PCI DSS – Why it matters

Steve Wilson

Head of Information Security Compliance

Visa Europe

Madrid

7 November 2007

What is PCI DSS ?

- ‘Common sense’ approach to data security
- Closely linked to other standards
  - BS 7799
  - ISO 27001
  - Sarbannes Oxley etc
- Focussed on card data
- Owned and managed by PCI SSC (independent of the card schemes)
  - Any organisation can become a participant

Why is PCI DSS important ?

A simple equation

Data = identity = money

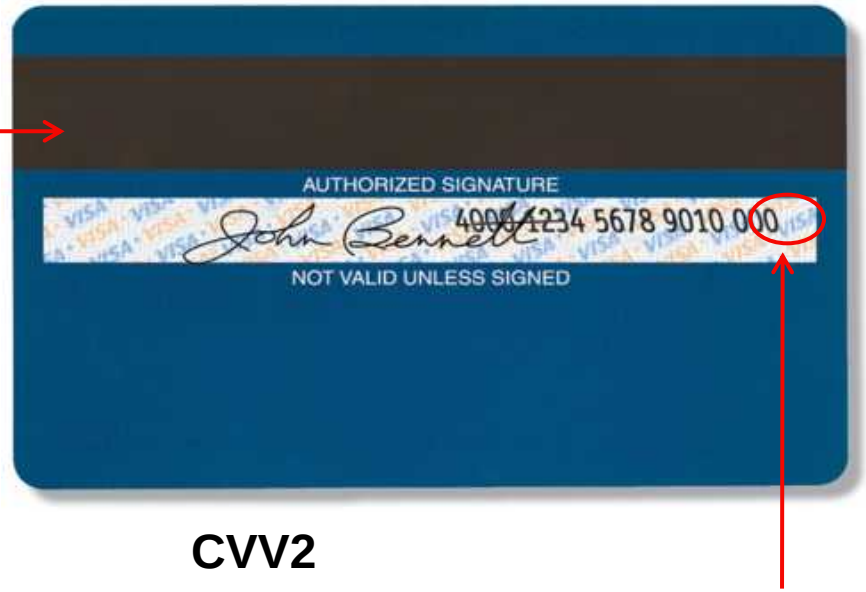
A Visa card…

Card number

Expiry date

A Visa card…(cont.)

Magnetic Stripe
made up of “Track 1” and
“Track 2” data



CVV2

The card account number, plus a three-digit Card Verification Value 2 (CVV2) is indent-printed on the signature panel

Track data and CVV2 should never be stored after authorisation

Card data is retained by companies for 3 weeks or longer after authorisation

Reasons given include:

- Marketing purposes
- As a unique customer identifier
- Fraud analysis
- Customer profiling

Data security and your brand

-How much would your brand be worth if you lose your consumers trust?

-Would your consumers stay with you?

-Would your shareholders stay with you?

Your brand needs security!

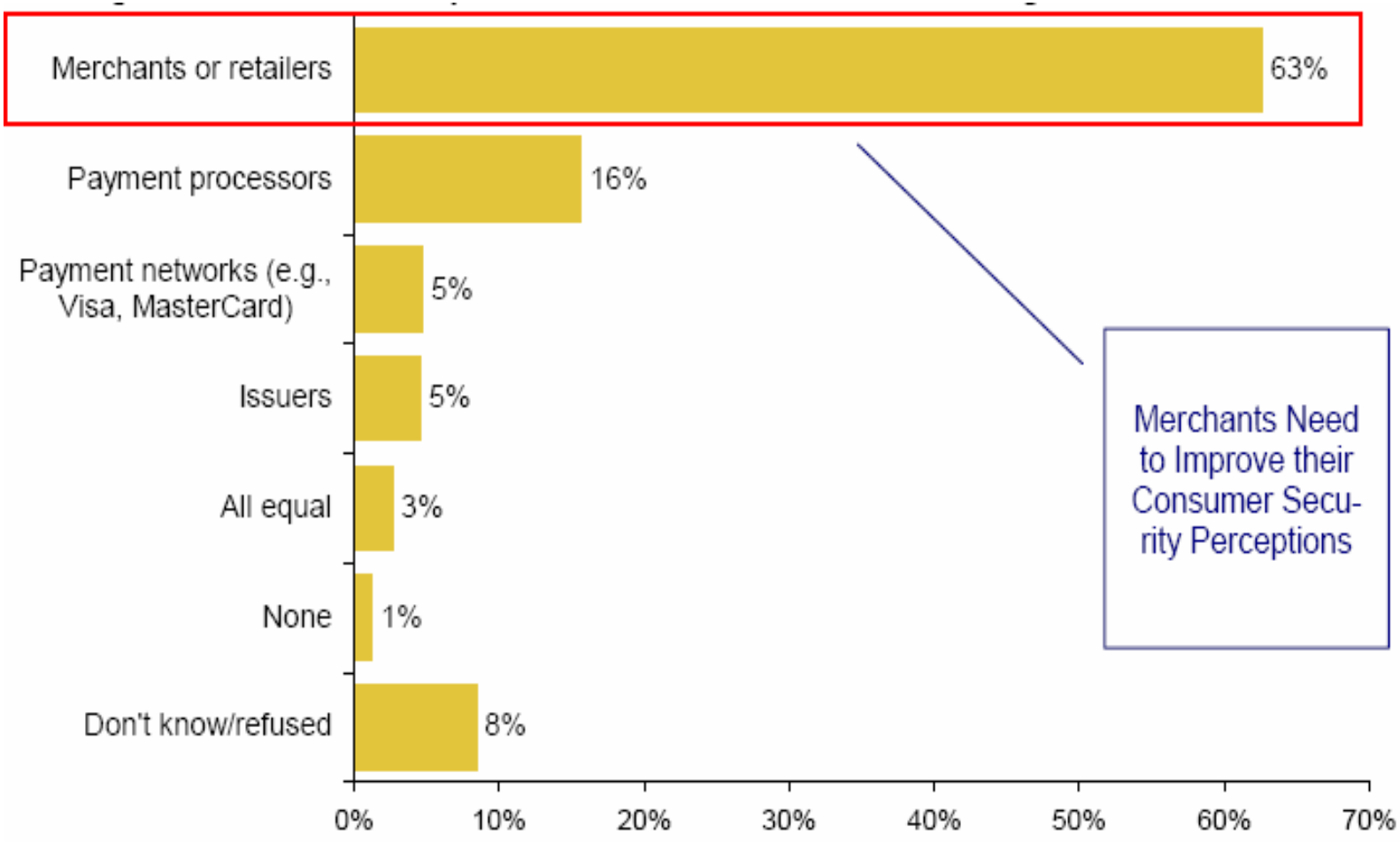
-Compromises do happen everyday, everywhere

-In the consumer's view, consumers, card schemes and merchants share responsibility for protecting their card data

Yet… 63% of consumers views merchants as the weakest link when it comes to protecting their data…[1]

[1]Source: Javelin Strategy and Research 2007

Merchants as the weakest link



Consumer confidence seriously impacted by a data breach

In the case of a breach….

49% of consumers believe merchants to be the most likely source of the data breach

3 out of 4 consumers won't shop again at a compromised merchant

Investing in PCI DSS should be part of your consumer retention plans

Media and regulators are watching us…

-National and European Government are showing increasing interest in the area of account information security

- The European Commission is considering legislation on the duty to notify (suspicion of breach and actual compromise) – already adopted in California, Minnesota and Texas

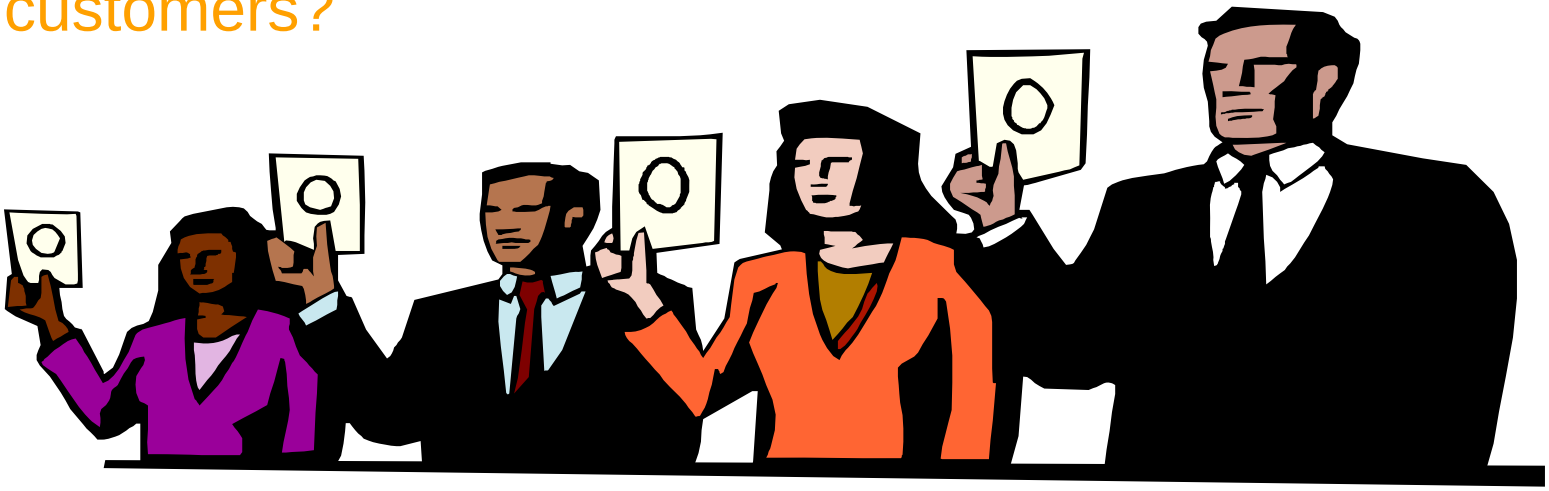
-Media increasingly questioning industry compliance and progress…..

Security and your corporate social responsibility strategy

84% of consumers want to shop at merchants who are security market leaders

A secure merchant secures consumers trust!

Can you retain your shareholders if you lose your customers?



Security/IT benefits

A socially responsible merchant is fully aware of how its systems work and what it is doing to protect card data in their possession

PCI DSS makes you aware of issues;

-This enables you to fix them

-This works towards protecting consumers and shareholders trust in your brand

Financial benefits

-The sheer financial cost of a compromise may prove hard to bear

-Large retailers indicate that their business case for investing in PCI DSS is based on the potential financial cost of reacting to a data breach

Costing the reaction to a data breach

= € 10,000,000[1]

+Hiring security firms to contain the compromise

+Replacing systems

+Increased customer service costs

+Actual costs of internal investigations

+Outside legal defence fees

+Discounted services offered

+Lost employee productivity

+Financial hit from lost customers

[1] Figure is based on the average cost of containing a compromise based on research by the Ponemon Institute

Some Tips from Large Merchants in Europe and US

Sr. management sponsorship is mandatory

- Assign dedicated people
- PCI DSS is as much about people and business processes as it is systems
- Map and document your business processes
  - Trace cardholder from point of sale to billing and settlement.
  - Map systems, applications and databases that support these processes
  - Re-engineer processes to remove duplicate or unnecessary data
- Reduce the scope as much as possible
  - Segment cardholder data network from rest of network
  - If you don’t need it, don’t store it!
- Engage a QSA early on in the project

Considerations

-We need to reduce our information footprint

-We need to rethink ways of achieving the same marketing ad fraud objectives without storing data unnecessarily

-We need to prioritise the removal of magstripe and card verification data

Support from Visa Europe

Collateral available from Visa Europe website

http://www.visaeurope.com/aboutvisa/security/ais/main.jsp

- Merchant implementation guides

-Service Provider guides

  - Available in English, French, Spanish, German, Italian

- List of certified Service Providers

- Work with Acquiring banks to provide
  - Merchant training
  - Guidance on specific issues

Thank you