

# La réglementation VisaCard, MasterCard PCI-DSS

---

*Conférence CLUSIF "LES RSSI FACE À  
L'ÉVOLUTION DE LA  
RÉGLEMENTATION" 7 novembre 07*

Serge Saghroune



# Overview of PCI DSS

## Payment Card Industry Data Security Standard

---

- Prior to September 2004
  - no standardization across card companies on credit card security requirements
  - difficult for merchants to become familiar with and adhere to competing standards from VISA, MasterCard, and others
- As fraud losses increased, card industry realized the need for consistent and well defined security standards

# Overview of PCI DSS

## Payment Card Industry Data Security Standard

---

- PCI DSS announced in September 2004
  - collaboration between VISA and MasterCard
  - endorsed by other card companies as well
  - “... offers a single approach to safeguarding sensitive data for all card brands...”

# Overview of PCI DSS

## Payment Card Industry Data Security Standard

---

- Applies to
  - all merchants that “store, process, or transmit cardholder data”
  - all payment (acceptance) channels, including brick-and-mortar, mail, telephone, e-commerce (Internet)
- Includes 12 requirements, based on
  - administrative controls (policies, procedures, etc.)
  - physical security (locks, physical barriers, etc.)
  - technical security (passwords, encryption, etc.)

# Card Security Programs

---

- The following programs incorporate PCI DSS:
  - VISA
    - Cardholder Information Security Program (CISP)
  - MasterCard
    - Site Data Protection (SDP) Program
  - American Express
    - Data Security Requirements
  - Discover
    - Discover Information Security and Compliance (DISC) Program

# PCI DSS requirements

## Payment Card Industry Data Security Standard

---

***Each requirement has many sub-requirements!***

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data

# PCI DSS requirements

---

4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need-to-know

# PCI DSS requirements

---

8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

# Merchant levels

---

- Merchant levels are based on yearly transaction volume of merchant
- Specific criteria for placement in merchant levels varies across card companies
- All merchants, regardless of level, must adhere to PCI DSS requirements
- Level into which merchant is placed determines PCI DSS compliance validation (and ultimately cost)
- Let's take a quick look at Visa's levels...

# Merchant levels - Visa

---

- Level 1:
  - merchants, regardless of acceptance channel, processing over 6,000,000 Visa transactions
  - **any merchant that has suffered a data compromise**
  - any merchant so selected by Visa
  - any merchant identified by other card brand as level 1

# Merchant levels - Visa

---

- Level 2:
  - merchants, regardless of acceptance channel, processing 1,000,000 to 6,000,000 Visa transactions
- Level 3:
  - any merchant processing 20,000 to 1,000,000 Visa e-commerce (Internet) transactions

# Merchant levels - Visa

---

- Level 4:
  - any merchant processing fewer than 20,000 Visa e-commerce (Internet) transactions
  - all other merchants, regardless of acceptance channel, processing up to 1,000,000 Visa transactions

# PCI DSS compliance validation

---

- Level 1 merchants
  - annual on-site assessment by approved assessor (generates a report on compliance)
  - quarterly network security scan by approved scan vendor
- Level 2 and 3 merchants
  - self-assessment questionnaire
  - quarterly network security scan by approved scan vendor

# PCI DSS compliance validation

---

- Level 4 merchants
  - self-assessment questionnaire
    - if required by acquirer
  - quarterly network security scan by approved scan vendor
    - if required by acquirer
  - will most likely hold merchants to higher standard than dictated by PCI DSS
    - especially for level 4 merchants