



Sense of Security Pty Ltd  
(ABN 14 098 237 908)  
306, 66 King St  
Sydney NSW 2000  
Australia

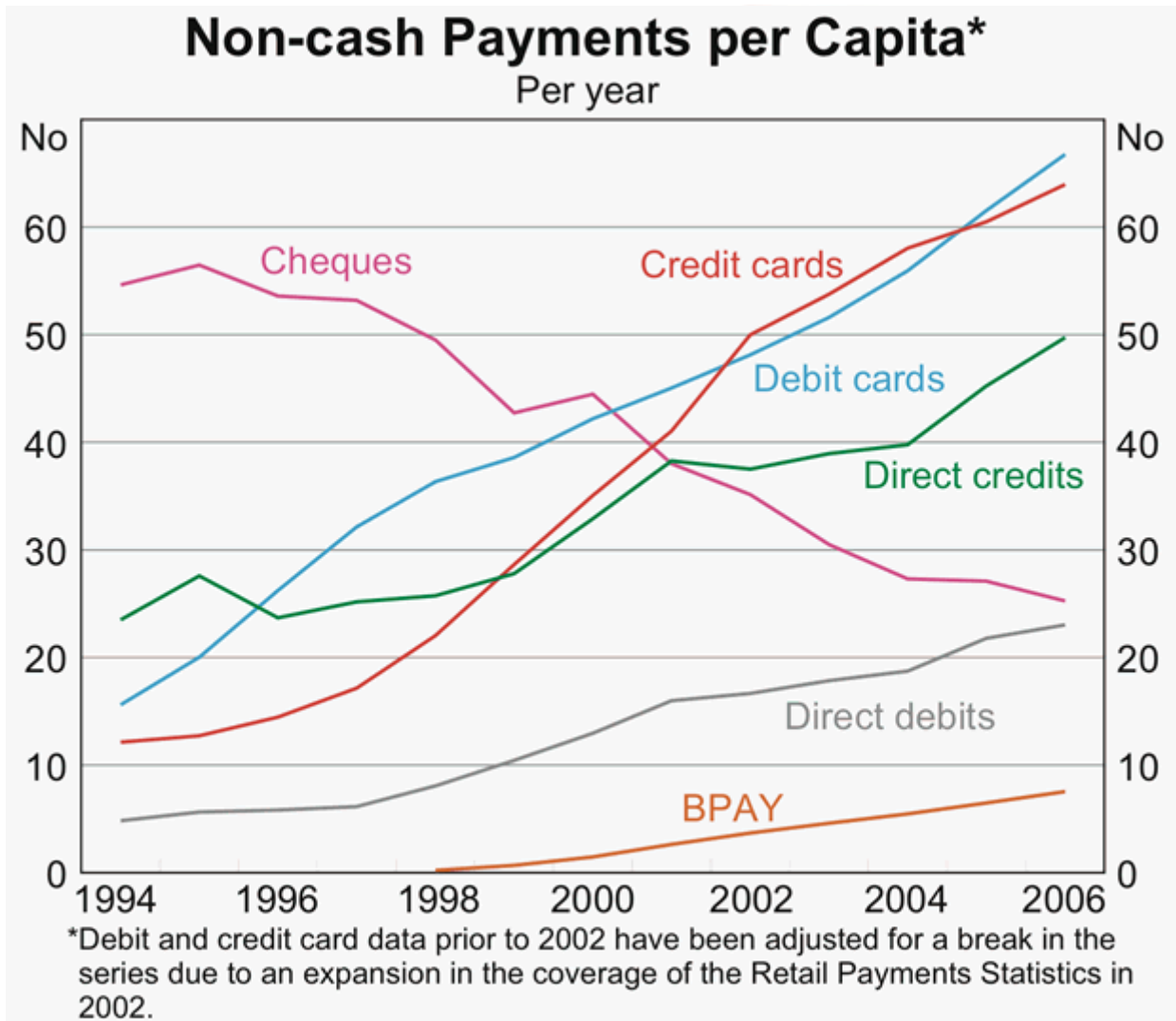
Tel: +61 (0)2 9290 4444  
Fax: +61 (0)2 9290 4455  
[info@senseofsecurity.com.au](mailto:info@senseofsecurity.com.au)

# PCI Compliance : What does this mean for the Australian Market Place?

Nov 2007

- Overview of PCI DSS
- Merchant Compliance Levels and Associated Compliance Requirements
- Risks and consequences of non-compliance
- Benefits of Compliance
- Current status of PCI in Australia

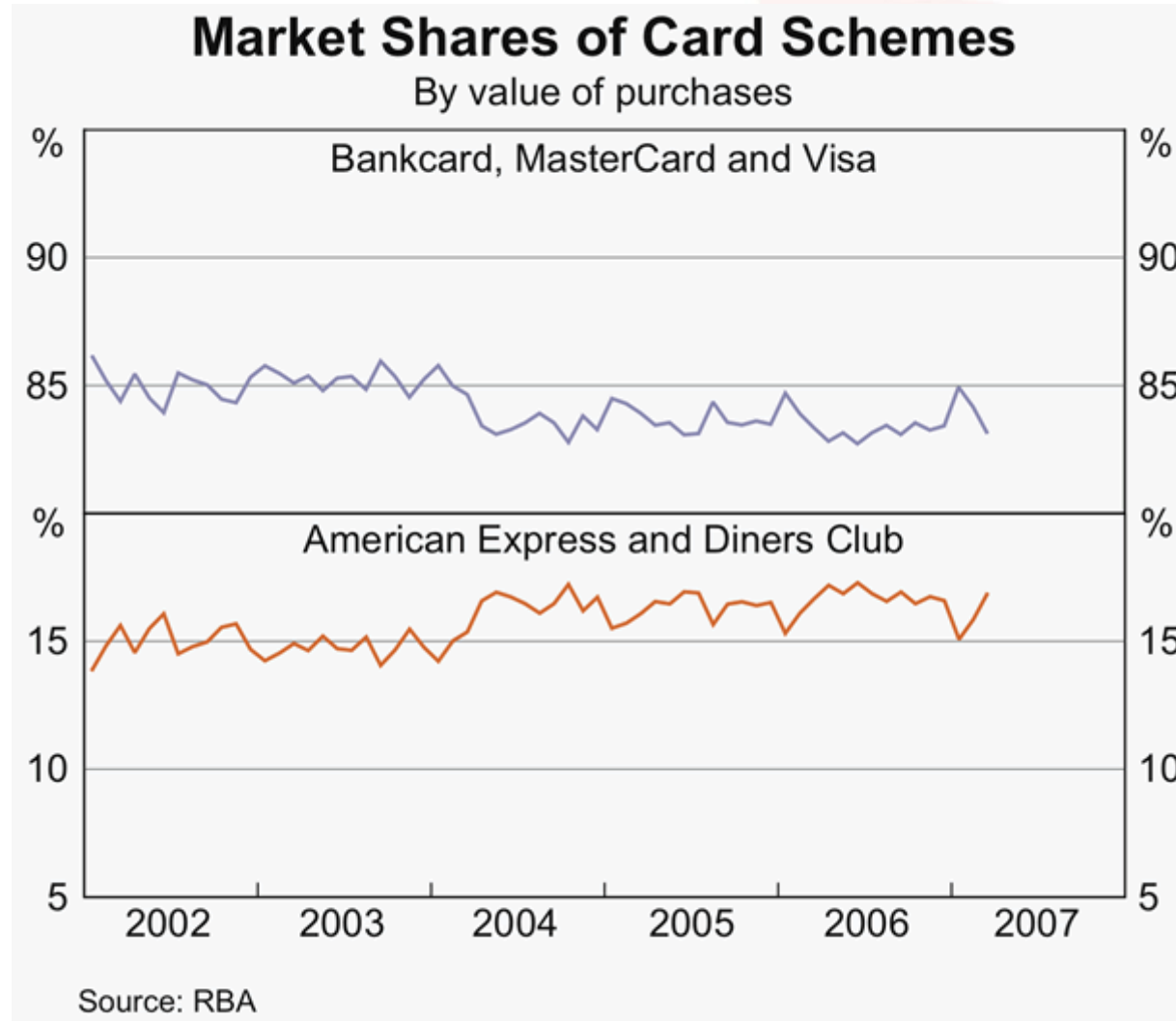
# Payment Card transactions - on the increase



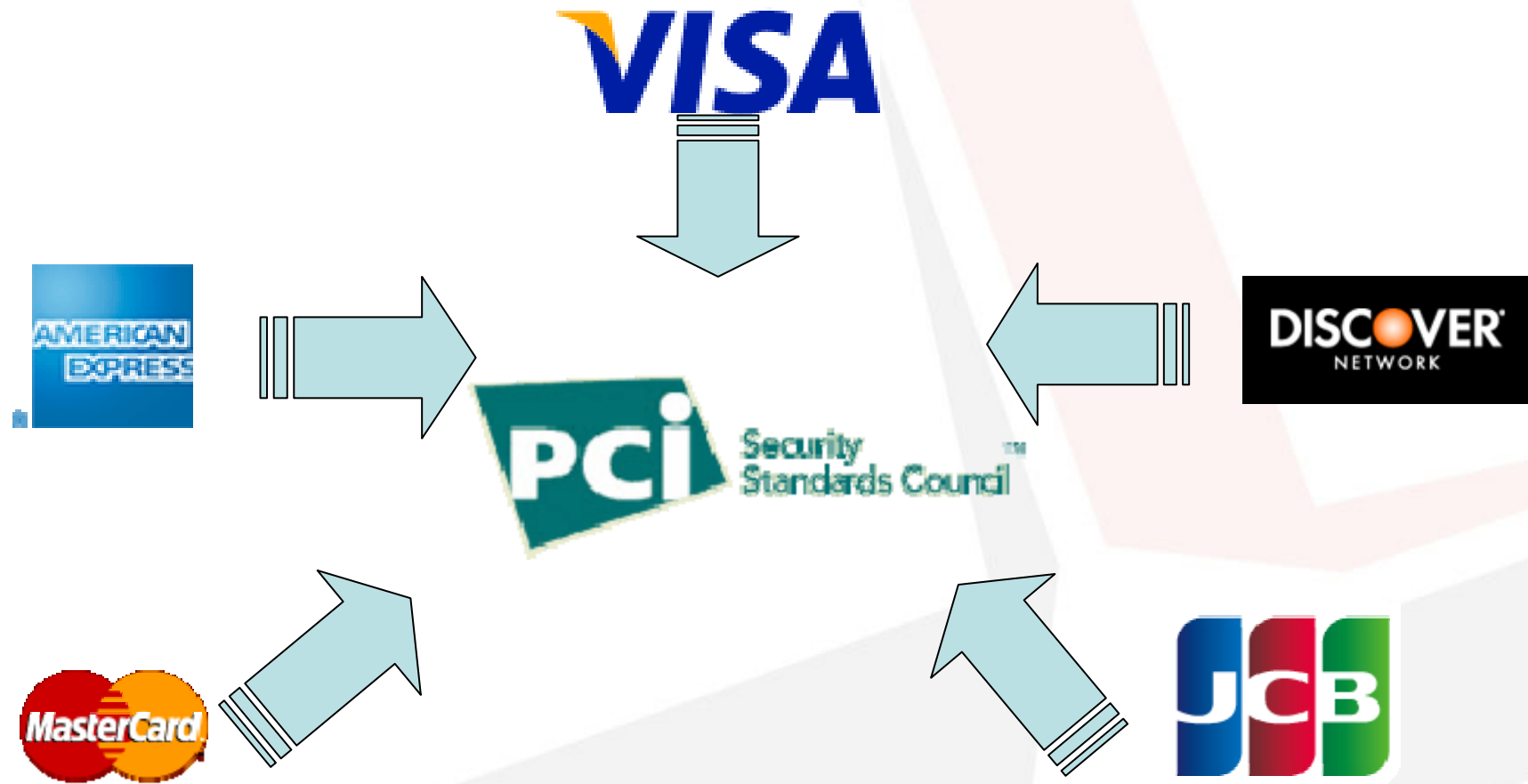
Sources: ABS; APCA; BPAY; RBA



# The big players in AU market



# The PCI Security Standards Council Members





# PCI Data Security Standard

## PCI DSS is:

- An open industry standard
- Tech requirements for data security
- PCI SSC maintains list of qualified PCI assessors (QSAs & ASVs)

## PCI DSS is not:

- A compliance program
  - Card Schemes run their own programs





# PCI DSS: Six Goals, Twelve Requirements

## The Payment Card Industry Data Security Standard (PCI DSS)

Build and Maintain a Secure Network	<ol style="list-style-type: none"><li>1. Install and maintain a firewall configuration to protect cardholder data</li><li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li></ol>
Protect Cardholder Data	<ol style="list-style-type: none"><li>3. Protect stored data</li><li>4. Encrypt transmission of cardholder data across open, public networks</li></ol>
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"><li>5. Use and regularly update anti-virus software</li><li>6. Develop and maintain secure systems and applications</li></ol>
Implement Strong Access Control Measures	<ol style="list-style-type: none"><li>7. Restrict access to cardholder data by business need-to-know</li><li>8. Assign a unique ID to each person with computer access</li><li>9. Restrict physical access to cardholder data</li></ol>
Regularly Monitor and Test Networks	<ol style="list-style-type: none"><li>10. Track and monitor all access to network resources and cardholder data</li><li>11. Regularly test security systems and processes</li></ol>
Maintain an Information Security Policy	<ol style="list-style-type: none"><li>12. Maintain a policy that addresses information security</li></ol>





## Who must comply?

- Everyone who stores, processes or transmits cardholder data
  - PCI compliance is mandatory
  - PCI applies to all parties in the payment process
  - You cannot be partially compliant: Compliance is PASS/FAIL

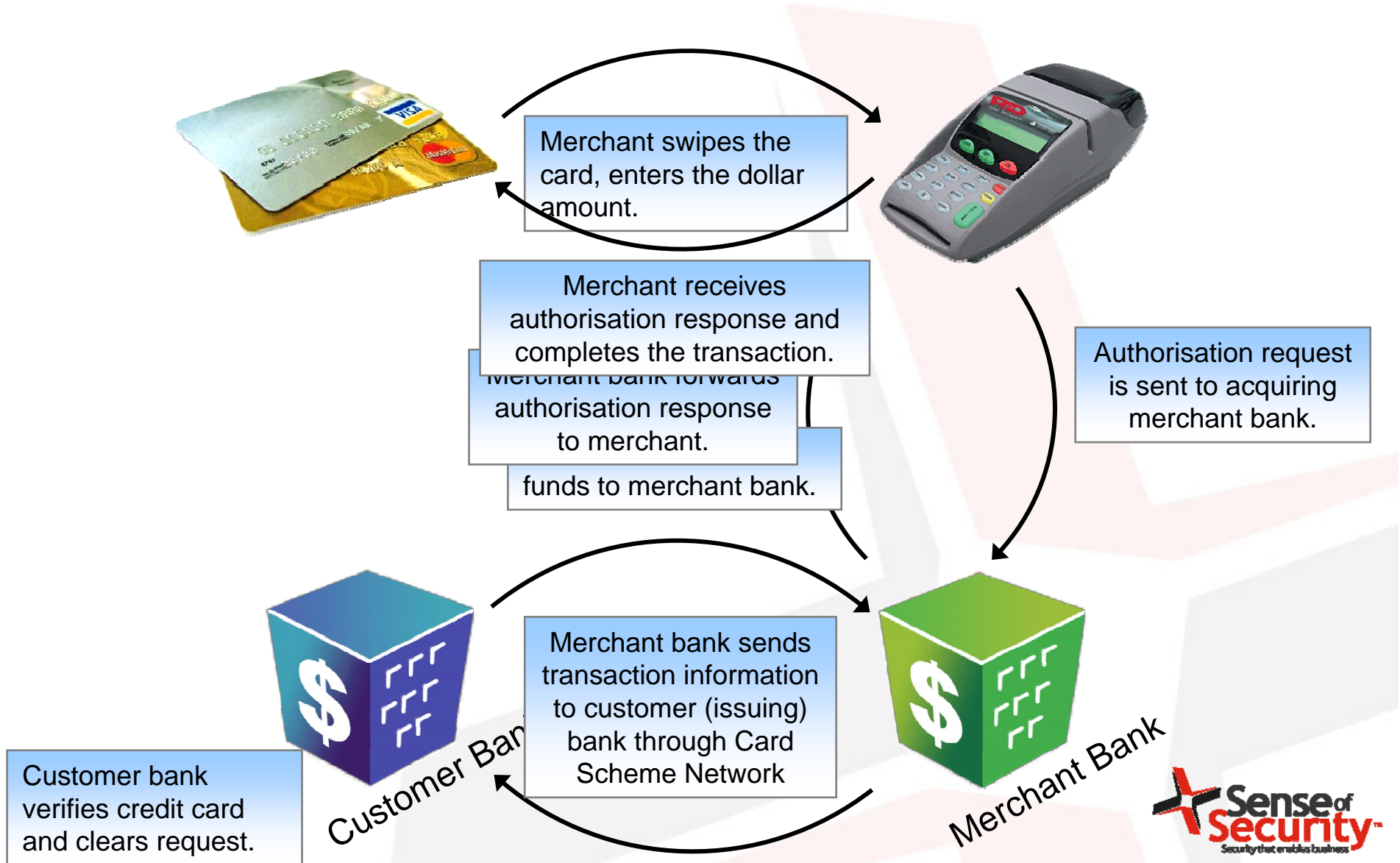




## How is PCI DSS Regulated?

- Regulated by the respective Card Scheme Compliance Programs.
- PCI is a technical standard of due care.
- PCI DSS is not law.
- The Payments System Board (PSB) of the Reserve Bank oversees the payments system in Australia.

# Card Present



# Merchant Levels - MasterCard & Visa from Jan08

	Level 1	Level 2	Level 3	Level 4
*Annually † Quarterly ‡Annually	More than 6M transactions	Between 1M and 6M transactions	Between 20K and 1M e-Commerce transactions	All Others
Self Assessment *	Not Reqd	Mandate	Mandate	Mandate
Vulnerability Scan †	Mandate	Mandate	Mandate	Mandate / Rec VISA
Onsite Review ‡	Mandate	Not Reqd	Not Reqd	Not Reqd



# Merchant Levels - Amex

† Quarterly ‡ Annually	Level 1	Level 2	Level 3
	More than 2.5M transactions	Between 50K and 2.5M transactions	Less than 50K transactions
Vulnerability Scan †	Mandate	Mandate	Highly Recommend
Onsite Review ‡	Mandate	N/A	N/A

ref: <http://www10.americanexpress.com/sif/cda/page/0,1641,17457,00.asp>

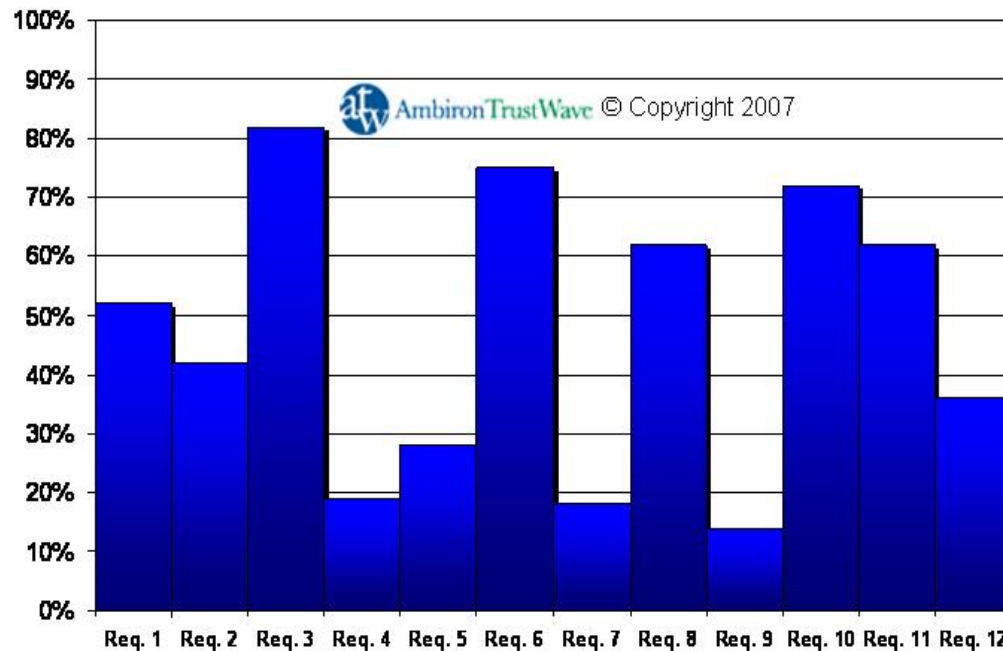




# What can and can't be stored

- What must not be stored (after authorisation):
  - Full magnetic stripe
  - Card verification values (CVV2, CVC2, CID)
  - PIN verification value
  - PIN and PIN block
- What can be stored (must be protected):
  - Primary account number
  - Cardholder name
  - Service code
  - Expiration date

# Most Common PCI Requirements Not Met



*\*Percentage of Compromised Merchants That Failed To Meet Each PCI DSS Requirement*

**\*Data gathered from more than 250 card compromise investigations conducted by ATW. This Slide is Copyright PCI Security Council**

## Requirement 1:

- Install and maintain a firewall to protect cardholder data

## Requirement 3:

- Protect stored data

## Requirement 6:

- Develop and maintain secure systems and applications

## Requirement 8:

- Assign a unique ID to each person with computer access

## Requirement 10:

- Track and monitor access to network and card data

## Requirement 11:

- Regularly test security systems and processes





## Risks and consequences of non-compliance

- Card Schemes may levy fines to the Acquiring Bank of a Merchant if Merchant is not compliant.
- Acquiring Bank may pass on fines to the Merchant in line with Merchant Contract or Bank's discretion.

- MasterCard has issued fines in AU.
- US\$25K for non compliant Level 1's & Level 1 and 2 Service Providers
- US\$5K for Level 2 and 3 Merchants.
- Penalty applied if Merchant/Gateway:
  - did not complete PCI DSS
  - did not take steps to mitigate the risks of an account data compromise.
- Operational Risks to consider:
  - Up to US\$100K for each incident + Up to US\$25K each day until member achieves compliance + Investigation and other related costs incurred.
  - Compensation: Up to US\$25 per card re-issued + Up to US\$5 per card monitored (without card reissue)

- Visa AP has not yet levied any fines in AU. Crunch time will come in Jan 2008.
- Visa AP can fine up to US\$500K if a threshold level is triggered.
- This threshold probably has been reached in AU (recent breach).
- \$500K comprised of \$100K in card replacement fees & \$400K if more than \$1M fraud reported.

- Safe harbor provides members protection from Visa fines in the event its merchant or service provider experiences a data compromise.
- To attain safe harbor status:
  - must maintain full compliance at all times, including at the time of breach.
  - must demonstrate prior to the compromise merchant was fully compliant .

• Ref: [http://usa.visa.com/merchants/risk\\_management/cisp\\_overview.html](http://usa.visa.com/merchants/risk_management/cisp_overview.html)



## Merchant Benefits of Compliance

- Protect customers' personal data
- Boost customer confidence through a higher level of data security
- Lower exposure to financial losses and remediation costs
- Maintain customer trust and safeguard the reputation of their brand
- Provide a complete "health check" for any business that stores or transmits customer information.



- Historically focused on large e-commerce & Level 1 Merchants. (Target Compliance 31Dec07)
- Visa looking for evidence of Merchant PCI Cert intent & Road Maps for '08 '09.
- Visa requires validation of Level 1 but not yet Level 2 Merchants.

- Not enough focus on Level 2's at present.
- At least 6 breaches on Level 2 and Level 3 ecom Merchants recently.
- Expect in 2008:
  - Certificate of compliance for Level 2's.
  - Education campaign for L3's but not looking for certificate of compliance yet.



## Service Providers

- 30-90 Service Providers in the AU Market.
- Expect merchants to look for partnership with a Service Provider to reduce Merchant exposure.
- Complexity when there is a 3<sup>rd</sup> Party involved.



# How big is the AU Market?

Level 1	}	300
Level 2		
Level 3		
Level 4		650,000 -750,000

Per info from MasterCard



# So how many Merchants are Compliant?

According to VISA USA: Ref: <http://corporate.visa.com/md/nr/press719.jsp>  
(30 Jul 07)

Level	Compliant	Working towards
1	40%	50%
2	33%	42%
3	52%	22%



## And in Australia?

- This type of info is not readily available to the public.
- Conflicting information. Some Acquirers confident for their L1's.
- Complexity of historical systems means that true compliance still requires significant effort.



## Australia's Position

- Research indicates that AU and NZ regions compare favourably with other APAC regions.
- Higher level of collaboration.
- Good work between banks and schemes.
- Scheme PCI Road Shows had good results.
- Fewer barriers with brands.



## Are we better off now than 12 and 24 months ago?

- Overwhelming answer YES from all schemes and acquiring banks interviewed.



## So where to from now?

- Merchants will likely consider hosted solutions.
- Expect more focus on Verified by Visa (vbv) and MasterCard SecureCode for cardholder authentication.
  - Called 3-D Secure if the Gateway offers both.
  - Merchants are no longer liable for chargebacks where the cardholder claims fraud or non participation

- **Clarity and Consistency:**
  - data definitions and cardholder data storage and protection.
- **Flexibility:**
  - compensating controls for data encryption
- **New Security Requirement:**
  - New application level requirement (6.6) web app code review or web app fw.

"Today, it's a one-size fits all but going forward we'll have four different versions based on the merchant's business," says Russo. "For instance, if they're small and just doing dial-up, there's no need for them to answer 200 questions, we'll just have 30 or 40 questions."

Ref: <http://computerworld.co.nz/news.nsf/scrt/6277ADB06EBBC57FCC2573870002C963> 5 Nov 07



## Card Scheme Focus in 2008

- Visa and MasterCard concur more education required for smaller sized merchants.
- MasterCard also noted focus on recalcitrant merchants.
- Payment Application Best Practices.



## What if you haven't started PCI Compliance Initiatives yet?

- There is plenty of help available.
- Speak to Merchant Services at your Acquiring Bank.
- Speak to your local Card Scheme office.
- Read the standards at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)
- Find a local QSA.
- Join a PCI Forum, read whitepapers
- Prepare your managers for the work ahead.





Thank you  
for participating in this research





Thank you

Questions?

Murray Goldschmidt

Sense of Security Pty Ltd

[info@senseofsecurity.com.au](mailto:info@senseofsecurity.com.au)

Tel: +61 2 9290 4442

