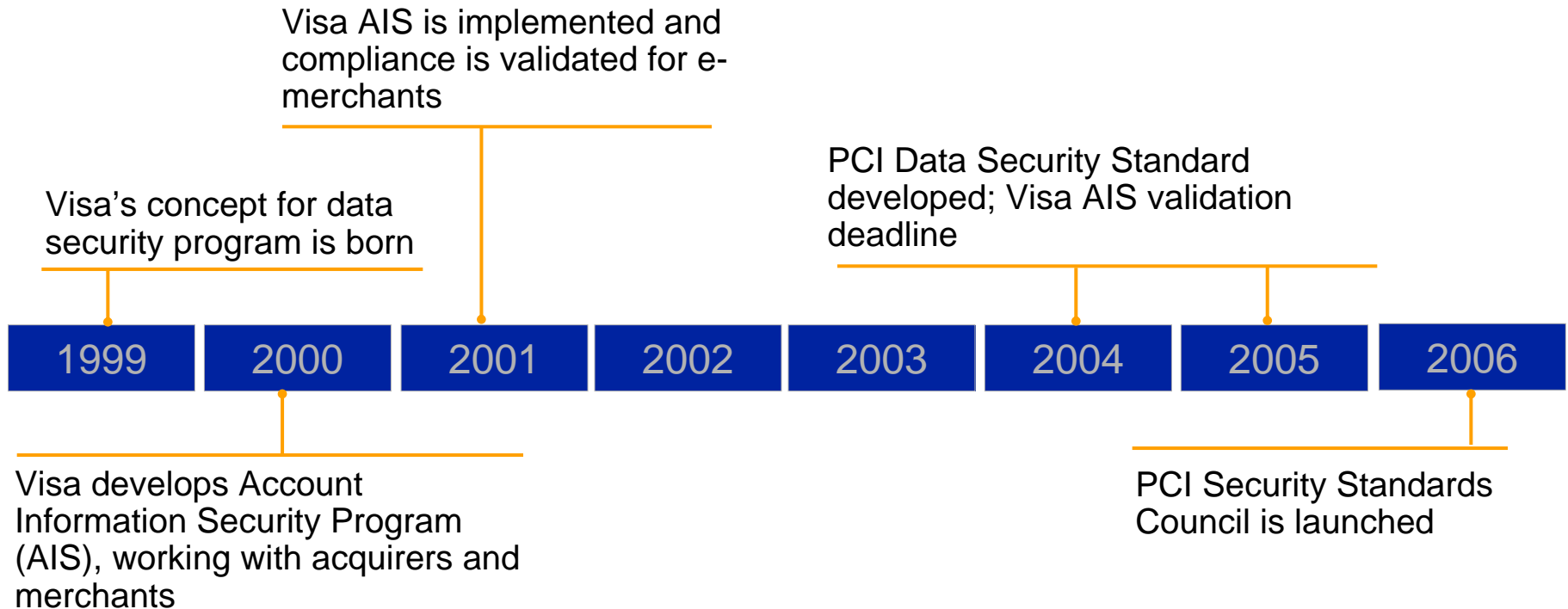




PCI DSS – Why it matters

Osman Inegol
Istanbul
15 April 2008

AIS Timeline





The importance of PCI DSS

This information is not intended, and should not be construed, as an offer to sell, or as a solicitation of an offer to purchase, any securities

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?

A simple equation




Data = identity = money

Your brand needs security!



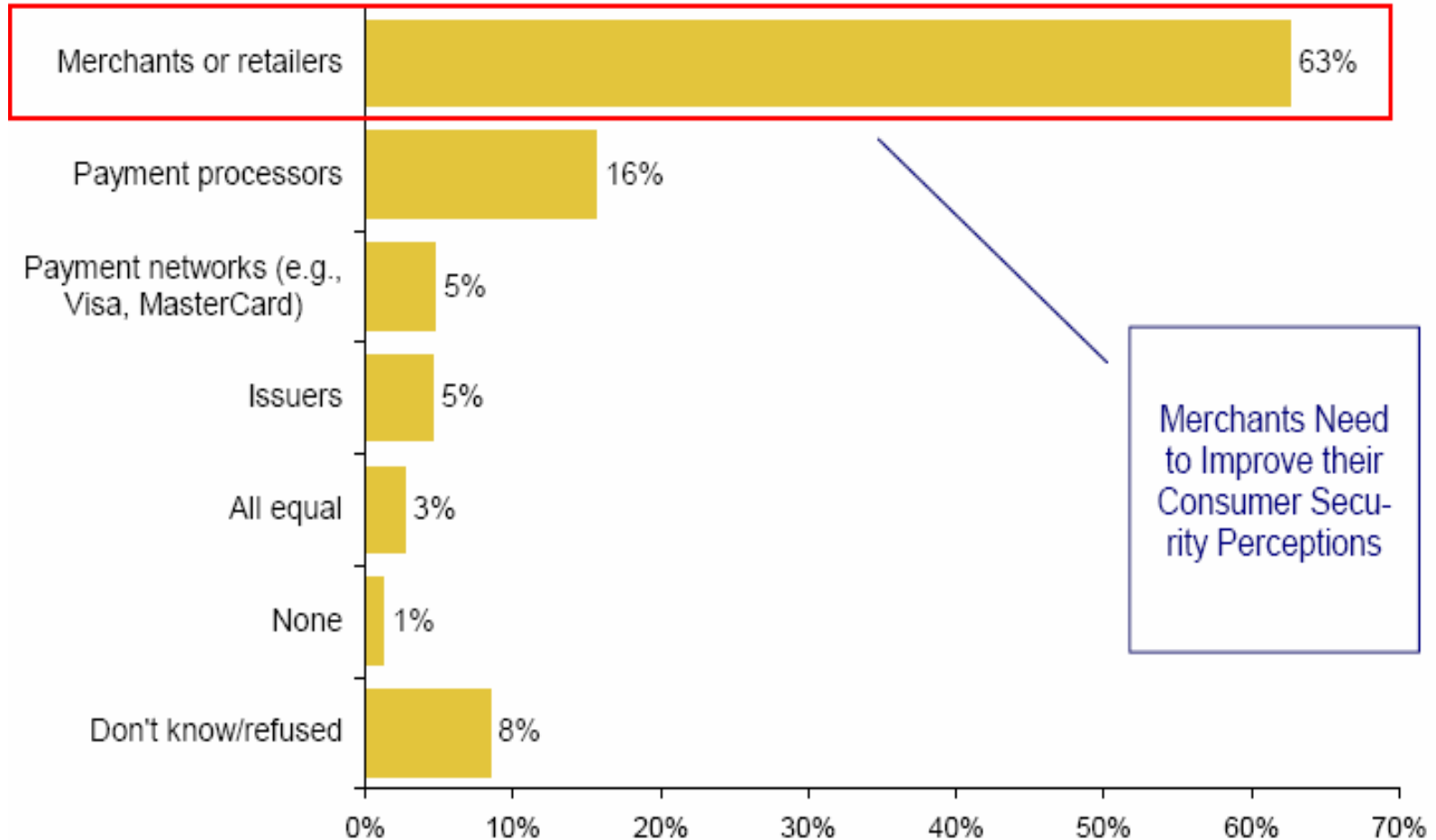
- Compromises do happen everyday, everywhere
- In the consumer's view, consumers, card schemes and merchants share responsibility for protecting their card data

A decorative graphic consisting of two overlapping curved shapes, one yellow and one blue, pointing towards the right.

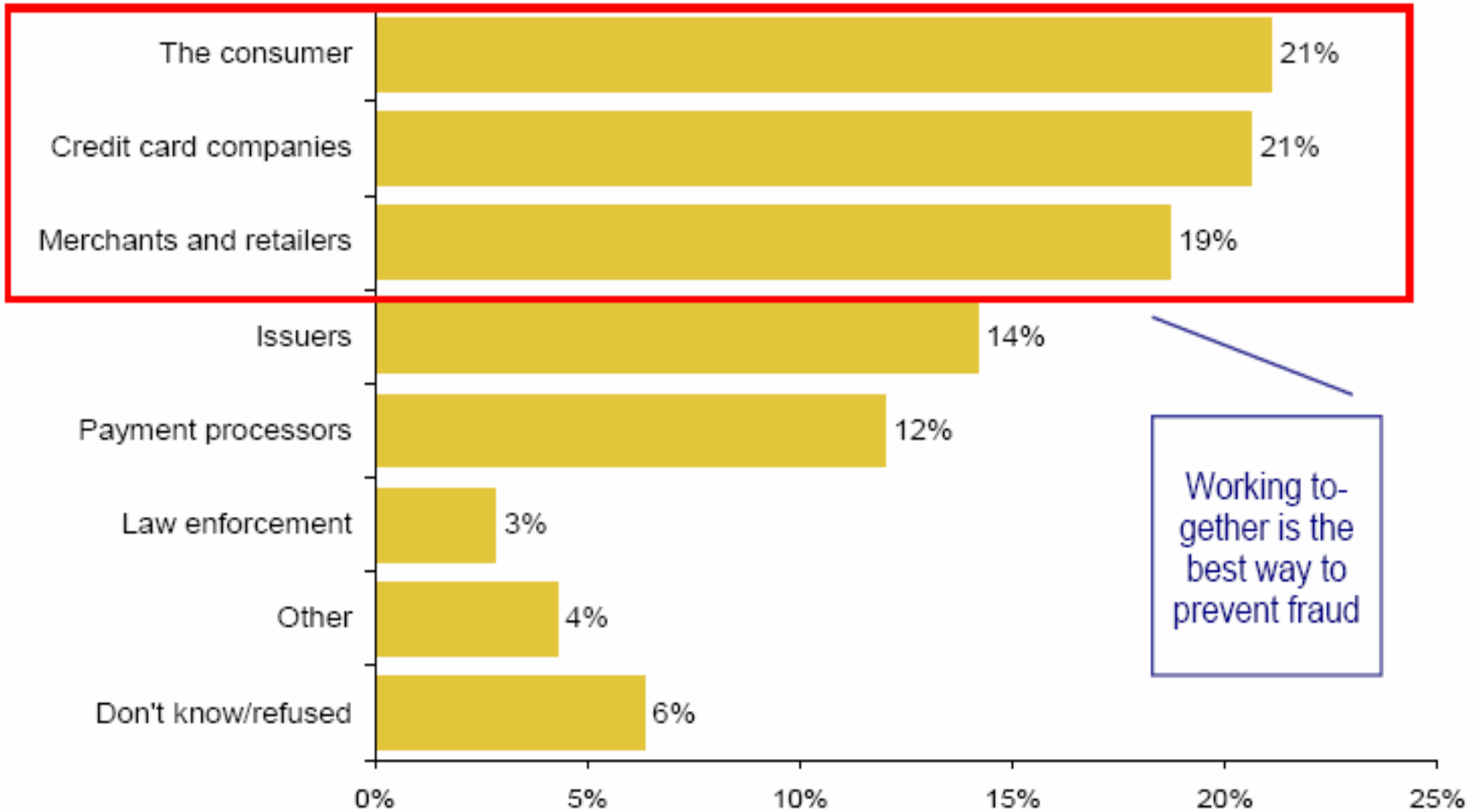
Yet... 63% of consumers views merchants as the weakest link when it comes to protecting their data...¹

¹Source: Javelin Strategy and Research 2007

Merchants as the weakest link



In consumers' eyes we all share responsibility to prevent fraud



Consumer confidence seriously impacted by a data breach



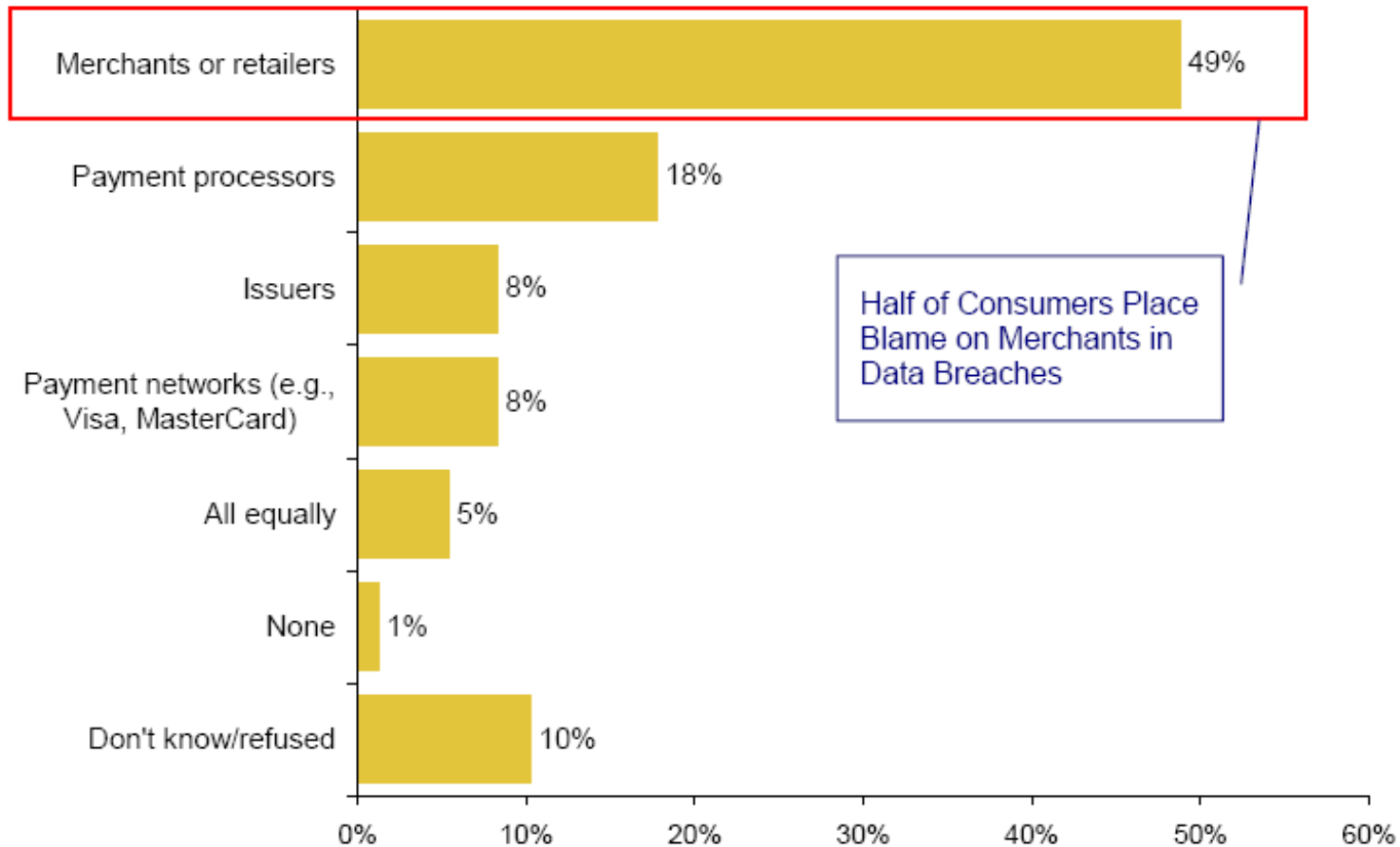
In the case of a breach....

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

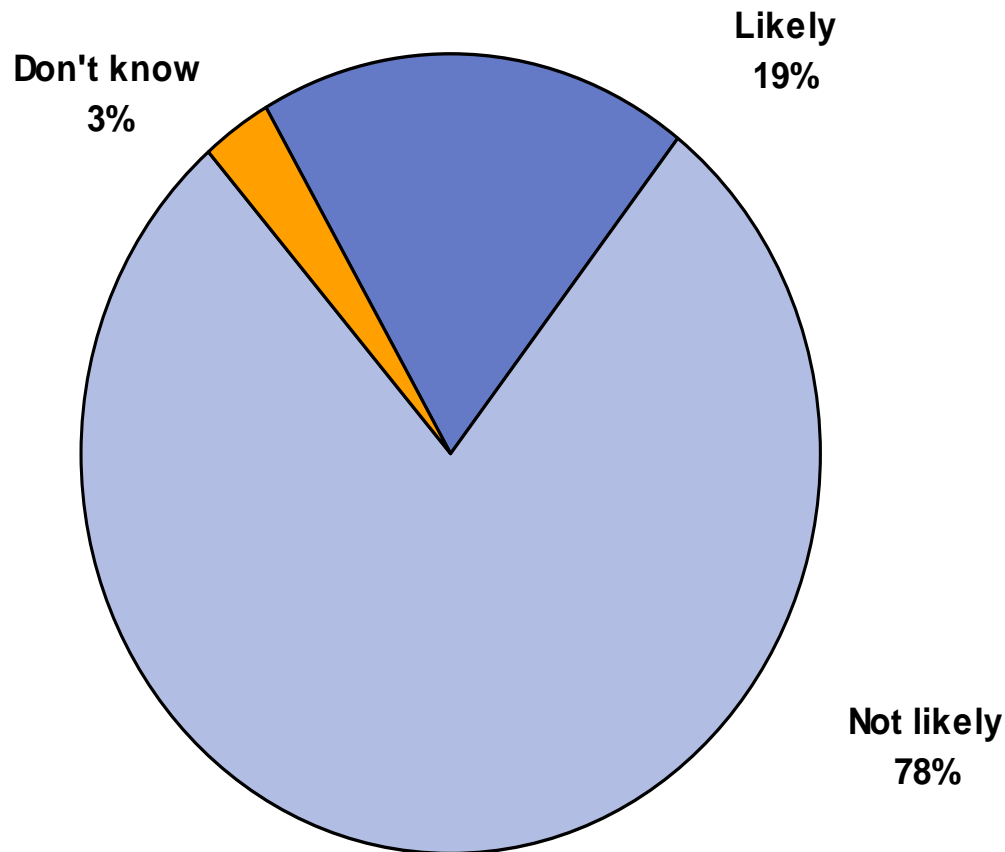
3 out of 4 consumers won't shop again at a compromised merchant

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

Consumers blame retailers for data breaches



3 out of 4 consumers will not shop again at compromised merchants



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.....

Over 80% of consumers are concerned about security when shopping online

How many of the UK's 27 million e-shoppers actually know a secure website when they see one?

As concern grows about the security of data, a survey conducted by UK managed hosting company NetBenefit reveals that over 80% of consumers are concerned over the security of their financial data when shopping online. Whilst approximately half of those surveyed said they would be prepared to spend up to £500 online, 70% of shoppers don't understand the significance of the green browser bar and 20% of those questioned do not understand what the golden security padlock represents.

Jonathan Robinson, Chief Operating Officer, NetBenefit says, “Secure website technology has been in place for some time now but it is staggering to find that so few consumers actually know how to make sure a website is secure. The industry has put standards in place to provide the online shopper with confidence but in actual fact many shoppers simply do not know what they are supposed to be looking for.”

With an estimated ecommerce spend of £84 million in the UK on Christmas Day alone, shopping online has never been more popular. However, NetBenefit is urging the UK's 27 million e-shoppers to ensure they shop 'e-safely' in 2008 by following a few simple guidelines.

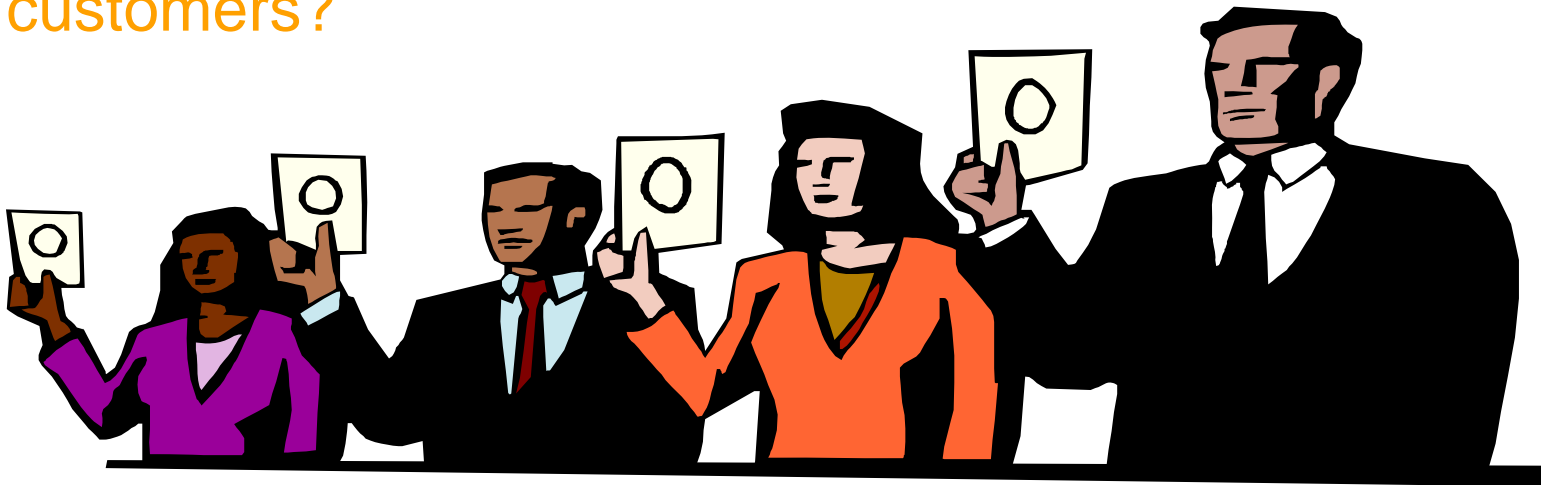
Security and your corporate social responsibility strategy



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



= €10,000,000¹

- +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

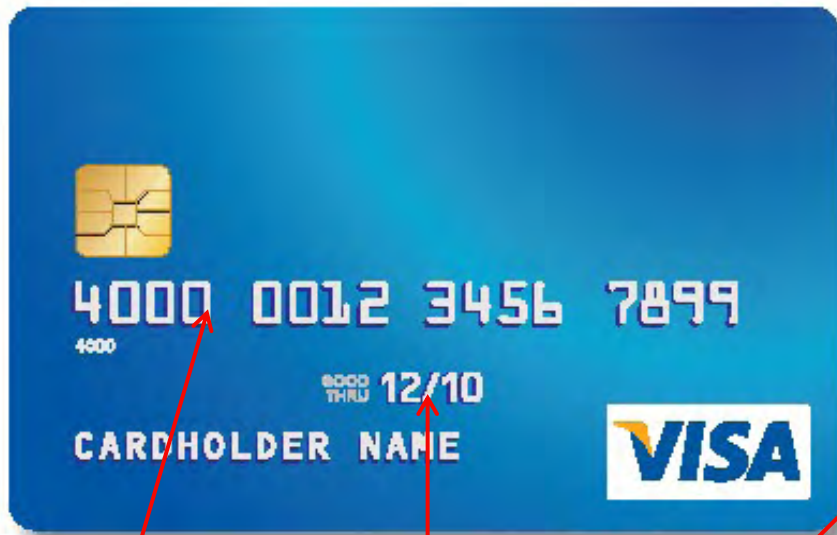
¹Figure is based on the average cost of containing a compromise based on research by the Ponemon Institute



Our goals

This information is not intended, and should not be construed, as an offer to sell, or as a solicitation of an offer to purchase, any securities

A Visa card...

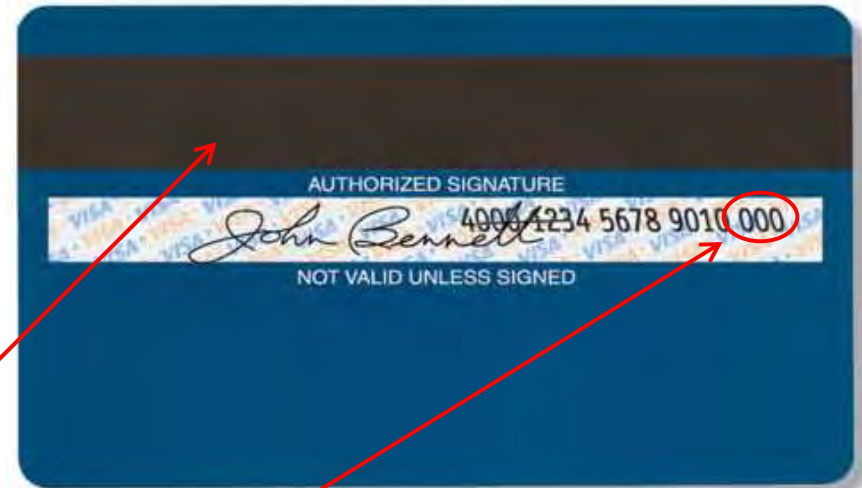


Card number

Expiry date

Magnetic Stripe

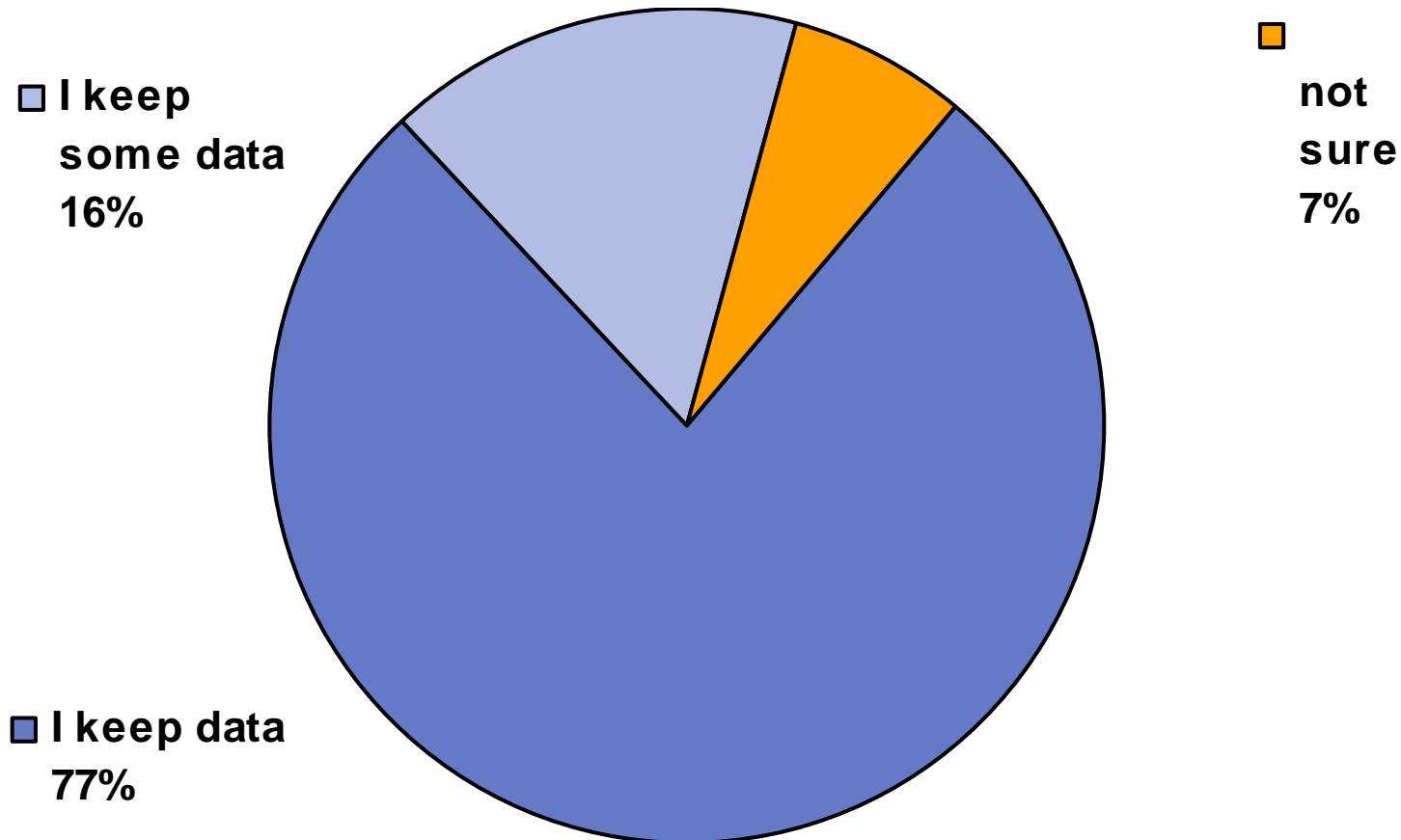
made up of “Track 1”
and Track 2” data



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

A fact – companies retain data after a transaction¹



¹Source: Visa Worldwide Services

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

Commons sense standards....



PCI Data Security Standard

Build and Maintain a Secure Network

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

Protect Cardholder Data

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

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



Our programme and its implementation

This information is not intended, and should not be construed, as an offer to sell, or as a solicitation of an offer to purchase, any securities

Merchant Validation requirements



| Level and criteria | Validation requirements |
|--|---|
| <p>Level 1: all channels</p> <p>Over 6,000,000 transactions a year</p> | <p><u>Mandated</u> annual onsite audit and quarterly network scan</p> <p><i>The audit can be done by a PCI DSS qualified auditor or by Merchant's internal audit team</i></p> |
| <p>Level 2: all channels</p> <p>1,000,000 to 6,000,000 transactions a year</p> | <p><u>Mandated</u> annual PCI Self-assessment questionnaire and quarterly network scan</p> |
| <p>Level 3: E-commerce</p> <p>20,000 to 1,000,000 transactions a year</p> | <p><u>Mandated</u> annual PCI Self-assessment questionnaire, and quarterly network scan</p> |
| <p>Level 4: all other merchants</p> | <p>Recommended annual PCI Self-assessment questionnaire, and annual network scan</p> |

The compliance framework in action – from commitment to compliance

-Level 1, 'OLD' Level 2 and Level 3:

- All merchants have to be at least 'committed'
 - 'Committed' merchants will be monitored through to compliance according to the timeframes indicated by the acquirer to Visa Europe.

- 'NEW' Level 2

- The deadline for merchants in this level to achieve full compliance is 31 December 2008.

Compliance vs. compliance validation



- These levels are validation guidance
- Compliance is mandated for everyone handling Visa cards
- In order to ensure you are compliant you need validation
 - **Regardless of level**
- Validation is not box-ticking
 - **The aim is reducing the risk to your system**

Merchant status definitions

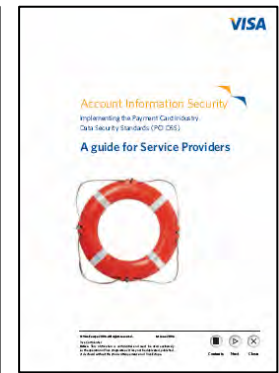


- **Non-compliant** – no progress
- **Preparing** – aware of requirements, doing gap analysis
- **Committed** – gap analysis completed and preparing remediation plan. Regular network scans with ASV. Signed up with QSA, or agreed internal audit with Acquirer.
- **In-progress** – implementing remediation plan and passing scans
- **Compliant**

Making PCI Compliance a Reality



- Visa provides the following guidance
 - Guides for Members, Merchants and Service Providers
 - Security Audit Procedures
 - Glossary
 - Self-Assessment Questionnaire
 - Security Scanning Procedures

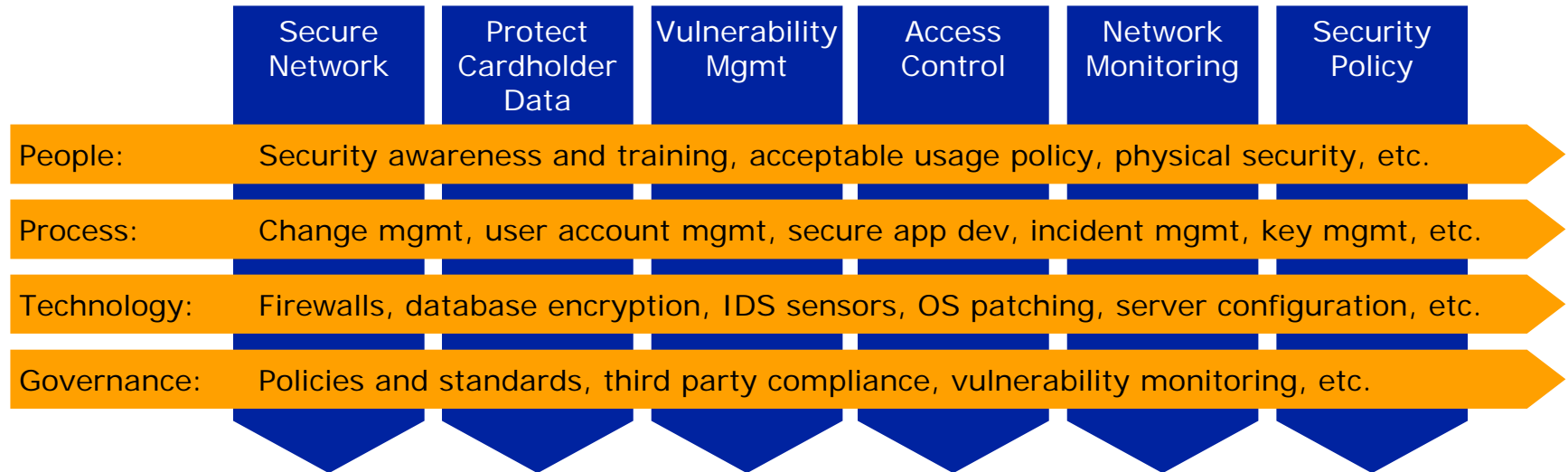


- Visa's recommended approach is
 - Complete data flow analysis early
 - Complete a comprehensive gap analysis
 - Define a detailed remediation plan



PCI DDS Project

High Level Approach



- Sponsorship is not always easy to assign given variety of stakeholders involved
- Some skill may be required to define the programme roadmap
 - translating control gaps into projects
 - prioritising projects
- Mobilising the programme may also require careful thought

- **It can be done!**
 - the large majority of UK/European merchants in your business segment are at least ‘committed’ to PCI DSS
 - An increasing number is ‘compliant’
- **Think creatively**
 - Think of ways of reducing the scope
 - No data+ no need for validation
- **Important things first**
 - Think risk mitigation – e.g remove Track/CVV2 as a priority

PCI DSS is part of doing business



- Critical mass is there
- Market leaders want to get there first
- Your business model requires high security
 - You are likely to be almost there already
- Think of PCI DSS as an investment in risk reduction



Thank you

<http://www.visaeurope.com/aboutvisa/security/ais/resourcesanddownloads.jsp>

This information is not intended, and should not be construed, as an offer to sell, or as a solicitation of an offer to purchase, any securities