UBC & PCI DSS Compliance

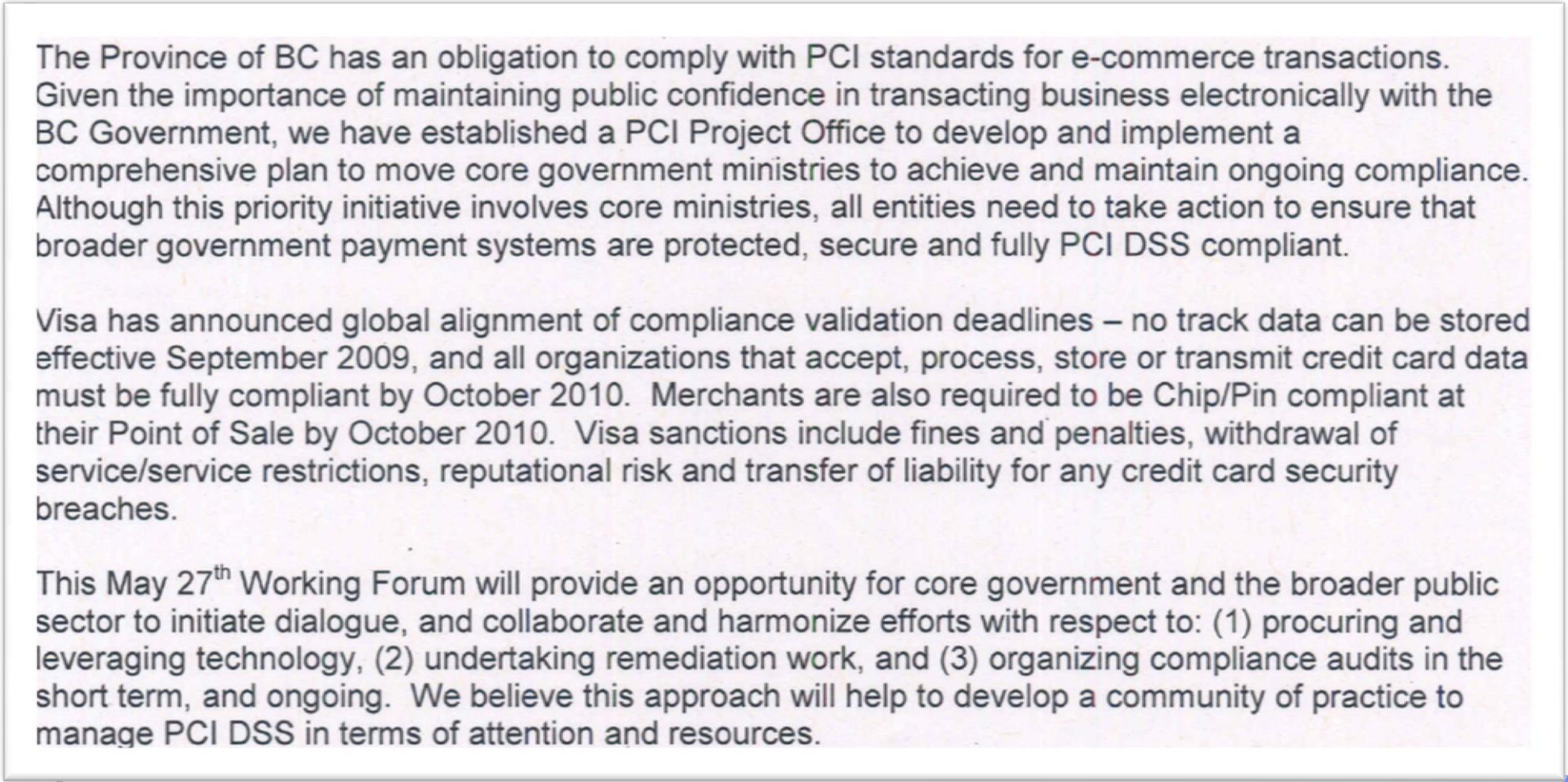
PCI = Payment Card Industry

Data Security Standards

Overview

- Direction from the Province
- Current Status
- Risk mitigation – outsource service hosting
- Who owns PCI Compliance for UBC
- Active Merchants

Direction from the Province

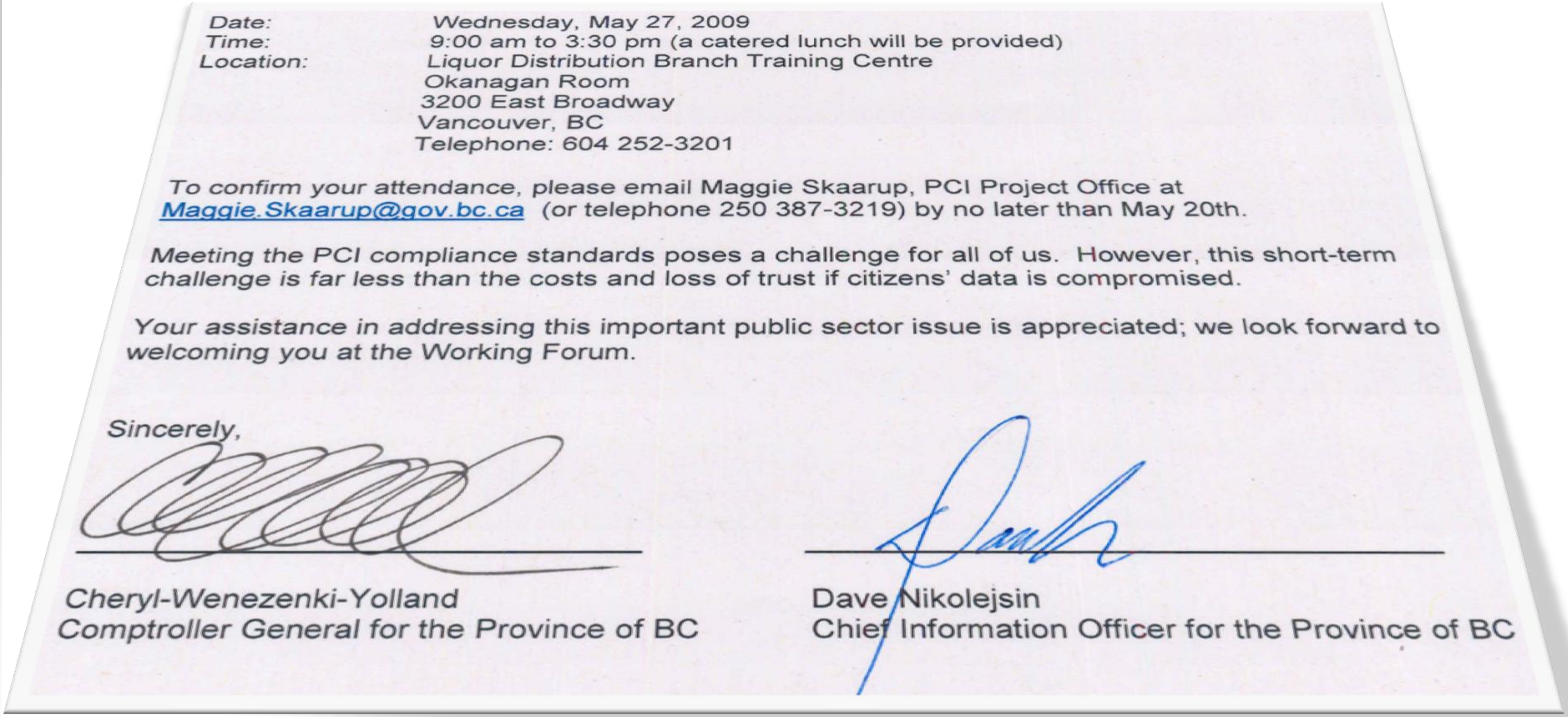


The Province of BC has an obligation to comply with PCI standards for e-commerce transactions. Given the importance of maintaining public confidence in transacting business electronically with the BC Government, we have established a PCI Project Office to develop and implement a comprehensive plan to move core government ministries to achieve and maintain ongoing compliance. Although this priority initiative involves core ministries, all entities need to take action to ensure that broader government payment systems are protected, secure and fully PCI DSS compliant.

Visa has announced global alignment of compliance validation deadlines – no track data can be stored effective September 2009, and all organizations that accept, process, store or transmit credit card data must be fully compliant by October 2010. Merchants are also required to be Chip/Pin compliant at their Point of Sale by October 2010. Visa sanctions include fines and penalties, withdrawal of service/service restrictions, reputational risk and transfer of liability for any credit card security breaches.

This May 27th Working Forum will provide an opportunity for core government and the broader public sector to initiate dialogue, and collaborate and harmonize efforts with respect to: (1) procuring and leveraging technology, (2) undertaking remediation work, and (3) organizing compliance audits in the short term, and ongoing. We believe this approach will help to develop a community of practice to manage PCI DSS in terms of attention and resources.

Direction from the Province



Date: Wednesday, May 27, 2009
Time: 9:00 am to 3:30 pm (a catered lunch will be provided)
Location: Liquor Distribution Branch Training Centre
Okanagan Room
3200 East Broadway
Vancouver, BC
Telephone: 604 252-3201

To confirm your attendance, please email Maggie Skaarup, PCI Project Office at Maggie.Skaarup@gov.bc.ca (or telephone 250 387-3219) by no later than May 20th.

Meeting the PCI compliance standards poses a challenge for all of us. However, this short-term challenge is far less than the costs and loss of trust if citizens' data is compromised.

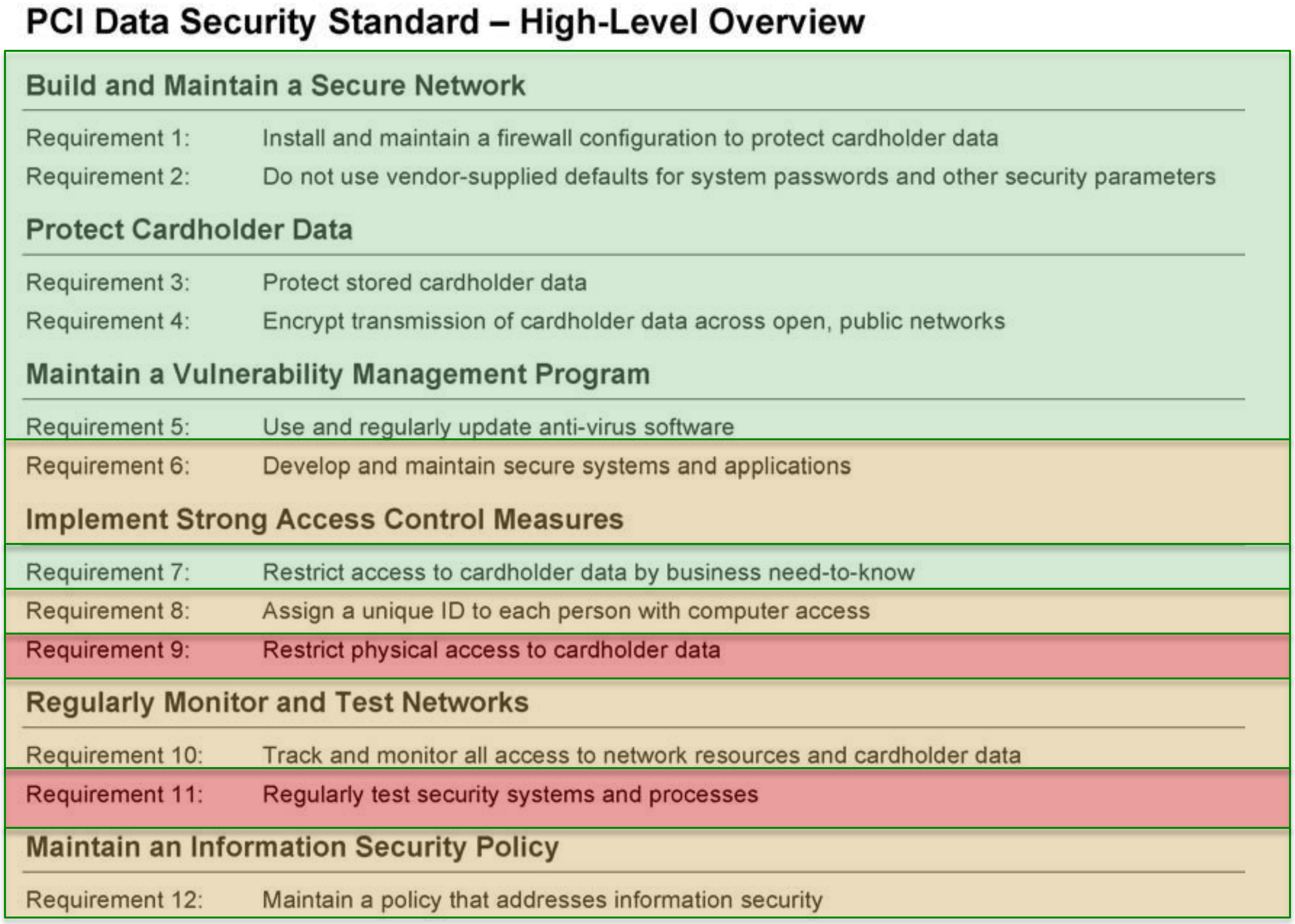
Your assistance in addressing this important public sector issue is appreciated; we look forward to welcoming you at the Working Forum.

Sincerely,

Cheryl-Wenezenki-Yolland
Comptroller General for the Province of BC

Dave Nikolejsin
Chief Information Officer for the Province of BC

Current Status – CBM Module @ UBC



PCI Data Security Standard – High-Level Overview

Build and Maintain a Secure Network 🟩

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

Protect Cardholder Data 🟩

Requirement 3:	Protect stored cardholder data	🟩
Requirement 4:	Encrypt transmission of cardholder data across open, public networks	🟩

Maintain a Vulnerability Management Program 🟩

Requirement 5:	Use and regularly update anti-virus software	🟩
Requirement 6:	Develop and maintain secure systems and applications	🟨

Implement Strong Access Control Measures 🟨

Requirement 7:	Restrict access to cardholder data by business need-to-know	🟩
Requirement 8:	Assign a unique ID to each person with computer access	🟨
Requirement 9:	Restrict physical access to cardholder data	🟥

Regularly Monitor and Test Networks 🟨

Requirement 10:	Track and monitor all access to network resources and cardholder data	🟨
Requirement 11:	Regularly test security systems and processes	🟥

Maintain an Information Security Policy 🟨

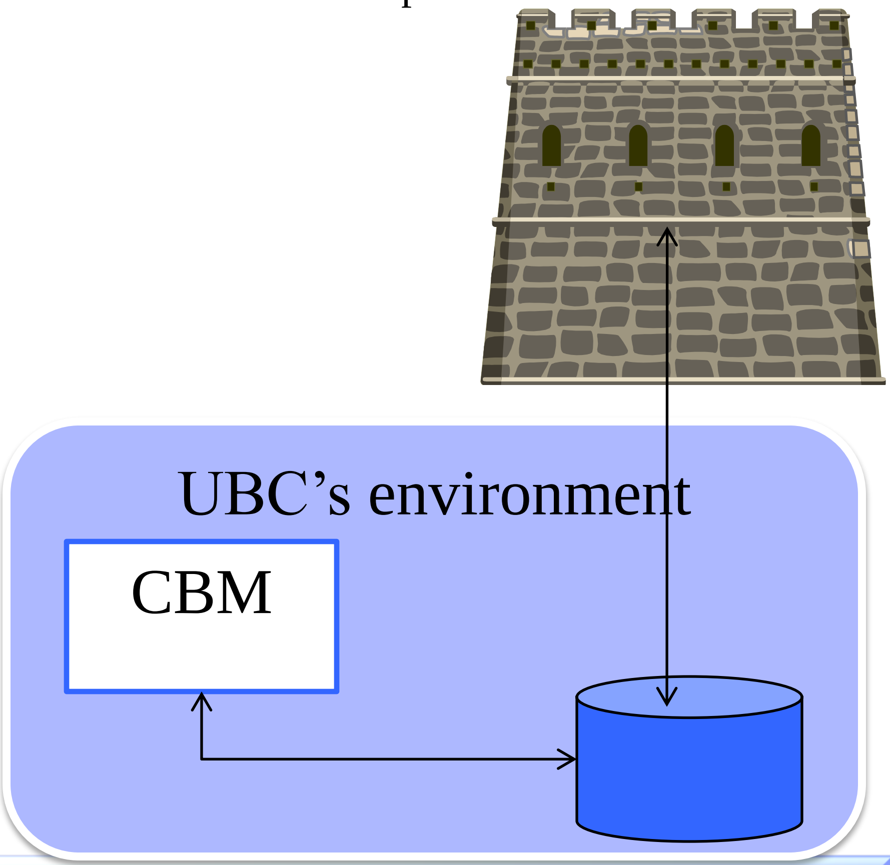
Requirement 12:	Maintain a policy that addresses information security	🟨

- 🟩 We are now in compliance for these areas
- 🟨 We are two to three month of work away from being compliant
- 🟥 We have a major uphill battle to become compliant here.

Risk mitigation - Plan

- CBM currently is a stand alone module
- It does not store credit card numbers
- It can be out-sourced to a PCI compliant 3rd party to host / manage
  - Already has the physical security in place
  - Already has the monitoring in place
  - Already has approved / audited procedures and policies in place

PCI Compliant service provider



Risk Mitigation

- RFI has been created and is currently open for response
- Four vendors have indicated that they will respond
- RFI closes on July 6th

peer1
Fully scalable hosting solutions

fusepoint

primus.
BUSINESS SERVICES

Moneris
SOLUTIONS

Who owns the PCI issue for UBC?

- Meetings held with Finance, UBC IT & Enrolment Services
- Agreed at the meeting that Ian Burgess owns the fiscal compliance issue.

- With the October 2010 compliance mandate – Internal Audit have been briefed and are preparing to review
- PCI compliance to be incorporated into UBC's fiscal reports to the Province

Merchants at UBC not using CBM

- Excluding the 70 +/- groups using Student Systems' CBM module - Central Finance identifies a variety of UBC merchants via bank:
  - **First data (BMO)**
  - **HSBC – Caledon**
  - **HSBC – Moneris**
  - **TD**
  - **CIBC**
  - **Royal Bank**
- Some are handling physical cards and issuing receipts, some are storing card details, others could migrate to use CBM
- Finance review of Merchants has identified that not all accounts are active.
- Previously though to be about 400 Merchants – this estimate is reduced to less than 200.
- Inspite of this good news – we are clearly going to be challenged to meet the Provincially mandated compliance date for UBC as a whole.