



# Risk-based Approach to PCI DSS Validation

Ingo Noka  
Regional Head, Data Security & ERM

25 June 2009



# PCI SSC risk prioritized roadmap



## Milestone One

- Remove sensitive authentication data and limit data retention

## Milestone Two

- Protect the perimeter, internal and wireless networks

## Milestone Three

- Secure applications

## Milestone Four

- Protect the cardholder data environment

## Milestone Five

- Protect stored cardholder data

## Milestone Six

- Finalize all the policies, procedures and processes needed to protect the cardholder data environment

# Risk-based PCI DSS validation



Visa announced the risk-based approach to PCI DSS validation in May 2009 via IML 13/09

## Objectives:

- Promote secure payments through multiple layers of security
- Recognise investments made in risk control measures such as chip technology and encryption
- Help merchants better manage risk and comply with annual validation requirements
- Drive chip migration and end-to-end encryption

# Eligibility



MERCHANTS that have implemented

- End-to-end encryption

OR

- Process EMV chip transactions in countries and territories where iCVV penetration is at least 75 percent

# End-to-end encryption



Sensitive account data is encrypted at the point of entry

- Magnetic stripe reader
- Chip reader
- Key entry (MO/TO)

# End-to-end encryption



encrypted data



encrypted data



encrypted data

No decryption of data here



Merchant Host or Service Provider

encrypted data



Acquirer

# What is a chip transaction?



1. Transaction from a chip card processed by chip-enabled terminal by reading the cardholder data from the magnetic stripe
  2. Transaction from a chip card processed by chip-enabled terminal by reading the cardholder data from the chip
  3. Transaction from a chip card processed by magnetic stripe terminal
  4. Transaction from a magnetic stripe card processed by chip-enabled terminal
- 1 and 2
  - 1 only
  - 2 only
  - 1, 2 and 3
  - All of the above
  - None of the above

# Risk-based PCI DSS validation



	Not compliant	Milestones 1-4 complete	Milestones 1-6 complete
End-to-end encryption or Chip*	<p><b>Fine</b></p> <p>Liability for data compromise losses**</p>	<p><b>No Fine</b></p> <p>Liability for data compromise losses**</p>	<p><b>No Fine</b></p> <p>Liability for data compromise losses**</p>
<u>No</u> End-to-end encryption or Chip*		<p><b>Fine</b></p> <p>Liability for data compromise losses**</p>	

\* In countries and territories with more than 75 percent iCVV penetration

\*\* if found non compliant **at the time of the breach**

# Merchant level reduction



Merchants that

- Have attested to not storing prohibited data
- Process EMV chip transactions in markets where iCVV penetration is at least 75 percent

May EXCLUDE chip transactions from their overall annual transaction volume

But their validation level can only be reduced by ONE level from the original validation level (e.g., from Level 1 to Level 3 or 4 is not allowed)

# Resources



## AIS

- [www.visa-asia.com/secured](http://www.visa-asia.com/secured)
- [www.visa-asia.com/padss](http://www.visa-asia.com/padss)
- [vpssais@visa.com](mailto:vpssais@visa.com)

## Registry of Service Providers

- [www.visa-asia.com/spregistry](http://www.visa-asia.com/spregistry)
- [apsregistry@visa.com](mailto:apsregistry@visa.com)

## PCI DSS

- [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

