



## Achieving Payment Card Industry (PCI) Data Security Compliance for your Organisation

Document prepared by Clinton Alver



## Table of Contents

---

1. Introduction	3
2. Requirements	3
3. Opportunities	5
4. Benefits	7
5. About Salmat VeCommerce	8



# 1. Introduction

The Payment Security Industry Data Security Standards (PCI DSS) was initiated by the major global credit card companies in September 2006 to ensure merchants and other organisations meet their obligations to properly secure cardholder data and combat security vulnerabilities and threats.

Administered by the PCI Security Standards Council (PCI SSC), the standard requires organisations to mitigate the risk of compromising sensitive cardholder data and requires them to address all areas where card data is obtained, stored, transmitted and recorded. Any company handling personal data can be attacked and be liable for losses, even if they themselves do not perform financial transactions.

Although led by card issuers in the United States, PCI obligations are global and have required organisations to comply since December 2007. Failure to comply can result in fines and legal action as well as bad publicity and loss of business.

This paper discusses the obligations introduced by PCI DSS and best business practise in the handling of sensitive customer data to protect customer privacy and security and business integrity.

## 2. Requirements

Many large companies handling personal and financial data generally consider their current security levels to be effective. This may well be the case but in some cases they haven't taken the time to understand all of the areas at risk of threats. Information about the obligations imposed by PCI DSS is not widespread outside the United States and many retail and banking organisations, particularly in Australia<sup>1</sup> have been unaware of their requirements.

Visa and the PCI SSC have reaffirmed that the obligations apply equally in Australia and any company processing, storing, or transmitting payment card data, regardless of their size, must be PCI DSS compliant or risk losing their ability to process credit card payments and facing large fines. Companies must also review their compliance annually through audit or self-assessment.

In March 2007, global retail group the TJX companies revealed that hackers had compromised over 45 million credit and debit cards. From July 2005 until the discovery in December 2006, the fraudsters penetrated a supposedly secure network environment. Even though the data was encrypted, they were able to decrypt and access sensitive data including credit cards, drivers' licences, addresses, dates of birth and other personal data.

Her Majesty's Revenue and Customs lost two disks containing personal information of over 25 million people in October 2007 putting them at risk of identity fraud and theft. Although their security policies are stringent, a weak link in physically transporting the data has had devastating effects.

---

<sup>1</sup> 'Aussie Merchant Card Security Standards a Sham, Nov 2007 <http://m.zdnet.com.au/339283849.htm>



Other organisations including GE Money, Citibank and ABN Amro have similarly faced the costs of repairing the damage from the loss of their customers' personal data.

The PCI DSS outlines 12 security requirements in 6 categories. These categories are summarised in the following diagram.



Figure 1: PCI DSS Categories

Many of the PCI requirements address ways to protect personal customer data in relation to operating systems and physical security, data and systems access, web-facing applications, storage and movement of critical personal data. They mandate that companies should limit the amount of data stored and the retention time to only that which is required for business, legal, and/or regulatory purposes. Sensitive authentication data, even if encrypted, should not be stored subsequent to authorisation. Organisations storing PINs, Credit Card Numbers and other unique identifiers are applying increasing levels of encryption but hackers have been able to respond by breaking this encryption.

A clear advantage in meeting PCI requirements can be gained by avoiding storing and transmitting personal details over public or private web services. This is only practical if an alternative method of customer authentication is available such as biometric voiceprint. Although the payment gateway ultimately needs the card details to make a transaction, this is often housed in a highly secure environment and is not the weak point that attacker's target. By implementing measures which avoid transmitting the sensitive details outside this environment, organisations will achieve the objectives of PCI DSS.



### 3. Opportunities

Salmat VeCommerce, as a solutions provider adheres to the PCI DSS requirements as well as promoting and delivering solutions for organisations themselves to meet the requirements. Under PCI guidelines, PCI DSS requirements are only applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. Salmat VeCommerce's VeSecure Biometric security solutions can eliminate the passing of this data between systems and processes and help keep cardholder data storage to a minimum. Essential data is stored in a highly secure environment but is effectively isolated from other business functions.

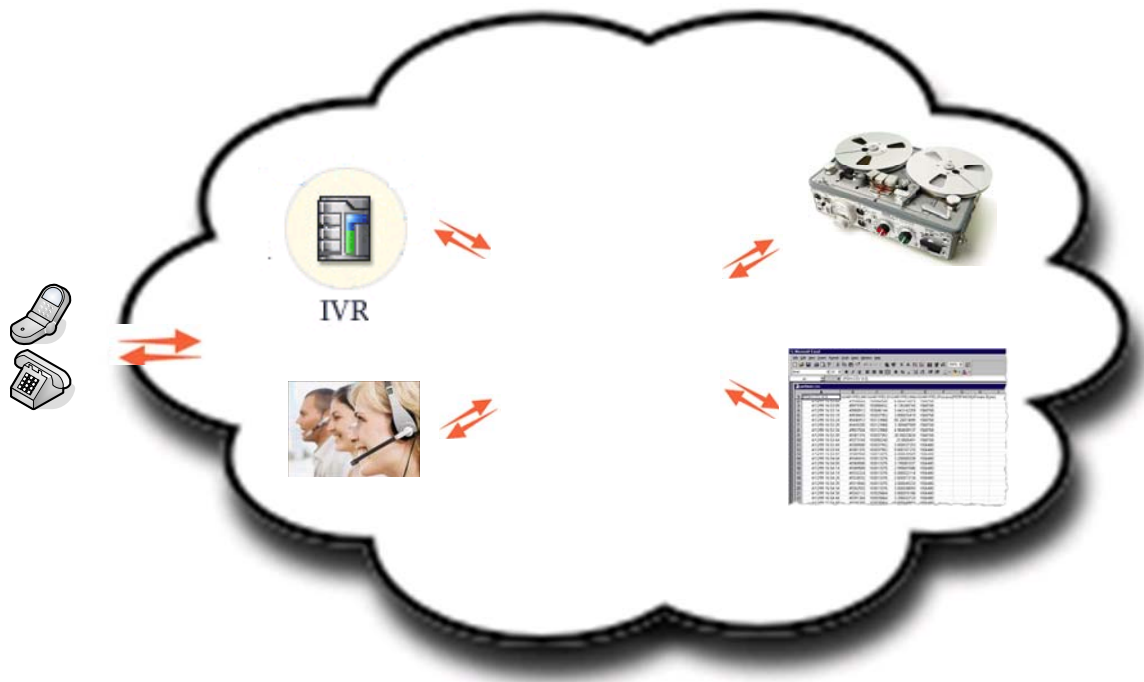


Figure 2: VeSecure isolates sensitive data

The following table outlines each of the PCI DSS requirements and illustrates how Salmat VeCommerce solutions can help address them, not only for compliance purposes but for strategic benefit and enhanced business outcomes.



Requirement Description	How Salmat VeCommerce can help with PCI
<b><i>Build and maintain a secure network</i></b>	
Install and maintain a firewall configuration to protect cardholder data	Firewalls are well defined for data networks but often not for other channels such as voice. VeSecure Biometric allows firewall isolation of voice and data related to multiple channels
Do not use vendor-supplied defaults for system passwords and other security parameters	VeSecure can be implemented for internal security as well as customer facing purposes. This eliminates the ability to compromise system passwords.
<b><i>Protect cardholder data</i></b>	
Protect stored cardholder data	By using biometric voiceprint, sensitive cardholder data can be retained within the highly secure environment. Only a non-sensitive customer identifier need be transferred between systems and an indication of verification and payment status.
Encrypt transmission of cardholder data across open, public networks	Many levels of encryption are able to be broken by hackers. Salmat VeCommerce solutions encrypt data as a matter of course but greater security is achieved by eliminating the need to transfer cardholder data across networks.
<b><i>Maintain a vulnerability management program</i></b>	
Develop and maintain secure systems and applications	Salmat VeCommerce solutions have been deployed for numerous customers worldwide in all industries including financial services and government. We pride ourselves on uncompromised solutions that deliver real value.
<b><i>Implement strong access control measures</i></b>	
Restrict access to cardholder data by business need-to-know	Data and physical access can be controlled using VeSecure Biometric and a risk or role-based access control policy.
Assign a unique ID to each person with computer	Using VeSecure Biometric to protect access to



access	internal data provides an audit trail that can identify individuals beyond repudiation, something a simple password or access card cannot do.
Restrict physical access to cardholder data	If required, physical access systems can be linked to the same voiceprint policy as data access ensuring consistency in access control.
<b>Regularly monitor and test networks</b>	
Track and monitor all access to network resources and cardholder data	Solutions are designed with full monitoring and access logging. This can provide separate reports or integrate into organisational management reporting.
Regularly test security systems and processes	Salmat VeCommerce systems support provides full maintenance, ongoing testing and audit to ensure optimal solution performance and security.
<b>Maintain an information security policy</b>	
Maintain a policy that addresses information security	Salmat VeCommerce solutions align to existing security policies and our consulting team can provide assistance or audit where required.

## 4. Benefits

Being PCI Compliant is not just about compliance, it is good business practise. Those organisations that embrace it as a strategic opportunity and differentiate themselves in the market will achieve rapid return on their investment rather than facing a cost burden. The high level benefits to the organisation include:

- Protecting corporate intellectual property and brand
- Protecting customer security and privacy
- Reduction in cost and time spent resolving a data breach
- Reduction in negative publicity and lost business caused by a data breach
- Increased customer and staff satisfaction
- Efficiency gains leading to increased revenue opportunities

Many companies are struggling to comply and find that although the principles of PCI DSS make sense, the detailed requirements remain unclear. Visa have estimated that on around 40% of companies comply or are addressing their obligations, despite the fact that compliance attracts lower payment processing fees and avoids substantial fines. Apart from these direct financial implications, industry analysts highlight the significant costs involved for a company in rectifying a breach of their sensitive data:



“If companies readily followed PCI DSS obligations, the savings for the company would far outweigh the financial burden of correcting a data breach after it happens<sup>2</sup> 60% of customers do not typically return to a merchant where they have had their card information stolen from”

## 5. About Salmat VeCommerce

Salmat VeCommerce Limited is a global leader in the provision of natural language speech recognition (NLSR) and speaker verification solutions. With over 23 years experience in the communications and call processing industries, its core focus is to provide tailored business solutions, using the latest in communications and speech technologies. These solutions allow callers to be accurately and quickly routed to the most appropriate resource, or to complete complex but routine transactions or enquiries without the need to struggle with frustrating push button menus or having to wait for an available operator to answer their call.

With one of the largest Speech Recognition and biometric Speaker Verification resource pools in the industry today Salmat VeCommerce has successfully implemented more than 100 commercially deployed speech solution projects globally, including the first public rollout of biometric voice verification for Australian health services organisation AHM. With specific business drivers such as improved customer service, improved security, reduced call length and increased call value for both members and agents. 95% of AHM members offered the use of voice biometrics choose to enrol.

In June 2006, Salmat VeCommerce was acquired by Salmat as part of its strategic acquisition program. The acquisition positions Salmat as a leader in enhancing customer experience through speech and voice biometric solutions, call centre outsource, business process outsourcing, document management and distribution.

Salmat VeCommerce’s head office is located in Sydney with regional offices throughout Australia, New Zealand, North America, the United Kingdom and Asia.

---

<sup>2</sup> Richard Stanton, CTO Controlscan