



# Global PCI DSS Framework

Emöke Bitter

Business Leader, Risk Management

26 February 2009

# Agenda



## Introduction

Merchants

Service Providers

Registry of Service Providers

Payment Applications


Resources

# Introduction



Account Information Security, or AIS, is a globally mandated program for all Visa clients, their agents and merchants that process, store and/or transmit cardholder data.

In November 2008, International Member Letter (IML) 28/08 was issued to inform Visa clients on the new global PCI DSS framework which affects the AIS validation and reporting requirements.

A decorative graphic consisting of two overlapping, curved shapes. The top shape is yellow and the bottom shape is blue, both pointing towards the right.

The AIS program aims to protect the interests of all parties involved in the Visa payment system in both the physical and virtual worlds



In the US, the AIS program is known as Cardholder Information Security Program (CISP)

# Merchants



All merchants fall into one of the four merchant levels based on Visa transaction volume over a 12-month period.

Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) from a merchant.

In cases where a merchant corporation has more than one Doing Business As (DBA), acquirers must consider the aggregate volume of transactions by the corporate entity to determine the validation level.



# Merchants – Levels & Requirements



Level / Tier <sup>1</sup>	All Regions	Validation Requirements
1	Merchants processing over <b>6 million</b> Visa transactions annually (all channels) <b>or</b> Global merchants identified as L1 by any Visa region <sup>2</sup>	<ul style="list-style-type: none"> <li>• Annual Onsite Review by QSA</li> <li>• Quarterly network scan by Approved Scanning Vendor (ASV)</li> </ul>
2	Merchants processing <b>1 million to 6 million</b> Visa transactions annually (all channels)	<ul style="list-style-type: none"> <li>• Annual completion of PCI DSS SAQ</li> <li>• Quarterly network scan by ASV</li> </ul>
3	Merchants processing <b>20,000 to 1 million</b> Visa <b>e-commerce</b> transactions annually	<ul style="list-style-type: none"> <li>• Annual completion of PCI DSS SAQ</li> <li>• Quarterly network scan by ASV</li> </ul>
4	Merchants processing <b>less than 20,000</b> Visa <b>e-commerce</b> transactions annually and all other merchants processing <b>up to 1 million</b> Visa transactions annually	<ul style="list-style-type: none"> <li>• Annual completion of SAQ recommended</li> <li>• Quarterly network scan by ASV if applicable</li> <li>• Compliance validation requirements set by acquirer</li> </ul>

<sup>1</sup> Compromised entities may be escalated at regional discretion.

<sup>2</sup> Merchant meeting level 1 criteria in any Visa country/region that operates in more than one country/region is considered a global Level 1 merchant. Exceptions may apply to global merchants if no common infrastructure and if Visa data is not aggregated across borders; in such cases merchant validates according to regional levels.

# Merchants – Compliance Deadlines



## 30 September 2009

**L1** and **L2** Merchants: No storage of prohibited data

## 30 September 2010

**L1** Merchants: PCI DSS compliant



Prohibited Data = Full track data; CAV2/CVC2/CVV2/CID; PIN/PIN block

# Merchants – Reporting Requirements



Acquirers must report to Visa twice a year (31st of March and 30th of September) the following:

- Compliance status of each Level 1 merchant
- Compliance status of each Level 2 merchant
- Statistical reporting metrics of the compliance status of Level 3 merchants

First reporting date: **31 March 2009**

# Merchants – Bi-Annual Report



## Merchant PCI DSS Compliance Report

Acquirer name:	
BID:	
Completed by:	
Signature:	
Title:	
Telephone #:	
E-mail address:	
Date:	

This document must be completed to demonstrate compliance status with the Payment Card Industry Data Security Standard (PCI DSS) Regulations requirement prohibiting the storage of sensitive cardholder account authentication information beyond authorization.

Acquirers must identify all level 1 and 2 merchants and include them in this report.

Acquirers must obtain validation documentation from their merchants including Report on Compliance, Attestation of Compliance for O Quarterly Scan Results and Self-assessment Questionnaire, and submit to Visa if requested.

Initial Identification Year	Merchant Name	Merchant Level	Compliance Status	Self Assessment Validation Date (DD/MM/YYYY)	Quarterly Network Scan Validation Dates (DD/MM/YYYY)	Date of Onsite Review by QSA or Merchant Internal Auditor (DD/MM/YYYY)	Prohibited Data Storage (e.g., track, CVV2, PIN Block)	Prohibited Data Identification Date (DD/MM/YYYY)

## Merchant PCI DSS Compliance Report

BID:	
Completed by:	
Signature:	
Title:	
E-mail address:	
Date:	

Period	Total # of Level 3 Merchants	Total # of Compliant Level 3 Merchants	% of Compliant	Total # of Remediating	Total # of Validation in Progress	Total # of Pending Commitment
31-Mar-09						
30-Sep-09						

**Legend:**  
 Compliant = ROC complete confirming PCI compliance  
 Remediating = Initial ROC complete; Remediating findings  
 In Progress = Initial ROC in progress, QSA has been engaged, Audit ongoing  
 Pending Commitment = Merchant identified; No commitment to validate

# Service Providers



Visa clients are required to register their relationship with all their service providers via Exhibit 5E (and Exhibit 5A if the service provider is directly connected to VisaNet via a VisaNet Extended Access Server) to the Agent Registration team at [apsgpagent@visa.com](mailto:apsgpagent@visa.com).

Those that store, transmit and/or process Visa cardholder data are required to be PCI DSS compliant and are automatically enrolled in the AIS program.

# Service Providers – Validation Requirements



	LEVEL 1 More than 300,000 Visa transactions* per year	LEVEL 2 Less than 300,000 Visa transactions* per year
PCI DSS onsite review	<b>Mandated</b>	<b>Recommended</b>
Quarterly network scan	<b>Mandated</b>	<b>Mandated</b>
Self assessment questionnaire (SAQ)	<b>Optional</b>	<b>Mandated</b>


*\* includes all transactions (for all clients), regardless of the type / channel*

# Service Providers – Reporting Requirements



## LEVEL 1

- Attestation of Compliance form (Appendix E of PCI DSS Requirements and Security Assessment Procedures v1.2)
- Executive summary and description of scope of work and approach taken from the ROC. The complete ROC is not required.

A decorative graphic consisting of two overlapping curved shapes, one yellow and one blue, positioned to the left of the text.

Clients are responsible to submit attestations to Visa on an annual basis for all their service providers.

Visa no longer notify clients in advance.

## LEVEL 2

- Completed PCI DSS Self-Assessment Questionnaire (SAQ)

# Registry of Service Providers



- New optional program for service providers to register directly with Visa and report PCI DSS compliance
- Clients not required to submit annual attestations to Visa if the service provider has registered under this program
- Only service providers that have been reported as PCI DSS compliant via an onsite review by a QSA are listed on the Registry



# Payment Applications



## Payment Application Data Security Standard (PA-DSS)

- PA-DSS is a set of requirements derived from PCI Data Security Standards (PCI DSS), developed to validate payment software / applications
- Safe applications implemented in a PCI DSS compliant environment will minimize the potential for security breaches leading to data compromises
- More information can be obtained at [https://www.pcisecuritystandards.org/security\\_standards/pa\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml)

A decorative graphic consisting of two overlapping, curved shapes. The top shape is yellow and the bottom shape is blue, both pointing towards the right.

Payment applications can store data without the merchant's knowledge

# 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)

## Third-Party Agent Registration

- [apsgpagent@visa.com](mailto:apsgpagent@visa.com)

## PCI DSS

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





**Thank You**

