Level 8, 66 King Street
Sydney NSW 2000 Australia
Telephone +61 2 9290 4444
or 1300 922 923

An article on

PCI Compliance for the Not-For-Profit Sector

In general, the Not-For-Profit (NFP) market relies heavily on credit card payments for regular and irregular giving. Organisations in this sector have also developed various channels for campaigns including call centres, online web sites, face to face marketing and traditional printed mail campaigns. As a result of dealing with these payments, this sector in general is faced with the requirement to be PCI DSS compliant and the fact that multiple channels exist whereby card payments are effected, the compliance requirements are made more challenging. Unfortunately, this sector is not immune to cyber security issues including hacking and loss of sensitive data, such as credit card details, through both online and offline exploitation. In order to bolster consumer confidence and manage the risk of the payment networks, payments effected through payment cards (credit and debit card) are regulated by card schemes and acquiring banks through the Payment Card Industry Data Security Standard (PCI DSS). All organisations that participate in the payment process of the cardholder data must comply with the PCI DSS if they transmit, store or process cardholder data.

> “The ultimate penalty is losing the ability to operate with payment cards due to termination of facility.”

Non-complaince with PCI DSS has its consequences. In general organisations suffering a breach and found not to be PCI DSS Compliant will have to address:

- Financial losses
- Reputation and brand damage
- Exposure to legal risks resulting from violating the privacy of cardholders
- Loss of business opportunities as a result of lack of trust
- Impact of downtime resulting from attacks
- Potential payment scheme penalties

The ultimate penalty is losing the ability to operate with payment cards due to termination of facility. As a result of dealing with these payments, this sector in general is faced with the requirement to be PCI DSS compliant. The fact that multiple channels exist whereby card payments are effected means the compliance requirements are made more challenging.

As the market matures and the compliance requirements have become more demanding and evident, organisations across the board have had to assess their exposure and plan for the most effective means to comply with the requirements so that they can maintain their income streams.

While the PCI DSS is a complex standard, organisations who have a requirement to comply with it should understand the core objectives of the standard in the first instance. The core objective of the PCI DSS is to protect cardholder data (CHD). While storing certain attributes of CHD is permitted under the standard, the controls required to protect it are complex and onerous. Therefore the first thing to determine is how to elimanate or reduce the data that is retained; and where data is elected to be retained, determine a compliant method to protect it. There are specialist software vendors and payment service providers who service this sector with donor and customer management systems.

The PCI Standards Security Council (PCI SSC) also maintains another compliance stream which applies to software developers who produce payment applications[1] and provide them to the market under licence. This compliance stream is called the Payment Application Data Security Standard (PA DSS). PA DSS applies only to third-party payment application software that stores, processes or transmits cardholder data as part of an authorisation or settlement. PA DSS does not apply to software applications developed by merchants and agents for in-house use only. These in-house software applications are covered within a merchant or agent's PCI DSS assessment.

Therefore when a NFP organisation is assessing products that will deal with card payments, it is important to select PA DSS compliant applications. Accordingly, the software vendors have recognised the value in attracting a broader market to thier product and many have already pursued, and achieved, PA DSS compliance. It is also noted that the leading card brands have stipulated that all new merchants can only be boarded if using PA DSS compliant applications or are PCI DSS Compliant and that acquirers must ensure all thier merchants and service providers use PA DSS compliant payment applications by 1 July 2012[2].

> "Leading card brands have stipulated that all new merchants can only be boarded if using PA DSS compliant applications or are PCI DSS Compliant."

Vendors are providing a variety of products to suit different business needs. If products are designed to retain data then appropriate protective measures (e.g. encryption, truncation and masking) will need to be addressed. Other vendors have implemented tokenised vault products whereby the client retains only a token (a reference to the CHD) on site and the CHD is stored in an encrypted vault at the service provider. This is commonly deployed as a cloud or software -as-a-service offering. Tokenised solutions are attractive because the token is not considered CHD itself (it is just a reference) and therefore the compliance obligations are reduced for the client.

[1] For purposes of the mandates, payment applications apply only to third-party payment application software that stores, processes or transmits cardholder data as part of an authorisation or settlement of a payment card transaction.

http://www.visa-asia.com/ap/au/merchants/riskmgmt/ais_applications.shtml#Introduction

[2] http://www.visa-asia.com/ap/au/merchants/riskmgmt/ais_applications.shtml#Introduction

http://www.mastercard.com/us/company/en/docs/MasterCard_PA_DSS_Mandate.pdf

Through the vast array of cloud computing products available, companies also find attractive the options to outsource the hosting of critical and public facing systems (e.g. web sites) to hosting service providers. Unfortunately, this has traditionally been a less regulated market and the capabilities of the service providers vary dramatically across the spectrum. In line with the direction that software vendors have taken, some service providers have pursued, and achieved, PCI DSS compliance.

Accordingly, it is important to select service providers that can deliver a service compliant with the requirements of the PCI DSS and also to very clearly determine all the responsibilities of the service provider. At a high level, all requirements under the PCI DSS will need to be addressed for the merchant – either directly by the merchant or by a service provider where that aspect has been outsourced. Consequently, where engaging with a service provider, the NFP organisation can leverage the capabilities of the service provider and assign responsibilities to handle as many requirements of the standard as possible thereby reducing the number of items that the NFP has to deal with in-house.

The market is now also being populated with specialist service providers who provide managed services to deal with the logging, monitoring and reporting requirements demanded by the PCI DSS. NFP organisations should now be considering these as it will likely make sense to outsource these items as well rather than employing and training staff to deal with this in-house (specifically because the standard requires staff to be available 24x7 to deal with security incidents).

The PCI DSS requires detailed documentation across all requirements addressing wide ranging matters including but not limited to Information Security Policy, Acceptable Use, Human Resources, Risk Assessment, Daily Operating Procedures, Security Guidelines (Operating System, Applications, Network, Software Development), Network Diagrams, etc. Like other industry sectors, the NFP sector will find the documentation requirements challenging due to the volume and level of detail required. To address this issue, Sense of Security has developed a broad range of documents to assist specific industry sectors with their compliance program so that the organisations would need to deal with only the specific requirements of their business and have the general requirements attended to through the suite of documents.

> “All organisations that participate in the payment process must comply with the PCI DSS if they transmit, store or process cardholder data.”

All organisations that participate in the payment process must comply with the PCI DSS if they transmit, store or process card-holder data. A NFP company will be considered a merchant if the entity is the recipient of funds derived directly from payment cards and has a merchant facility with an acquiring bank. In general merchants are assigned a merchant level (1, 2, 3 or 4) which is broadly based on the number of transactions per card scheme per annum. In general, Visa and MasterCard aligned their merchant levels to be[3]:

- Level 1: more than 6 million total transactions annually
- Level 2: more than one million but less than six million total transactions annually
- Level 3: 20,000 to 1,000,000 e-commerce transactions
- Level 4: all other merchants (MasterCard); or Any merchant processing fewer than 20,000 e-commerce transactions per year, and all other merchants - regardless of acceptance channel - processing up to 1,000,000 transactions per year (Visa).

The other card schemes have different levels because the volume for these cards is normally smaller. If you meet the requirements for Visa or MasterCard you should meet the requirements for the other card schemes.

All merchants must comply with the same standard – PCI DSS. The reporting requirements differ between the levels. Merchant level 3 and 4, where many NFP companies are likely to be, are required to submit annual self-assessment questionnaires (SAQ) along with their respective Attestation of Compliance (AOC) and conduct quarterly external vulnerability scans of their internet perimeter through an Approved Scanning Vendor (ASV).

“Non-compliance with PCI DSS has its consequences.”

[3] See the specific merchant levels at:

http://www.visa-asia.com/ap/au/merchants/riskmgmt/ais_merchants.shtml#Merchant%20Levels

http://www.mastercard.com/au/merchant/en/security/what_can_do/SDP/merchant/levels.html

https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=US&tabbed=merchantLevel

There are four different SAQ’s (A, B, C, D) which have been defined by the PCI SSC to accommodate different operating models for businesses. SAQ A has been developed to address requirements applicable to merchants who retain only paper reports or receipts with cardholder data, do not store cardholder data in electronic format and do not process or transmit any cardholder data on their premises. SAQ B has been developed to address requirements applicable to merchants who process cardholder data only via imprint machines or stand-alone dial-up terminals. SAQ C has been developed to address requirements applicable to merchants who process cardholder data via payment applications (for example, POS systems) connected to the Internet (via high-speed connection, DSL, cable modem, etc.), but who do not store cardholder data on any computer system. SAQ D has been developed for all SAQ-eligible merchants not meeting the descriptions of SAQs A-C. Organisations that must validate against SAQ D are likely expected to validate against all the PCI DSS Requirements. Your acquiring bank should confirm your requirements.

Non-compliance with PCI DSS has its consequences. While the card schemes have broadly aligned their merchant levels and a number of mandates, each card scheme maintains their own compliance program, enforcement procedures and fines. In general organisations suffering a breach and found not to be PCI DSS Compliant will have to address:

- Financial losses
- Reputation and brand damage
- Exposure to legal risks resulting from violating the privacy of cardholders
- Loss of business opportunities as a result of lack of trust
- Impact of downtime resulting from attacks
- Potential payment scheme penalties or termination of facility

In the event of a breach the card scheme may perform a forensic investigation as it deems appropriate, and may assess all investigative costs to the client in addition to any fine that may be applicable[4]. Fines are applied to the acquirer who may then pass the fine onto the merchant. Fines can accumulate on a monthly basis until the entity is compliant and can be very significant, particularly for higher level merchants or where the breach is significant. Fines are not published in Australia.

> “Non-compliance impacts brand reputation and exposes organisations to extensive negative publicity that undermines consumer confidence.”

[4] http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf

From an operational point of view, level 2, 3 or 4 merchants and service providers that have network security breaches, can have their level escalated to level 1. This has an adverse impact in terms of costs since compliance in the level 1 tier is more demanding. In addition, non-compliance impacts brand reputation and exposes organisations to extensive negative publicity that undermines consumer confidence. The ultimate penalty is losing the ability to operate with credit cards.

Overview of PCI DSS Requirements

The following 12 areas are addressed under the PCI DSS. All organisations transmitting, storing or processing cardholder data are expected to be PCI DSS Compliant. In general all areas must be addressed unless specifically excluded under the type of business model you operate in and your eligibility to validate under one of the Self Assessment Questionnaires (SAQ):

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.

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

Requirement 5: Use and regularly update anti-virus software or programs.

Requirement 6: Develop and maintain secure systems and applications.

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.

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Regularly test security systems and processes.

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

The objective of the PCI DSS is to protect cardholder data (CHD). Unfortunately many organisations have deficiencies across all layers from network to operating system, application and information security management and as a result there are inadequate measures to protect CHD.

> “The objective of the PCI DSS is to protect cardholder data (CHD)”

In order to become PCI Compliant all the requirements will need to be addressed; or your scope can be reduced by effectively outsourcing to service providers and adopting a different business model. In order to prioritise your effort we recommend considering the following:

- Review current applications and determine long term objectives for processing and storage of cardholder data. Where possible cardholder data should not be stored because the protective measures that need to be applied to it are complex and onerous. Determine if payment systems will be managed in house or consider revising your business processes and outsourcing part or all of your functions to compliant service providers.

- Review current practices around the handling of printed materials containing cardholder data if more people have access to the materials than require the access.

- Review current practices for hosting technologies, both public facing and internal systems. Engage with service providers that specialise in hosting for regulated sectors where their capabilites can be leverged to address requirements that you are not able to address yourself.

- Organisations may find deficiencies across numerous requirements and may require the assistance of a Qualified Security Assessor (QSA), who is trained to assist organisations deal with understanding and addressing the requirements of the PCI DSS.

> “Sense of Security is a leading provider of information security and risk management services to the NFP sector and their service providers”

About Sense of Security

Sense of Security is a leading independent provider of information security and risk management services to the NFP sector and their service providers in Australia. Our broad spectrum of services includes security governance, risk, compliance, application and network assurance, mobility, virtualisation and audit. We have also developed information security documentation suites specifically adapted to the NFP sector, enabling organisations to readily adopt industry proven frameworks to align with regulatory requirements. Our consultants are information security experts with a thorough knowledge and understanding of the technical, commercial, and regulatory aspects of information and communications technology (ICT) security.

Sense of Security is accredited as a Qualified Security Assessor (QSA) company by the PCI Security Standards Council and employs QSA’s who are authorised and trained to provide these services to assess compliance in line with the Payment Card Industry Data Security Standard (PCI DSS).

Web: http://www.senseofsecurity.com.au
Email: info@senseofsecurity.com.au
Tel: 1300 922 923