

FINANCE AND CIVIC DEVELOPMENT COMMITTEE

*HIS WORSHIP, THE MAYOR
AND COUNCILLORS*

**SUBJECT: PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS
(PCI-DSS) PROJECT**

RECOMMENDATION:

1. THAT Council approve funding in the amount of \$65,000 from the Stabilization Reserve to begin the process of Payment Card Industry Data Security Standards Certification, as outlined in this report.

REPORT

The Finance and Civic Development Committee, at its meeting held on 2013 January 24, received and adopted the *attached* report seeking funding approval in the amount of \$65,000 from stabilization for the initial phase of the City's Payment Card Industry Data Security Standard (PCI-DSS) project.

PCI-DSS standards were introduced in 2006 to reduce merchant fraud for businesses and organizations that provide credit and debit card payment acceptance services to their clients. The City is required to meet these standards to achieve annual certification. Failure to complete certification can result in fines, lawsuits and revocation of merchant privileges.

Respectfully submitted,

Councillor D. Johnston
Chair

Councillor C. Jordan
Vice Chair

Councillor P. McDonell
Member

Copied to:	City Manager Director Finance
------------	----------------------------------

TO: CHAIR AND MEMBERS
FINANCE AND CIVIC DEVELOPMENT
COMMITTEE

DATE: 2013 January 16

FROM: DIRECTOR FINANCE

FILE: 6900-20

**SUBJECT: PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS
(PCI – DSS) PROJECT**

PURPOSE: To request funding approval in the amount of \$65,000 from stabilization for the initial phase of the City’s PCI-DSS project.

RECOMMENDATIONS:

1. **THAT** Finance and Civic Development Committee recommend Council approve funding in the amount of \$65,000 from the Stabilization Reserve to begin the process of Payment Card Industry Data Security Standards Certification as outlined in this report.

REPORT

For businesses and organizations that provide credit and debit card payment acceptance services to their clients, industry regulatory standards called Payment Card Industry Data Security Standards (PCI-DSS) were introduced in 2006 to reduce merchant fraud. PCI-DSS standards are a set of 12 general requirements aimed at strengthening cardholder data security. The standards were set forth by the Payment Card Industry Standards Security Council (PCI-SSC) comprised of credit card industry representatives from Visa, MC, Amex, Discover and JCB card brands. The PCI-SSC determined that stronger security and control measures were required globally to ensure appropriate action and care is in place to help prevent fraudulent activities or the loss of sensitive credit card data.

PCI-DSS measures include system vulnerability scans, policy and procedure documentation, audit of certification and the attestation of certification completion. Larger merchants such as Best Buy, Home Depot, and WalMart were required to meet the most stringent set of PCI-DSS requirements first given the size and volume of their daily credit card transactions.

The City of Burnaby, like most municipalities and small businesses, are considered the lowest level of threat but the City is still required to meet PCI-DSS standards and achieve annual certification based on our level of credit card dollar transactions and volume. Failure to complete certification or being involved in a fraudulent activity in which a security breach has been confirmed can result in fines, lawsuits and revocation of merchant privileges.

The City of Vancouver has successfully achieved PCI-DSS certification. Staff visited their team and discussed their process, which was comprehensive and extensive. Vancouver utilized an outside consultant to assist during the preparation phase (costs of which were approximately \$150,000) to develop a detailed implementation plan for certification. They appointed an internal team and spent approximately two years making the required changes to their business processes and systems at a cost that exceeded one million dollars. In addition, to conduct annual certification an ongoing sustainment program with 1.5 RFT staff has been setup to sustain PCI-DSS compliance.

In 2009/2010 Burnaby Treasury, Internal Audit and IT staff conducted a preliminary review of the City's status for the purpose of PCI certification. Findings concluded that the City will need to commit significant effort over the next two years to achieve certification. Temporary internal staff resources will be needed to support the process and a Qualified Security Assessor (QSA) consultant hired to enable staff to move forward with this project.

QSA's contractors are certified under PCI-DSS guidelines and have the knowledge and experience required to assist staff in the development of a PCI-DSS implementation roadmap. Specifically, the QSA consultant will work with staff to provide:

- an assessment of the remediation and gap analysis already conducted by City staff
- identification of the work effort, specific resources and steps required for certification
- a detailed project plan and timeline with work assignment, milestones and set deliverables
- a cost estimate to reach certification and a plan for ongoing annual compliance.

Funding in the amount of \$65,000 is required to obtain the services of a QSA consultant and staff resource. The QSA contract will be under the direction of the Manager Treasury Operations. The findings of the QSA consultant will be reported back to Council in early September when the full scope of the requirements will be clarified and a timeline and project plan put forward for Council's consideration.

RECOMMENDATION

To support City staff in accomplishing Payment Card Industry Data Security Standards Certification staff request that the Finance and Civic Development Committee recommend Council approve funding from the Stabilization Reserve in the amount of \$65,000 to begin the process of Payment Card Industry Data Security Standards Certification as outlined in this report. Stabilization funding for this project would be included in the 2013 Annual Financial Plan once Council approval is received.

Denise Jorgenson
DIRECTOR FINANCE

DJ:ds /ml

Copied to: City Manager