Securing The Data

Payment System Forum
Bank Negara Malaysia
27th November 2014

Murugesh Krishnan
Head of Risk, South & Southeast Asia

Disclaimer

Case studies, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. You should consult with your legal counsel to determine what laws and regulations may apply to your circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Forward Looking Statements Disclaimer

These presentations contain forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. These statements can be identified by the terms “objective,” “goal,” “strategy,” “opportunities,” “continue," “can,” "will" and similar references to the future. Examples of such forward-looking statements include, but are not limited to, statements we make about our corporate strategy and product results, goals, plans and objectives. By their nature, forward-looking statements: (i) speak only as of the date they are made, (ii) are neither statements of historical fact nor guarantees of future performance and (iii) are subject to risks, uncertainties, assumptions and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors, including: the impact of new laws, regulations and marketplace barriers; developments in litigation or government enforcement; economic factors; industry developments; system developments; loss of organizational effectiveness or key employees; failure to effectively develop products and businesses; Visa Europe’s exercise of their put option, and the other factors discussed in our most recent Annual Report on Form 10-K filed with the U.S. Securities and Exchange Commission. You should not place undue reliance on such statements.

Data Breach - a case study

Source: New York Times, March 25, 2010

Overview
Millions of card data breached by an international identity theft ring

Vulnerabilities
Insecure domain controls, malware & inadequate monitoring

Fraudulent Use
Fraudulent transactions, reselling of cardholder data

*All brand names and logos are the property of their respective owners, are used for identification purposes only, and do not imply product endorsement or affiliation with Visa.

Data Breach – continues in 2014

Overview
High profile merchant data breaches, reported by respective companies, including card account and other personal information

Vulnerabilities
Potentially insecure domain controls, malware & inadequate monitoring

Fraudulent Use
Fraudulent transactions, reselling of cardholder data

Data Breach – issues in Southeast Asia

PART B HOME MONEY SPORT

HOME

THE STRAITS TIMES
FRIDAY, JULY 20, 2012

B1

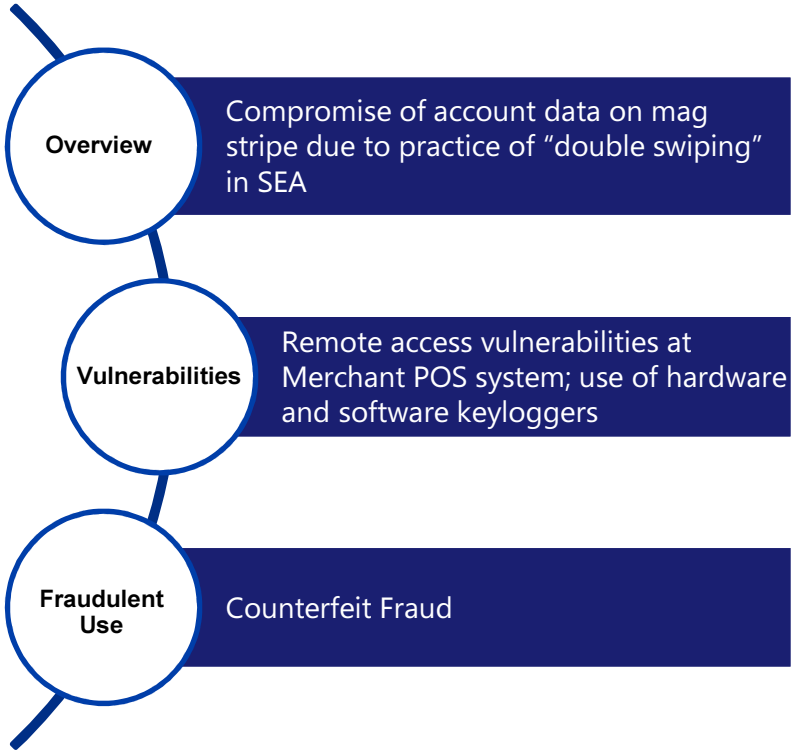
B12 Block party: Dressing up for National Day B4 Photographer gives back to the arts

BANKS TELL RETAILERS:
NO DOUBLE SWIPING

SCARY SWIPES
It makes me afraid if a merchant swipes too many times. It is so easy to skim personal data off the magnetic stripe on cards for illegal withdrawals.
– Restaurant owner Jeremy Reynolds

Merchants typically swipe customers' credit cards on their cash tills even after a transaction has been approved. This leads to card data being stored in the tills. PHOTO: LIOU VINODY JR FOR THE STRAITS TIMES

Practice compromises card security



Multi-Layered Approach To Mitigate Risk

Data Devaluation

Data Security

Fraud Prevention

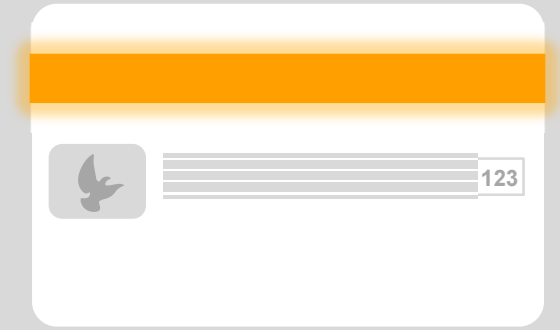
Breach Response

What Data is Sensitive?

4 0 0 0 1 2 3 4 5 6 7 ^ S I E W N E E ^ 0 1 2 0 1 2 ^ 1 0 1 ^ 2 1 7 ^...

Card Number | Name | Expiry | Service Code | CVV

Magnetic Stripe Data is Static



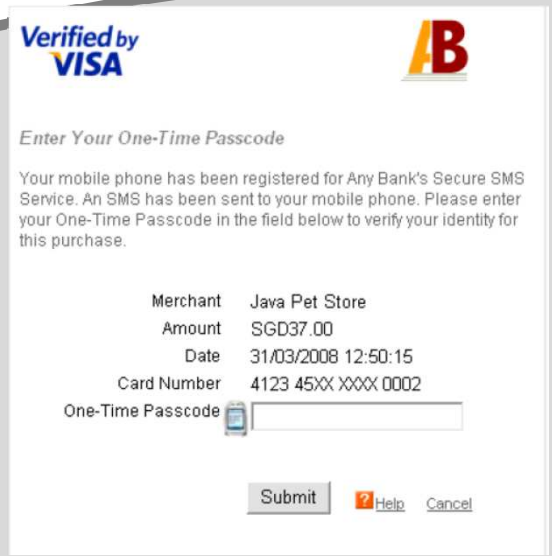
EMV Chip Mitigates Fraud

Chip Generates Dynamic Data

What Data is Sensitive - Ecommerce

Payment Page – Account Number, Expiration Date, CVV2

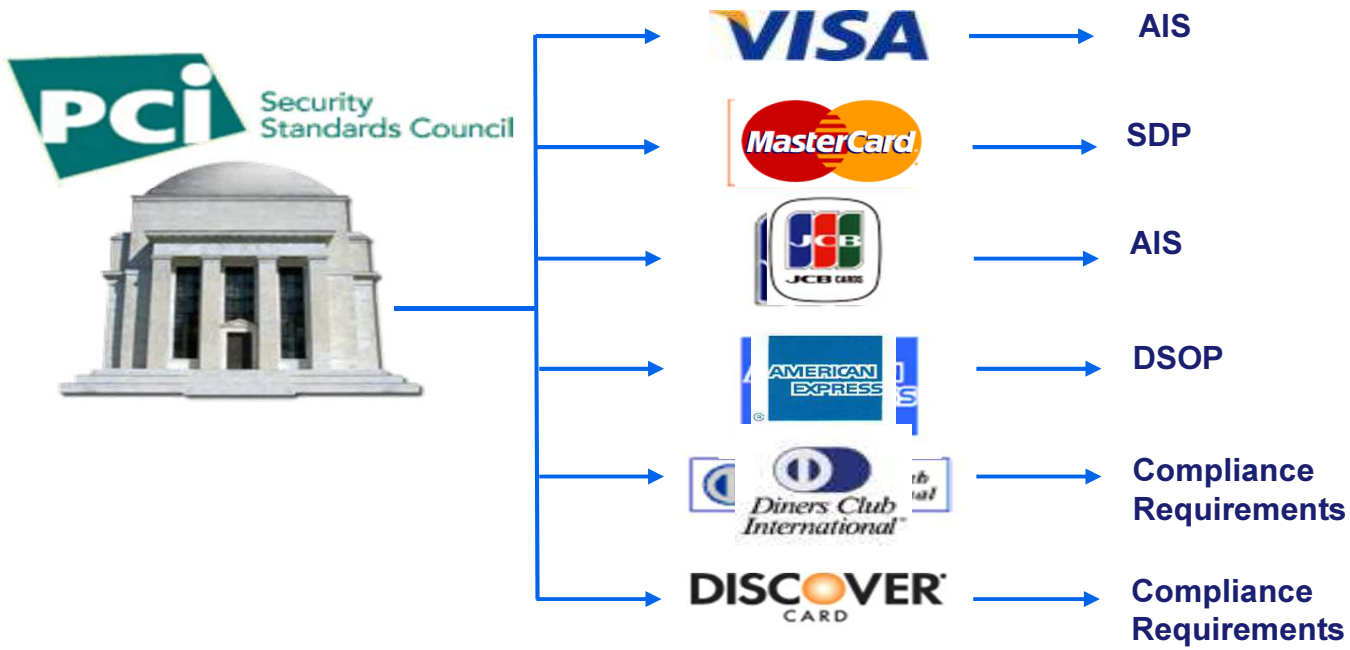
Dynamic Data



- PCISSC established in response to industry call for a common standard
- Founded in Sep 2006 by Visa, MCI, Amex, JCB, Discover
- Move ownership to industry
  - Executive Council
  - Board of Advisor (~40 companies from industry)
  - Focus/Advisory Groups
- Manages
  - Data Security Standards
  - Accreditation (QSAs, PA-QSAs, ASVs, ISAs, PFIs)
  - Awareness programs

PAYMENT CARD INDUSTRY SECURITY STANDARDS

PCI DSS – Role & Responsbility



PCI Data Security Standard

The PCI DSS is a set of comprehensive requirements for enhancing payment account data security. It represents common sense steps that mirror security best practices.

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder 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 for all personnel

PCI DSS - applicability

- Entities that **process**, **store** and/or **transmit** cardholder data

Merchants

Service Providers

Banks

Merchants

PCIDSS - Definitions

- Self Assessment Questionnaire - SAQ
  - ~400 test points or questions
  - Five versions available to simplify assessment for various merchant needs
- Report of Compliance – ROC (completed by QSA)
- Attestation of Compliance - AOC (issued by QSA)
- Approved Scanning Vendor - ASV
  - Non-intrusive vulnerability scan at Internet facing Ports/Access

Merchants – Four Groups

Level	Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels)	• Annual Report on Compliance by QSA • Quarterly network scan by ASV • Attestation of Compliance Form
2	Merchants processing 1 – 6 million Visa transactions annually (all channels)	• Annual SAQ • Quarterly network scan by ASV • Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million Visa **e-commerce** transactions annually	• Annual SAQ • Quarterly network scan by ASV • Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa **e-commerce** transactions annually and **all other merchants** processing up to 1 million Visa transactions annually	• Annual SAQ **recommended** • Quarterly network scan by ASV if applicable • **Compliance validation requirements set by acquirer**

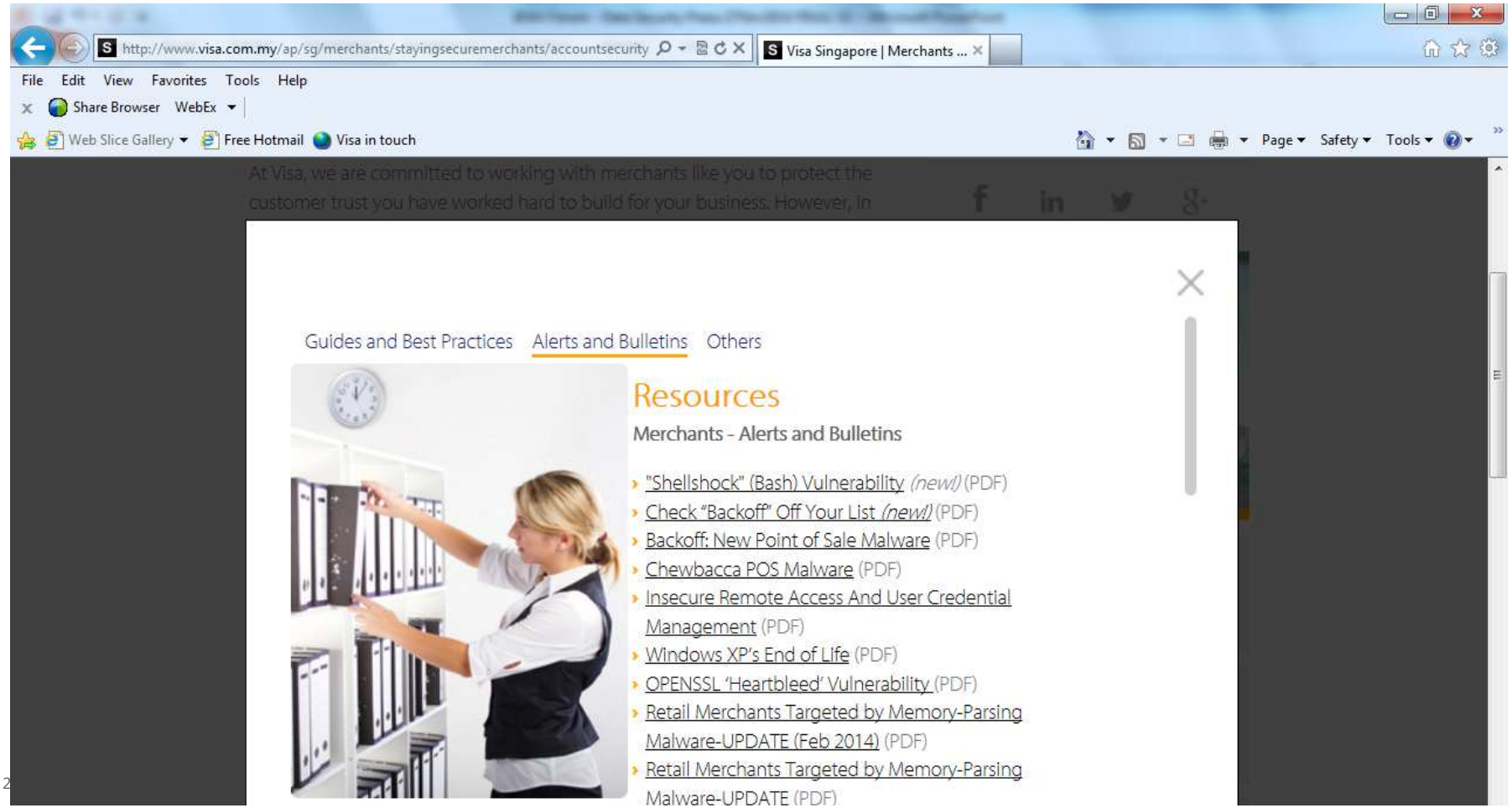
Payment applications

Payment Application Data Security Standard (PA-DSS)

- PA-DSS is a set of requirements derived from PCI Data Security Standards (PCI DSS)
- PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment application are sold, distributed, or licensed to third parties
- This includes payment applications that are typically sold and installed "off the shelf"
- List of validated payment applications can be found at www.pcisecuritystandards.org/security_standards/vpa

www.visa-asia.com

www.visa-asia.com



PCISSC Website

- PCI Security Standards Council (PCI SSC)
www.pcisecuritystandards.org

- PCI DSS
www.pcisecuritystandards.org/security_standards/pci_dss.shtml

- PA DSS
www.pcisecuritystandards.org/security_standards/pa_dss.shtml

- PCI DSS Prioritized Approach
www.pcisecuritystandards.org/security_standards/documents.php

- List of Validated Payment Applications
www.pcisecuritystandards.org/security_standards/vpa/

Summary

- Review Your Card Acceptance Practices
  - Do Not "Double Swipe"

- PCIDSS is a Useful Framework for All Merchants
  - Stand-alone device
  - Integrated-POS Device
  - Self Service Devices (Auto Fuel Dispenser, Payment Kiosks)
  - Ecommerce & Mobile Commerce

- Verify/Register Third Party Agents (Merchant Servicers)

- Stay Informed (Consult Your Bank, PCISSC & Card Scheme websites)