PREPARING FOR PCI-DSS COMPLIANCE

Presenter:
Bob Brown
CISO | FirsTech & Busey

firstech

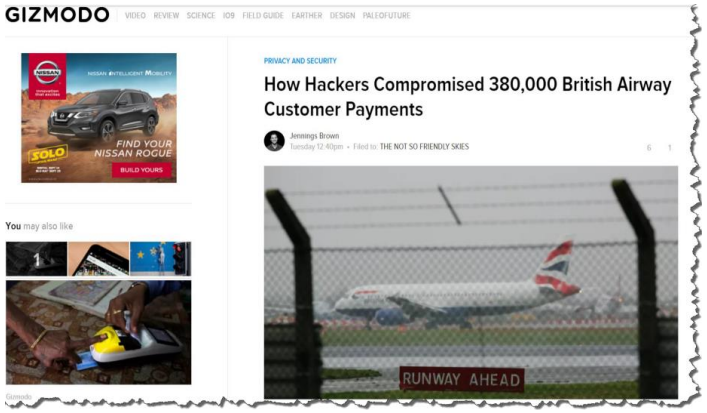
What Level Are You At?

	Level 1	Level 2	Level 3	Level 4
Level Qualifiers	• Greater than 6M credit card transactions per year • Any company that has been compromised	• Between 1-6M credit card transactions per year	• Between 20K and 1M e-commerce credit card transactions per year	• Less than 20K e-commerce credit card transactions per year • Less than 1M traditional credit card transactions
PCI DSS Requirements	• Annual on-site PCI Data Security Assessment • Quarterly external network vulnerability scans	• Annual PCI DSS Self-Assessment Questionnaire • Quarterly external network vulnerability scans	• Annual PCI DSS Self-Assessment Questionnaire • Quarterly external network vulnerability scans	• Annual PCI DSSS Self-Assessment Questionnaire • Quarterly external network vulnerability scans
To Be Validated By	• Qualified Security Assessor Internal Audit (with report signed by company officer) • Approved Scanning Vendor	• Merchant • Approved Scanning Vendor	• Merchant • Approved Scanning Vendor	• Merchant • Approved Scanning Vendor

AGENDA

- Industry Background
- Organizations Goals
- Organizational Challenges
- Strategies to Reduce Risks and Costs
- Q&A

Who’s Been Hacked Recently?



What's The Fine for Non-Compliance?

Duration	Level 1	Cumulative Level 1	Level 2	Cumulative Level 2
One to Three Months	• $10,000 Monthly	• $30,000	• $5,000 Monthly	• $15,000
Four to Six Months	• $50,000 Monthly	• $180,000	• $25,000 Monthly	• $90,000
Seven+ Months	• $100,000 Monthly	• $450,000	• $50,000 Monthly	• $240,000

Breach Consequences- Even if a company is 100% PCI compliant and validated, a breach in cardholder data may still occur. Cardholder Breaches can result in the following losses for a merchant.

- Suspension of credit card acceptance by a merchant's credit card account provider
- Loss of reputation with customers, suppliers, and partners
- Possible civil litigation from breached customers
- Loss of customer trust which effects future sales

Source: focusonpci.com/pci-concompliant-consequences

What's The Typical Cost Of A Breach?

(Not So) Fun Facts:

- Average Merchants, at time of compromise, were **NOT** compliant with 47% of PCI-DSS Requirements
- 39% of organizations were breached through insecure remote access
- Verizon's Forensic Team(10+yrs) have never found an organization fully compliant at the time of a breach

Source: 2018 IBM – Global Cost of a Data Breach Report

How's The Typical Cost Calculated?

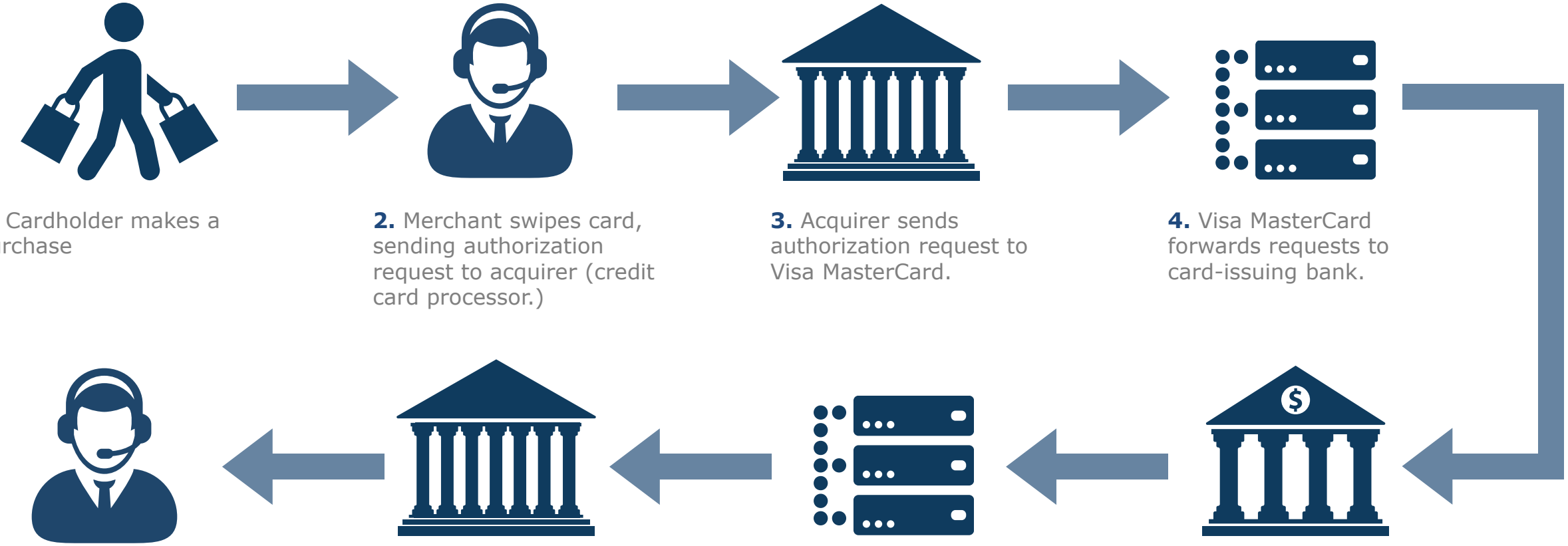
Discovery & Immediate Response:
- Forensics, Investigation
- Assessment of Impact
- Communication & PR Outreach
- Prep Notices
- Updated Call Center & Emp Training

Aftermath Activities:
- Audits, Consulting
- Legal Services, Defense & Compliance
- Discounts offered
- ID Protection Services
- Lost Customer Business
- Customer Acquisition

Final Analysis:
- Direct Costs: As, mostly, described above
- Indirect Costs: Amount of time, effort & org resources redirected
- Opportunity Costs:
  - Deflated Business Projects
  - Evaporated Business Initiatives
  - Revamped Marketing Efforts

Source: 2018 IBM – Global Cost of a Data Breach Report

Payment Ecosystem: Authorization Flow



1. Cardholder makes a purchase

2. Merchant swipes card, sending authorization request to acquirer (credit card processor.)

3. Acquirer sends authorization request to Visa MasterCard.

4. Visa MasterCard forwards requests to card-issuing bank.

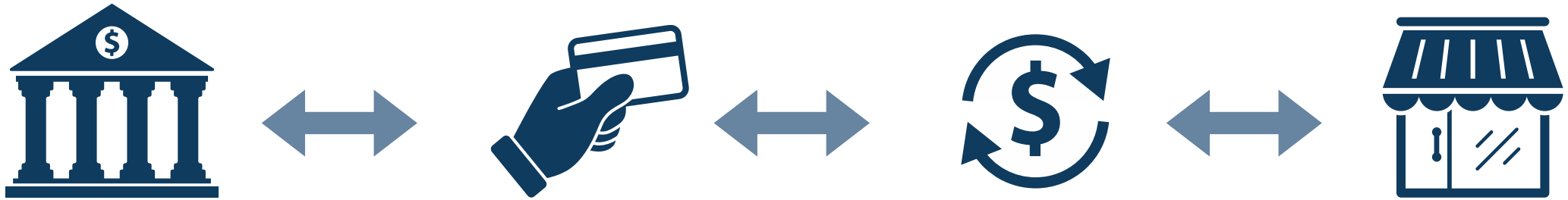
5. Issuer Bank sends response to Visa MasterCard.

6. Visa MasterCard forwards response to card-issuing bank.

7. Acquirer forwards response to merchant.

8. Merchant completes transaction.

Description of Roles & Relationships



Issuing Banks

- Issue credit and debit cards to cardholders
- Authorize payment transactions and settle with merchants
- Receive payments from card holders

Major Credit Card

- Each major brand has its own data protection program
- Oversees enforcement of PCI DSS compliance
- Issue fines to acquiring banks (acquirers & processors)

Acquiring Banks & Credit Card Processors

- Process payment card transactions
- Server as proxy for brands to enforce PCI DSS compliance
- Issue and collect fines from merchant & service providers
- **Service Providers**: Process, store or transmit payment card data on behalf of merchants

Merchant

- Classified as L1-L4 based on credit card transaction volume
- All merchant levels have to comply with the PCI DSS
- Validation procedures vary by merchant level
- **Service Providers**: Process, store or transmit payment card data on behalf of merchants
- **Assessor/Consultant:** Qualified Security Assessor Approved Scanning Vendors Third-party Consultants

Overview of PCI-DSS Categories

Build and Maintain a Secure Network 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplier defaults for system passwords and other security parameters	**Implement Strong Access Control Measures** 7. Restrict access to cardholder data bay business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Protect Cardholder Data 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks	**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 Vulnerability Management Program 5. Use and regularly update antirust software 6. Develop and maintain secure systems and applications	**Maintain an Information Security Policy** 12. Maintain a policy that addresses information security

Common Drivers for PCI-DSS Compliance

- Increased awareness and general concerns over data privacy
- Significant fines and penalties that can be imposed by credit card brands (including expulsion from programs)
- Potential reputation and brand damage, leading to loss of revenue
- Concerns over civil liability resulting from customer identity theft
- Industry peer pressure
- Alignment with corporate risk management guidelines

Why Companies Struggle to Comply?

- View compliance as “an IT problem”
- Lacking a clear definition of payment environment that is in scope for PCI DSS certification
- Underestimating the extent and complexity of PCI DSS compliance
- Controlling logical access to systems containing payment card data
- Logging and monitoring events
- Protecting stored payment card data
- Putting PCI DSS contractual language in place for third-party service providers
- Obtaining management support for scalable remediation solutions
- Taking siloed approach to compliance
- Placing too much reliance on the QSA

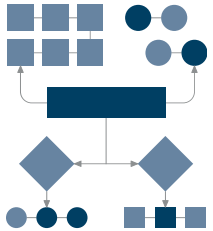
An Approach to Attaining PCI-DSS Compliance

- Define the relevant in-scope environment
- Assess risks without this environment using the PCI DSS as a controls framework
- Remediate identified vulnerabilities according to risk prioritization
- Assist in implementation of a program to maintain the controls framework and facilitate certification on an ongoing basis (analogous to implementation of an information security management system for an ISO 27001 certification).

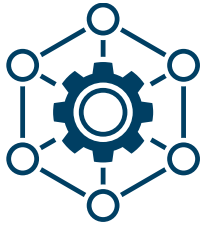
5 Strategies for Reducing the Risk & Cost of Compliance

Reduce or eliminate the user of payment card data

Purge payment card data



Redesign the payment environment



Outsource payment processing

Consolidate and centralize

THANK YOU!