



# PCI Impact on Merchants Utilizing POS Solutions

---

WSAA – October 2009

# Card Compromise Trends

**Criminals are becoming more organized and sophisticated.** Carders are largely responsible for the upward trend in data breaches.

- A new brand of criminals, known as “**Carders**”
- “**Carding Forum**” Websites, dedicated to the resale of large volumes of sensitive data, creating a new **black market**
- Organized crime was responsible for over **90% of the 285 million** records compromised in 2008\*



## Former Carding Forum

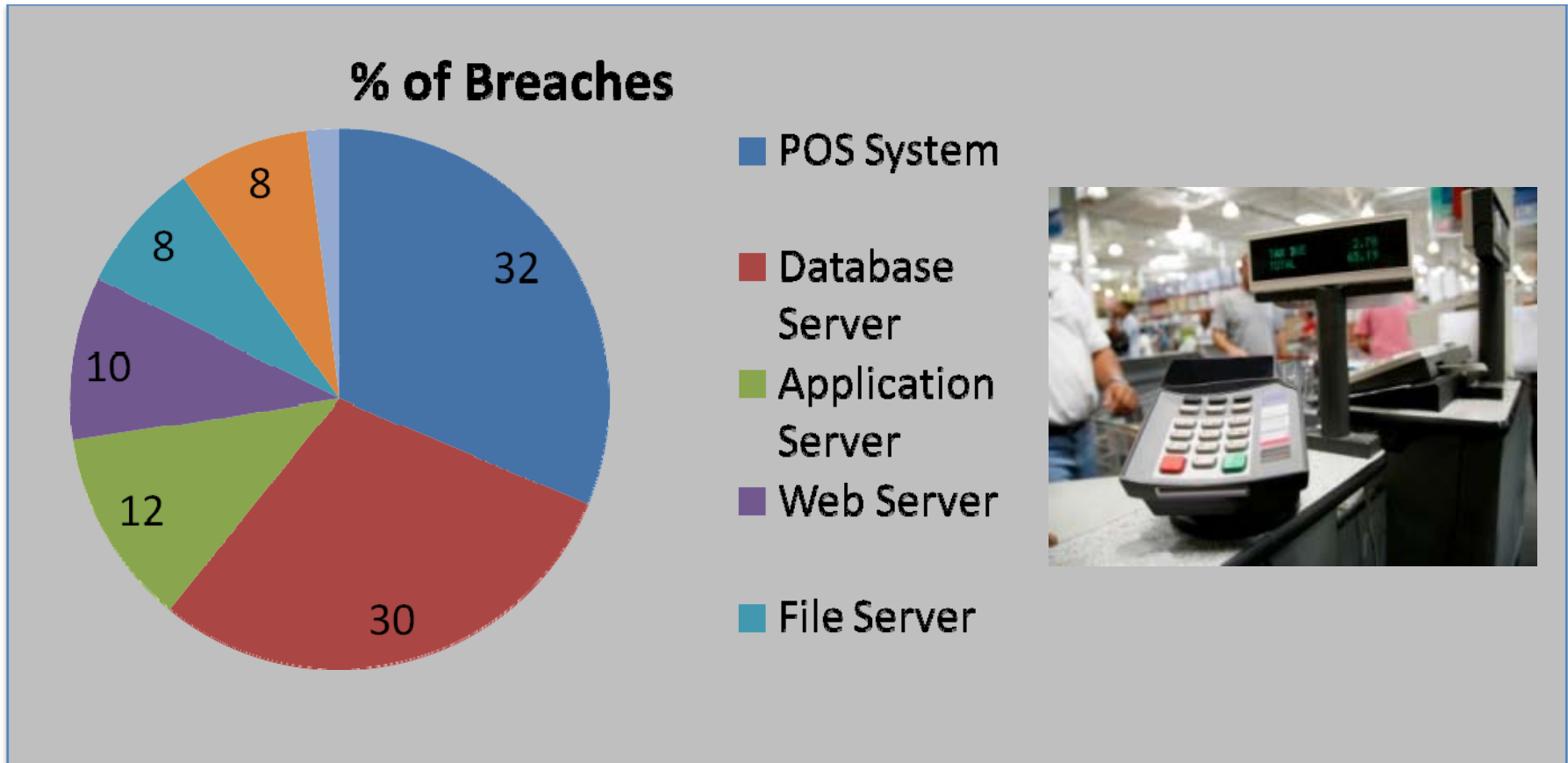
- Tutorials and hacking tools
- Postings to buy/sell stolen data
- Downloadable code for phishing attacks

Source: DOJ “Data Breaches: What the Underground World of ‘Carding’ Reveals”

\*Source: Verizon Business Data Breach Report

# Card Compromise Trends

The Verizon Business 2009 Data Breach Report shows that **POS Systems** were the most commonly exploited system among engagements analyzed.



Source: Verizon Business 2009 Data Breach Investigations Report

© ControlScan, Inc. 2009 Proprietary and Confidential

Objective of the Payment Application Data Security Standard (PA DSS) is to **drive prohibited data storage out** of the payments environment.

- **Formerly** under the supervision of Visa - Payment Application Best Practices (PABP)
- Pertains to payment applications that are **sold, distributed or licensed** to 3rd parties (POS, Shopping Cart, Kiosk, etc); **not:**
  - **Customized** payment applications for in-house use only
  - **Standalone/dial-up** terminals
- Aimed at helping software vendors **develop secure** payment applications
- **Enforcing** use of a **compliant payment application** is the **Acquirers** responsibility

# PA DSS Compliance Deadlines - Visa

**Phase III** requires Acquirers to only issue a **new MID** if the merchant has validated **PCI Compliance** or is using a **compliant payment application**. **Phase V** pertains to **Acquirer's existing merchant base** and requires them to only use compliant payment applications.

<i>Phase</i>	<i>Compliance Mandates</i>	<i>Effective Date</i>
I.	Newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (“VNPs”) and agents must not certify new payment applications to their platforms that are known vulnerable payment applications	1/1/08
II.	VNPs and agents must only certify new payment applications to their platforms that are PABP-compliant	7/1/08
III.	Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or use PABP-compliant applications	10/1/08
IV.	VNPs and agents must decertify all vulnerable payment applications	10/1/09
V.	Acquirers must ensure their merchants, VNPs and agents use only PABP-compliant applications	7/1/10

Most are scrambling to meet Phase V

# PCI DSS Self-Assessment Questionnaire (SAQ)

The **SAQ** is the primary vehicle for small merchants to **demonstrate compliance** with PCI Data Security Standards (PCI DSS).

SAQ Validation Type	Description	SAQ	# of Questions
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced to a PCI-Compliant Service Provider	A	11
2	Imprint-only merchants with no electronic cardholder data storage	B	25
3	Standalone dial-up terminal merchants, no electronic cardholder data	B	25
4	Merchants with payment application systems connected to the Internet, <b>no</b> electronic cardholder data storage (ex: internet-facing POS, shopping cart, etc)	C	38
5	All other merchants (not included in descriptions for SAQs A-C above) and all service providers defined by a payment brand as eligible to complete an SAQ	D	226

Merchants using **POS software** applications typically complete **SAQ C or D**.

**Requires Vulnerability Scanning**

# The Consequences

A data breach typically has a **significant financial** and **operational impact** on a small merchant.

Costs may include:

- **Forensics audit** costs: \$8,000 to \$20,000
- **Card replacement costs:** generally between \$5 and \$10 per card
- **Productivity Loss:** Varies - a lot of paperwork and overhead to manage the post-breach process. Think “IRS Audit.”
- **Compliance fines:** Could range from \$5,000 to 250,000 depending on the size of the breach and the nature of the offense that led to the compromise
- **Brand damage:** Hard to quantify, but at the end day this could be the most damaging of all



# Key Takeaways

**As trusted allies**, Acquirers/ISOs are uniquely positioned to help educate merchants on the **importance of becoming PCI compliant and using certified POS systems.**

- POS solutions are among the most widely compromised
- Risk mitigation strategy -- focus your initial compliance efforts on merchants using POS solutions
- Remember: PA DSS supports PCI DSS; however, using a compliant payment application alone does not make your merchants PCI Compliant

