

Deloitte.

CONFIDENTIAL

Payment Card Industry (PCI) Compliance



Presentation to ISACA Edmonton Chapter

Paul Zonneveld
Partner, Deloitte

Audit • Tax • Consulting • Financial Advisory.

Objective

1. What problem are we trying to solve?
2. What are the challenges for Organizations?
3. Lessons Learned
4. Questions

Background to the development of PCI

- Significant Fraud losses were occurring globally in both card present (swiped) & card not present (online) environment
 - Stored data was not protected by acquirers/merchants
 - Data was not protected by processors
 - Transmission of credit card data in clear text, making it easy to compromise
 - Organized crime infiltrated major organizations
 - High proportion of compromise had a major internal component
 - Lot more information continues to be stored than needed
- Brand impact can be significant, resulting in loss of confidence by consumers being impacted by the compromise.
- Significant costs to manage the fraud losses, not to mention loss of business
- Card brands were concerned that fraud losses related to data breaches were becoming acceptable as “cost of doing business”

Some statistics

- Credit card transactions in Canada - \$190B (2005)
- Credit cards in circulation (Canada) – 56m
- Estimate of fraud in Canada - \$500m
 - Counterfeit credit card – 37%
 - Lost or Stolen Cards – 23%
 - No-Card Fraud – 10%
 - Non-Receipt Fraud – 7%
 - Identity Theft Fraud – 4%

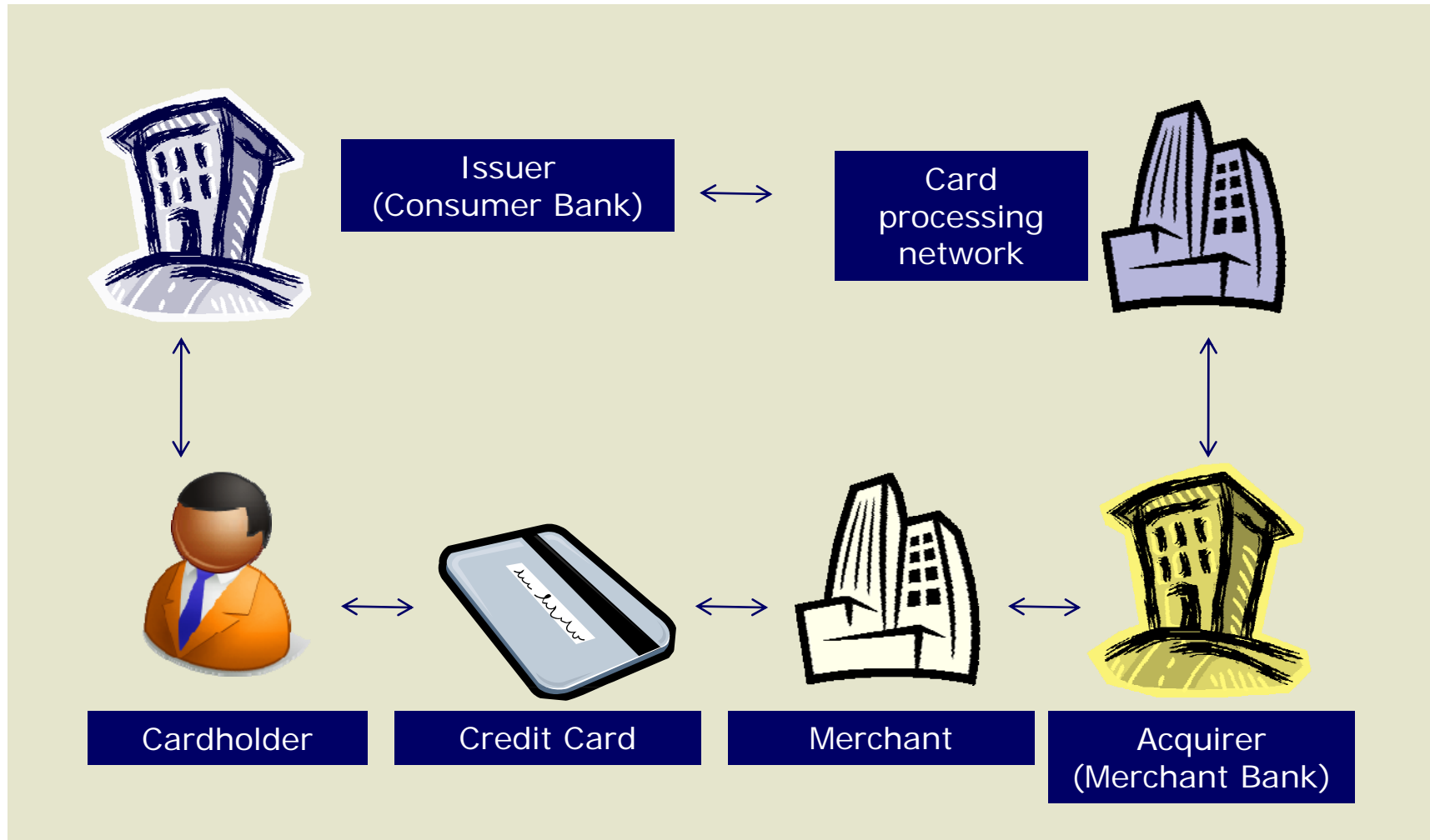
What led to Account Information Security

- A minimum standard was required to hold responsible merchants, acquirers, processors, issuers and anyone else that stored, processed or transmitted credit card data
- A standard was required that would enforce best practices and education/awareness to minimize/prevent the opportunities for data compromises
- Although Acquirers had agreements in place that held merchants responsible, the challenge was that a lot of operating regulations/rules/processes originated from a paper based business
- Some of the Banks outsourced the Acquiring business (low margin business) creating some additional challenges

PCI – a compliance requirement that is applicable to merchants or service providers – they have little choice but to become compliant

- Anyone that stores, processes or transmits cardholder information must become compliant
- Those that reach certain levels of transaction volumes are required to demonstrate compliance
- Adopted by major card issuers – Visa, MasterCard, AMEX, Discover, and JCB
- However, the process may not be standardized:
 - May be differences in: level / category or type, validation requirement, reporting of compliance requirement

Card flow simplified



7 How should compliance officers cope with the new PCI standards?

All merchants and service providers need to be compliant

- Includes Brick & Mortar, Mail order and telephone order and electronic commerce
- Effective March, 2005, depending on annual Visa transaction volume and merchant type, merchants falls under one of four categories/levels
- Requirements range from annual on-site review, vulnerability scan, and/or self-assessment questionnaire
- For every level, each entity is required to re-certify annually, those who fail to re-certify are no longer considered to be compliant with the program

The value of compliance

- Demonstrate due diligence over Account and Transaction Information
- Enhance the ability to maintain confidentiality, integrity and authenticity of information
- Gain competitive edge – maintain a positive image and enhance trustworthiness
- Safe Harbor – complied merchant or entity will be granted “safe harbor” from any penalties / fees / fines from Visa Canada after a hack or compromise if the appropriate actions are followed

PCI data security standard

Six major areas and twelve requirements to review:

- Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

– Protect Cardholder Data

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

– Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus information
6. Develop and maintain secure systems and applications

PCI data security standard (cont'd)

Six major areas and twelve requirements to review (cont'd)

- Implement Strong Access Control Measures

7. Restrict access to 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

PCI compliance validation levels – merchant

	Annual Visa Transaction Volume	Self-Assessment Questionnaire	Vulnerability Scan	On-site Review
1	Over 6m or experienced a breach		Quarterly	Annual
2	1m to 6m	Annual - verified	Quarterly	
3	20,000 to 1m	Annual – verified	Quarterly	
4	<20,000	Annual - verified	Annual	

* - Mail Order and Telephone Order

PCI compliance validation levels – Service provider

	Annual Visa Transaction Volume	Self-Assessment Questionnaire	Vulnerability Scan	On-site Review
1	Over 300,000		Quarterly	Annual
2	Less than 300,000	Annual	Quarterly	

* - Mail Order and Telephone Order

Version 1.2 of the standard is out (2008)

- General
 - Provided greater guidance on network segmentation
 - Provided greater guidance on compensating controls
 - Clarified many items in the standard, provided guidance on some requirements
- Summary
 - Evaluate and determine if network segmentation can be a method to reduce the assessment scope
 - Evaluate and determine if compensating controls can be used to meet the requirements, in the event that a particular requirement cannot be met exactly as stated

Challenges that Organizations face

The current reality & challenges – Environmental

- Continued lack of understanding as to who the standard applies to, compliance dead-lines and penalties
- Communication about compliance (deadlines, ramifications etc.) is not effective or in some instances non existent
- PCI is NOT part of broad regulatory/compliance and therefore there is no ongoing oversight or program/strategy in place to sustain compliance
- Lack of effective controls over the “Point of Sale” terminals and other systems, allowing the possibility of tampering & compromise of confidential data
- Lack of Strategy in dealing with “Card Not present” fraud

The current reality & challenges – Organizational

- Organizational silos prevent a holistic view to the magnitude of the problem and create subsequent losses
- Fraud is seen by many organizations as a “cost of doing business”
- Approach to compliance does require the involvement of multiple stakeholders
- There is no clear enterprise wide owner/sponsor
- The traditional way of compliance (letter of the law) proves to be very costly or impractical
- Building a business case to justify to the business the need for compliance & ROI
- Widespread access to critical data
- Lack of effective access controls

What lessons have
we learned?

Observations & lessons learned

- Communication & Awareness has been lacking, minimizing the chances of effective & timely implementation and benefits to the Organization
- All stakeholders have not been involved with PCI
- Many Organizations are doing the minimum just to comply as opposed to looking at this as an opportunity to enhance the organizations security posture
- Organizations are storing data that is not required to conduct the business, leading into redundant processes & storage of redundant and unnecessary data
- Some Organizations are repeating the exercise as their challenges were not dealt with properly in the first instance
- The approach to PCI compliance process, by some organizations, is a one time effort, and thus NOT geared towards a sustainable process

Observations & lessons learned (continued)

- PCI has not been part of the overall security framework and is seen as a “credit card” or in some cases, IT problem only
- Process for the development of new applications/processes in some instances does not take into account the PCI standards requirements to keep the organization compliant
- Some credit card processing has been outsourced without adequate due diligence
- Some Organizations have embarked upon remediation, without first doing data classification/discovery, to ensure that they limit their activities to the highest areas of priority

Observations & lessons learned (continued)

- The road to PCI compliance does cross many departments and therefore must have buy-in from the top; otherwise organizations risk failure and/or continued exposure
- Contracts managing third parties do not keep pace with changing business needs and in some instances, have not stipulated the right to audit the third parties. Statement printing, frequent flyer programs, loyalty programs, target marketing have been outsourced by many organizations without adequate oversight ability
- PCI and Chip & Pin (if applicable) projects are dealt with differently. They both carry liability shift and impact the same area of the business with synergy. Furthermore, combining the two could lead reduce the scope of PCI

Most companies are faced with several fundamental issues to compliance

- Scoping of the project is too large – operating a flat network and no network segmentation – all network components are in scope
- Running legacy systems, operating systems, and software that does not support PCI requirements
- Lack of resources that have PCI knowledge (interpretation of controls) to handle the compliance and remediation efforts
- Lack of formal processes or procedures
- Complex organizations may not know what systems need to be in scope, often times, are surprised to find out unknown applications or systems through the assessment. Note that having a safe harbour status but a security breach occurs on applications that were not assessed will not be covered under this status.

Most companies are faced with several fundamental issues to compliance – con't

- Storing, processing, and transmitting data when there is no business requirement. Removing the actual functions, data, and or system is not an easy process
- More mature organizations have many different applications developed by different teams that all have similar functions. Consolidation efforts would be rewarded in the long run; however, not realized and considered for the short term
- Third parties that develop software, and provide service to merchants are not compliant to PCI (more on this later)

Merchants and service providers are required to comply, and many are working towards closing the gaps from the first assessment

- Current trends:
 - Most merchants have completed their first assessment
 - Most merchants have identified the security gaps, and are in the process of identifying solutions or remediation strategies
 - Timeline to close the identified gaps is unclear – no clear guidance. General consensus is based on risk level – high risk gaps should be addressed first
 - Cost of full compliance can be significant
 - The evaluation of compensating controls – a new requirement in version 1.2 of PCI

Merchants and service providers are required to comply, and many are working towards closing the gaps from the first assessment – con't

- Current trends:
 - Organization's focus – passing the controls/validation vs. reducing the risk
 - Payment application best practice program – may be the trend in the next few years as it can reduce some validation effort / issues
 - Cost of non compliance is usually not driven by fines but by reputation and brand
 - Proactive monthly network scanning (requirement is quarterly)
 - Large merchants with many stores across the globe that have data sent back to the back end processing

Service providers and third party

- Merchants are
 - Responsible for which service provider, third party that they choose to do business with, hence, how the third party, service provider handles or have access credit card holder data could affect the results of merchant's PCI assessment results
 - Third party developers may not necessarily have access to credit card holder data; however, they have to have security in their development process
 - Require service provider and third party to demonstrate compliance to PCI
 - Most service providers, and third parties do not have compliance yet
 - Other third party reports such as SAS70 or CICA Section 5900/5970 do not have PCI in scope and hence, assessment at the third party is still required
 - Tend to have the most pushback and are generally more difficult to deal with especially because legal matters are involved

Network scanning is a PCI requirement for all merchants, but can be problematic for larger merchants

- Required to be scanned by ASV for the Internet facing IP range for all merchant levels
- Vulnerability scanner is run against active Internet facing PCI systems
- Systems hosted by a third party are in scope, may trigger issues
- Required to be performed on a quarterly basis but merchants are proactively scanning on a monthly basis
- If no clean report (any vulnerability not a false positive category 3 to 5), continue scanning until obtained (which then quarterly scans are still required continually)
- No formal holistic vulnerability management from detecting applicable vulnerabilities to a formal remediation process

Some of the requirements deserve more attention – compliance benchmark

PCI Requirements	Compliance benchmark
1 – install and maintain a firewall configuration to protect data	53%
2 – do not use vendor supplied defaults for system passwords and other security parameters	16%
3 – Protect stored data	21%
4 – Encrypt transmission of cardholder data and sensitive information across public networks	22%
5 – use and regularly update anti-virus software	50%
6 – Develop and maintain secure systems and applications	37%

Some of the requirements deserve more attention – compliance benchmark

PCI Requirements	Compliance benchmark
7 – Restrict access to data by business need-to-know	50%
8 – Assign a unique ID to each person with computer access	45%
9 – Restrict physical access to cardholder data	48%
10 – Track and monitor all access to network resources and cardholder data	46%
11 – Regularly test security systems and processes	16%
12 – Maintain a policy that addresses information security	48%

Top weakness areas – identifying the high risk areas and prioritizing the risk reduction / remediation effort

- Security testing of network systems
 - Periodic testing were not performed. No formal process.
- Operating system security configuration
 - Mainly hardening of O/S – services, clear text admin tools used.
- Data encryption and key management of sensitive stored data (storage and masking of data – Requirement 3)
 - No encryption software, no formal key management process
- Vulnerability / patch management (Requirement 6)
 - No formal process

Top weakness areas – identifying the high risk areas and prioritizing the risk reduction / remediation effort

- Secure application development practices (Requirement 6)
 - Security not build into the SDLC process
- Logging and monitoring
 - Logging too much incoming transaction data (CVV2, full magnetic stripe, and PVV data are prohibited)
 - Not logging enough (failure to comply to the standard)
- Third party access (Requirement 12.8)
 - No requirement / controls to govern third-party responsibilities
 - SLA constructed without PCI compliance requirement
- Backup and storage of data

Companies are now focused on closing the identified gaps, and obtain a “clean” report on compliance

- Tactical vs. holistic view – passing the validation vs. risk reduction (control existence vs. operating effectiveness)
- Data protection
 - controlling and monitoring data coming into the organization, processing and leaving the organization
 - storing less, better access control, understanding the data flow, better planning
- Maximize benefits – complying multiple standards / requirements. Implementing program to achieve and maintain compliance.

Remediation recommendation

- Perform a thorough scoping project to determine all credit card data flows from transaction to billing
- Scope out the effort between reducing PCI environment against efforts required to be PCI compliant for flat network
- Determine the options available applicable to your environment
- Keep close relationship with acquirer to understand their expectations; sometimes, acquirer can choose to deem a particular Not in Place item to be acceptable under certain circumstances
- Train / hire staff that have PCI knowledge

Thank-you

- For more information, please contact:
 - Paul Zonneveld – 403.503.1356
 - Vis Viswanathan – 780.421.3733

Deloitte.

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services through more than 6,800 people in 51 offices. Deloitte operates in Québec as Samson Bélair/Deloitte & Touche s.e.n.c.r.l. The firm is dedicated to helping its clients and its people excel. Deloitte is the Canadian member firm of Deloitte Touche Tohmatsu.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.

© Deloitte & Touche LLP and affiliated entities.



Member of
Deloitte Touche Tohmatsu