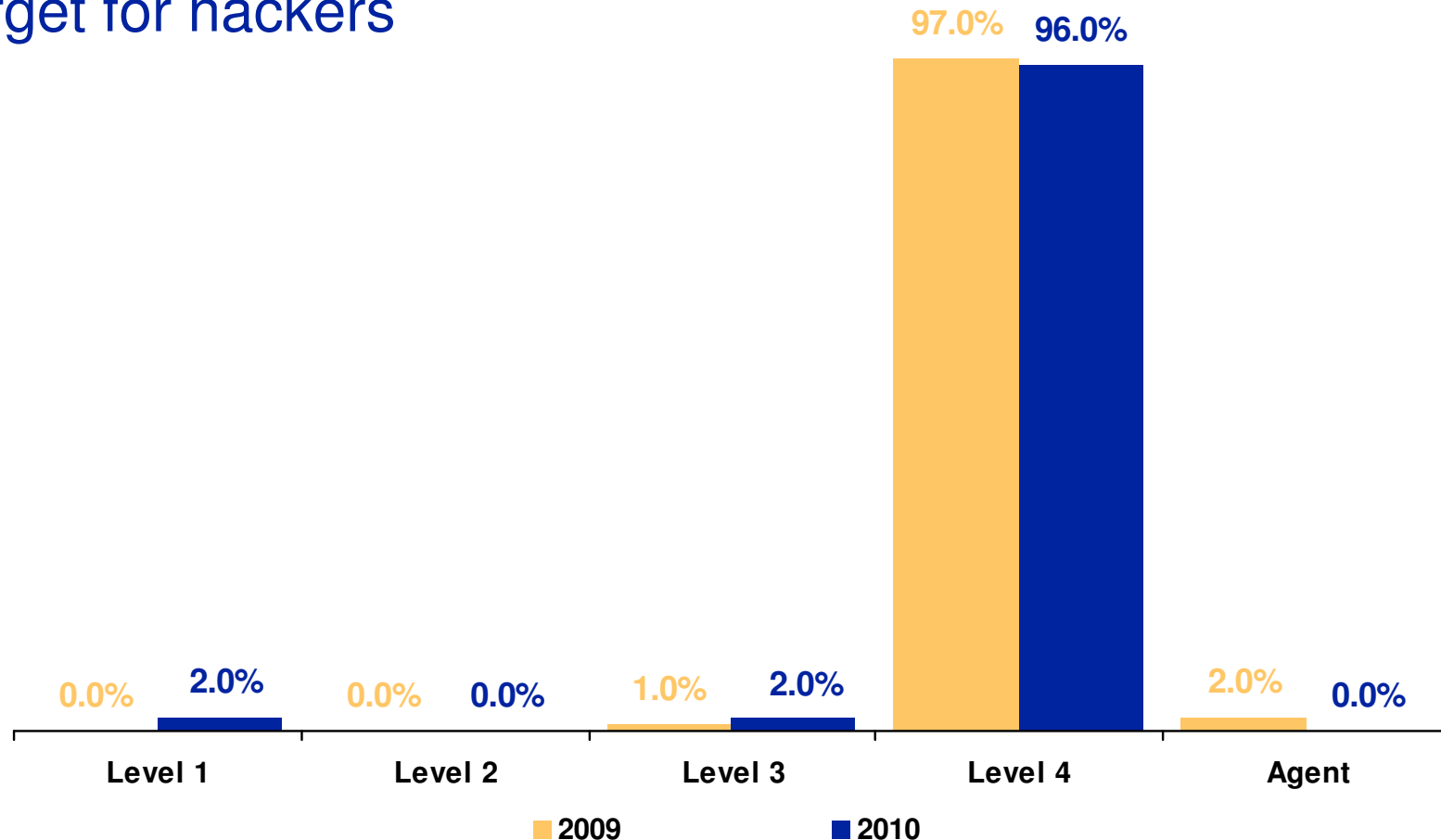




Impacted Compromised Entity Level

January 2009 through June 2010

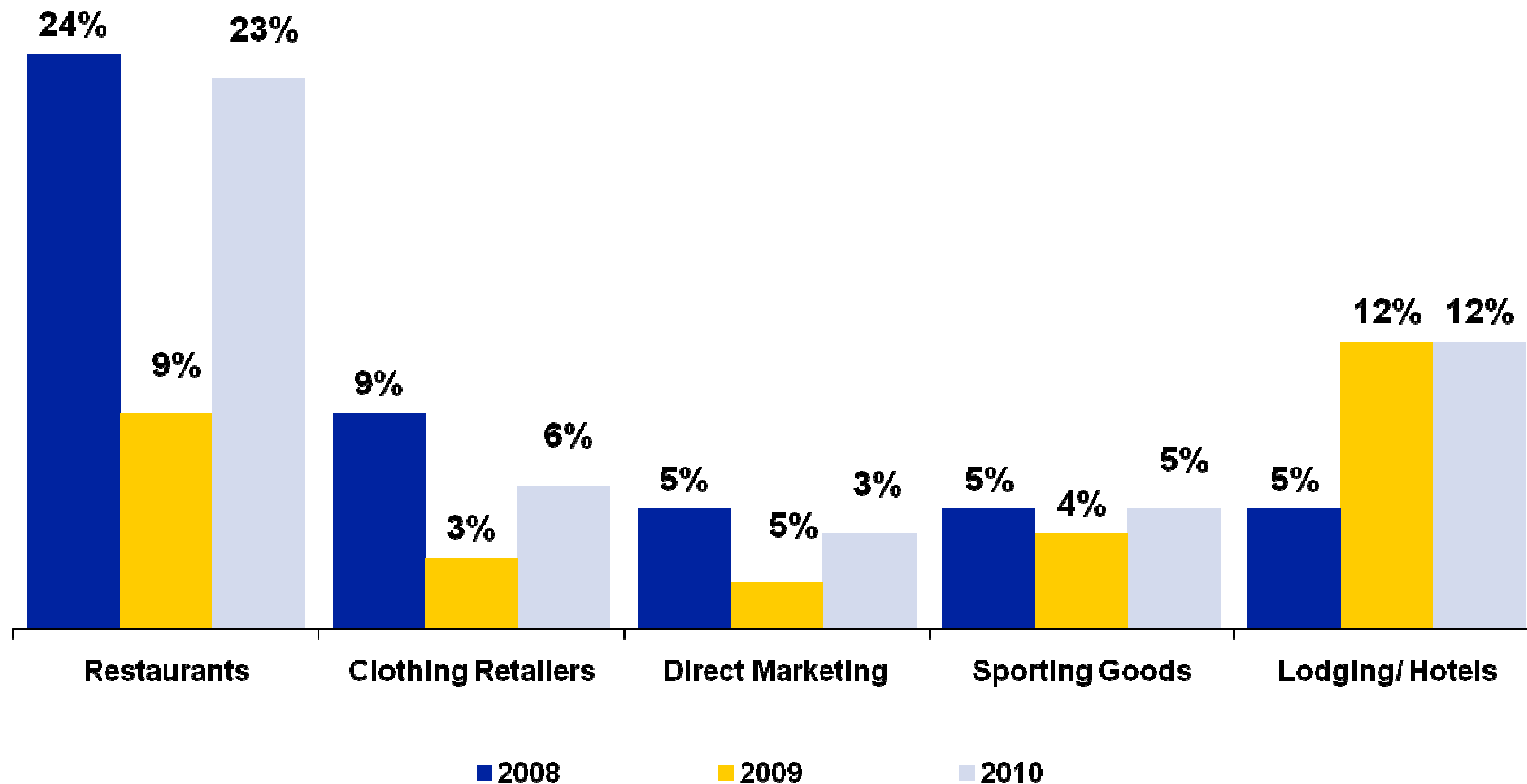
Level 4 merchants, specifically franchisees are primary target for hackers





TOP 5 Impacted Industries – Global System Compromise Incidents

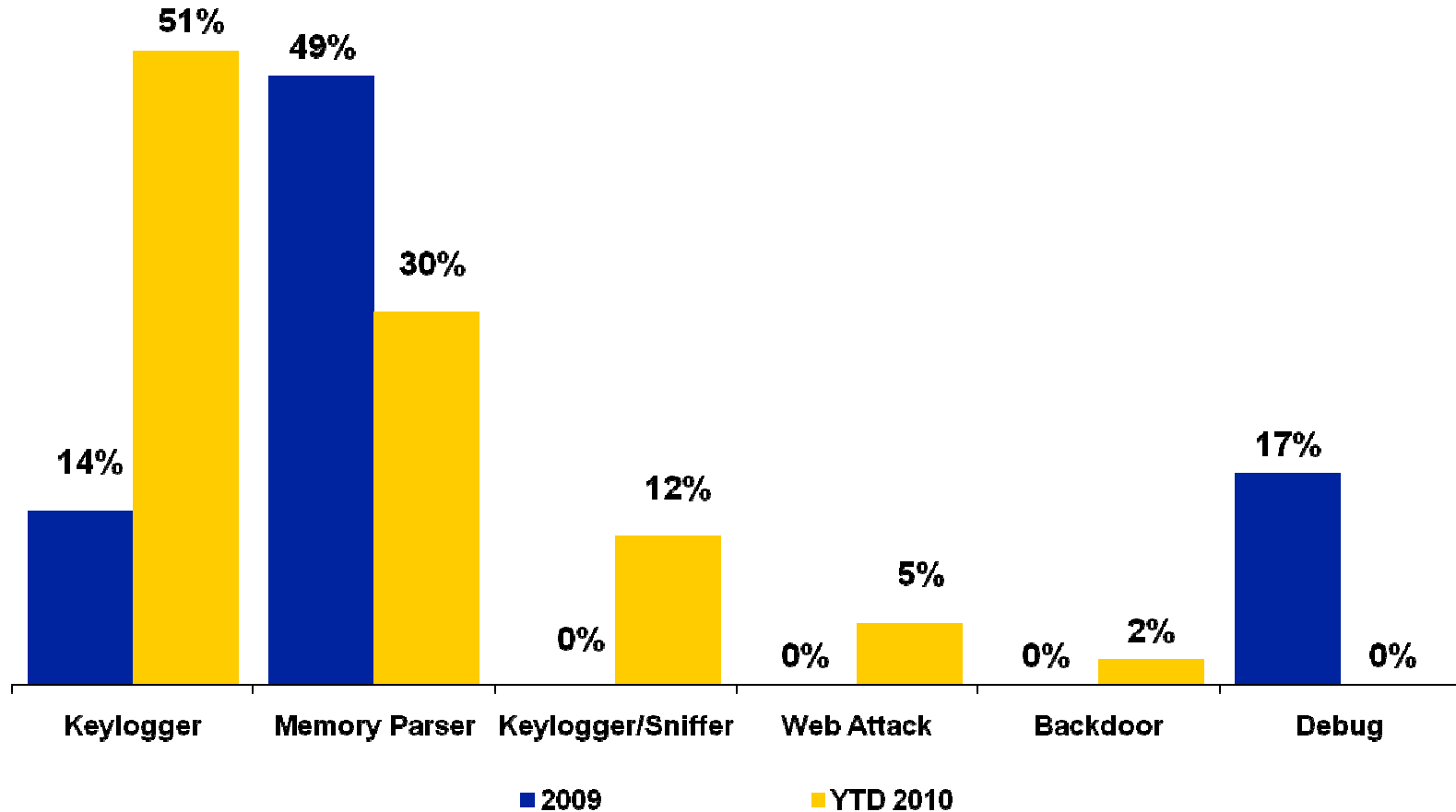
January 2008 through July 2010





Malware Types

January 2009 through June 2010



Payment Card Industry Data Security Standards (PCI DSS)

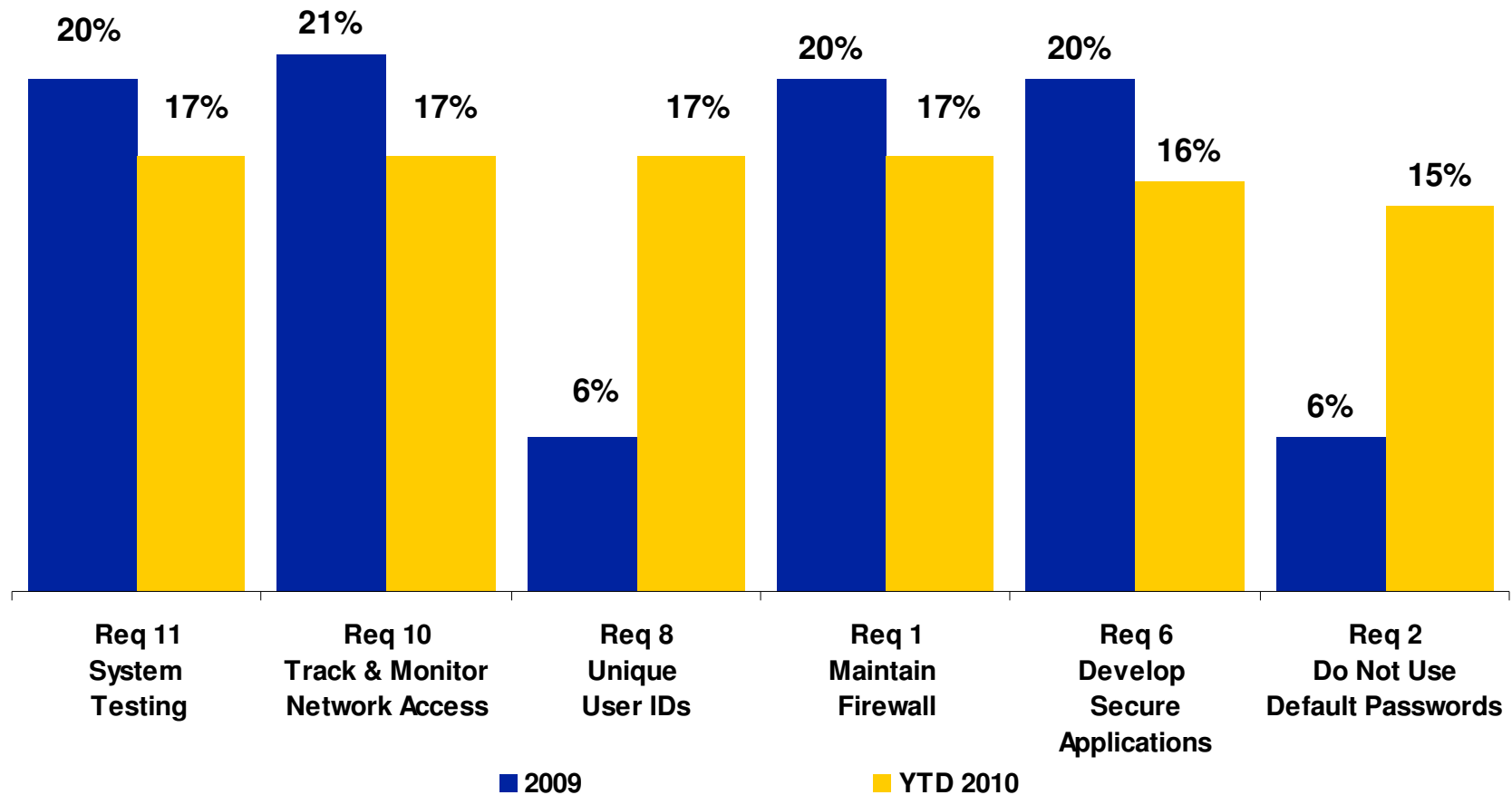


Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect data2. Do not use vendor-supplied defaults for system passwords and other security parameters
	<ol style="list-style-type: none">3. Protect stored data4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to data by business need-to-know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security



Top PCI DSS Violations

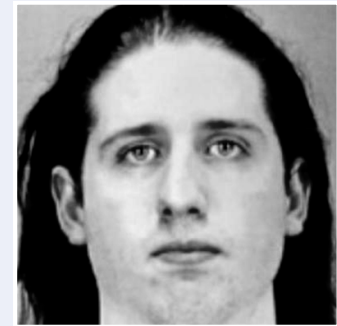
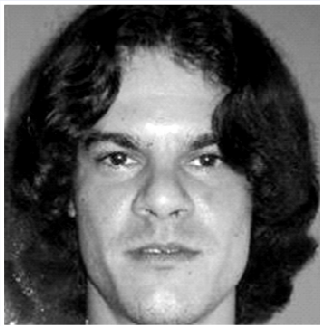
January 2009 through June 2010



Law Enforcement Successes



➤ International arrests, prosecutions and prison terms on the rise



The New York Times

20-Year Sentence in Theft of Card Numbers -- Albert Gonzalez of Miami, pleaded guilty last year to breaking into computer systems of major retailers.

25 March 2010

THE JERUSALEM POST

'The Analyzer' pleads guilty in NY - Hacker Ehud Tenenbaum admits to stealing \$10 million from US banks.

26 August 2009

WIRED

Coder Journeys From Wall Street to Prison -- a handful of convicted accomplices in Gonzalez's schemes check themselves into federal prison for years.

7 May 2010

PCWorld

A Ukrainian national has been arrested in India in connection with the most notorious hacking incident in U.S. history.

14 May 2010



Leading the Way in Data Security

The PCI DSS has been one of the key pillars in Visa's compromise prevention strategy

- Visa requires all entities that store, process or transmit Visa account data to comply with the PCI DSS
- Compliance validation requirements focus on VisaNet processors, third party agents and large merchants
- Visa Compliance Acceleration Program provided a combination of payments and fines to incentivize compliance among the largest U.S. merchants
 - PCI DSS compliance validation among the largest merchants has reached 96% in the U.S. and 77% worldwide
- Acquirers must maintain a small merchant security compliance program
- Progress three-part strategy to address franchise data security

* Data as of 9/30/10



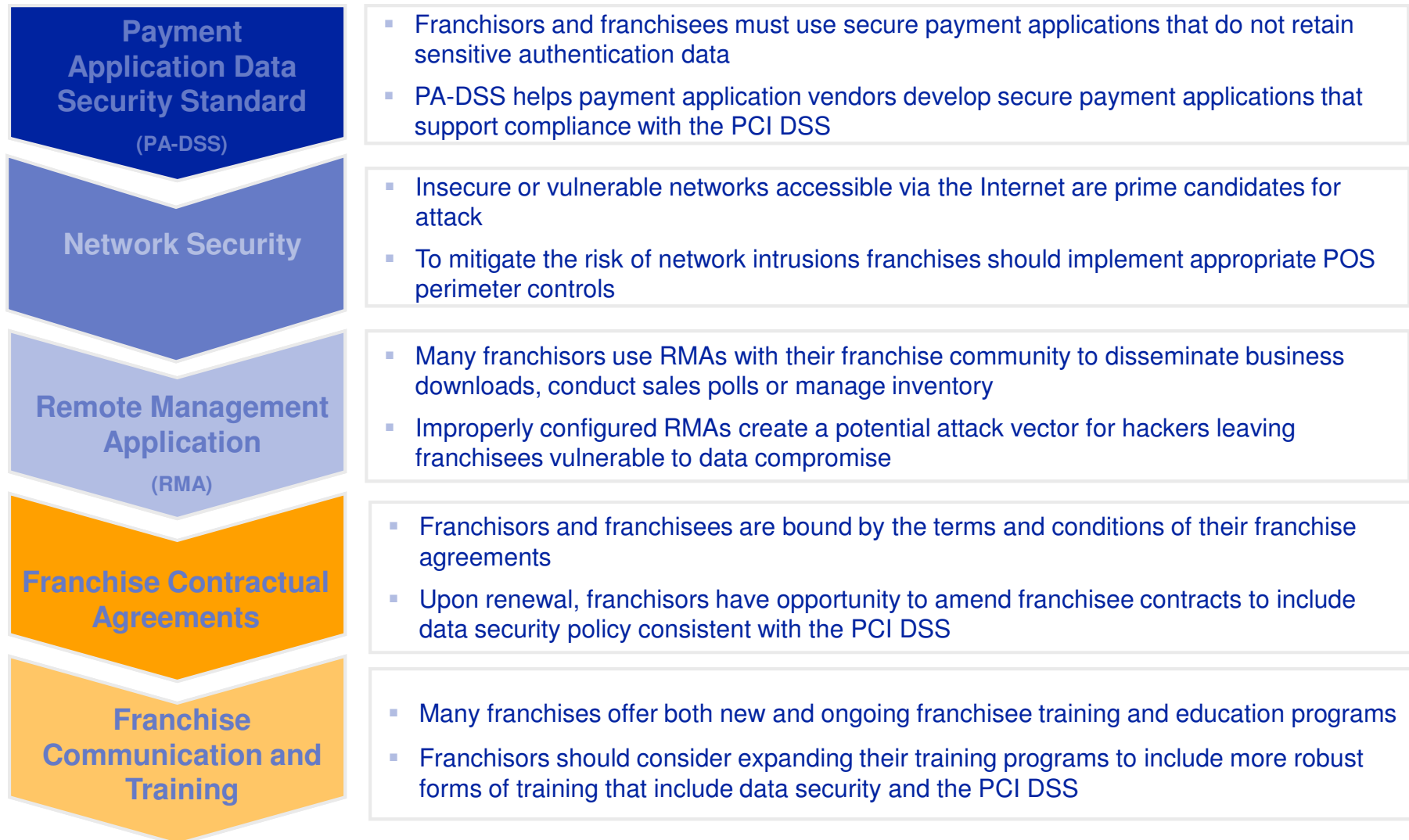
Franchise Data Security Strategy

■ Objectives

- Communication
- Education and Training
- Compromise Response
- Ensure franchisees use compliant payment applications and eliminate use of vulnerable payment applications
- Expand use of franchise data security strategy globally
- New franchise service provider category created to ensure corporate payment infrastructure operates in compliance with PCI DSS

Franchise Cardholder Data Security:

Key Security Tips





Preventive Techniques – Firewalls

Proper firewall rules configuration and management of network devices is critical to preventing unauthorized access

- Identify normal data flows for cardholder information into and out of the network
- Identify any systems that store, process or transmit account data
 - Define separate network security zones to include systems that have similar risk levels, such as account data
- Permit network traffic only where there is a defined business need and deny all other network traffic



Preventive Techniques – Administrative Accounts

Secure all local and domain administrative accounts to help ensure unauthorized software cannot be installed on ANY systems

- Administrative Level Account Credentials should be:
 - Complex (e.g., alpha numeric, special characters)
 - Frequently changed
 - Not easily guessable (e.g., baker967 vs. BaKer \$09)
 - Implemented at 'least' privilege necessary for system and application accounts
 - Checked for 'backdoor' accounts (sometimes are created by employed domain administrators)
 - Regularly audited of domain and local system administrator accounts



Preventive Techniques – Remote Access

Implement ‘on demand’ remote desktop services

- Service should only be allowed on only when needed and terminated at completion of remote necessity
- Vendors will argue this cannot be done, however this is a necessity at this point
- Hackers learn “POS” Vendor support account credentials to gain access via remote desktop services and access your infrastructure
- Implement latest remote access products and configure securely (e.g., IP filtering, strong encryption)
- Implement change control procedures

Ensure accounts that have remote desktop (including terminal services) capabilities take advantage of complex and frequently changed passwords

- Vendors or third-parties may resist complex passwords; however this is your **right** as a customer



What To Do If Compromised

- **Please review the “What to do if Compromised” Manual**
- **Types of compromise Visa investigates:**
 - Network intrusions
 - Skimming
 - Lost or stolen receipts
 - Lost or stolen computers
- **How Visa is notified:**
 - Issuer notification through common-point-purchase (CPP) analysis
 - Acquirer notification
 - Compromised entity notification
 - Visa identifies compromise
 - Law enforcement
 - Media reports



What To Do If Compromised

Requirements for Compromised Entities

- If you detect a suspected or confirmed breach, you must:
 - Immediately contain and limit the exposure
 - Preserve evidence and facilitate the investigation
 - Alert your internal Information Security group and Incident Response Team
 - Contact your merchant bank and provide documentation (i.e., sequence of events)
 - If you do not know your merchant bank, contact Visa Regional Fraud contact;
 - **Contact your local law enforcement office**
- It is critical to work with your merchant bank and Visa to assist with containment

The Future of Payments Security and Risk



- 1 Dynamic Authentication:** allowing merchants to focus less on security and more on commerce
- 2 Powerful Security:** among stakeholders who retain vulnerable data
- 3 Intelligent Response:** to shut down fraud and reduce the costs to stakeholders
- 4 Solutions that Engage Consumers:** to protect themselves from fraud
- 5 Innovation, Leadership & Collaboration:** partnering and enabling clients & stakeholders to grow their business