How to achieve complete Payment Card Industry Data Security Standard, (PCI DSS) peace of mind

Adoption of the PCI DSS by all payment card brands presents a huge challenge for contact centres, as many handle sensitive customer payment card information on a daily basis. In this whitepaper we will discuss what you can do to help pass a PCI DSS audit and be certified as having implemented the processes and technology to comply.

What is PCI DSS?
The PCI DSS is the global data security standard adopted by the payment card brands for any organization that processes, stores or transmits cardholder data. The PCI DSS has become the global standard for protecting cardholder data. The standard has evolved over time as newer technologies have become available and there is ever-greater pressure from payment providers to ensure that organisations utilising a customer’s financial details adhere to it.

Why should I comply with the standards?
PCI compliance is an increasingly crucial part of providing a quality service to your customers. What’s more, it can actually deliver a good number of business benefits, including:

• Ensuring that your systems are secure, meaning your customers can trust you and are more likely to buy with confidence.

• Enhancing your reputation with payment providers and allowing you to do business more easily

• Future-proofing your contact centre, as fraudsters and criminal activity develops and becomes more sophisticated; the PCI Security Standards Council is continually working to stay ahead.

• You are more likely to be compliant with other regulations as they come along – and it may even help you create more efficient and effective IT systems.

Plus, there are many negative consequences if you do not become compliant, including: potential reputational damage if just one customer’s details are compromised, negative impact on share price after an incident, possible insurance claims and large fines.

While we have researched this topic extensively, we are not affiliated with the PCI Security Standards Council (SSC). The information presented in this whitepaper does not replace PCI SSC Security Standards or their supporting documents. Full details can be found at www.pcisecuritystandards.org
So how can I achieve compliance?

The table below summarises the PCI DSS goals and how to achieve them:

<table>
<thead>
<tr>
<th>Goal</th>
<th>How to achieve it using PCI DSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and maintain a secure network</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect cardholder data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a vulnerability management program</td>
<td>5. Use and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement strong access control measures</td>
<td>7. Restrict access to cardholder data on a need-to-know basis</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly monitor and test networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an information security policy</td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>

Requirements 1, 2, 6, 7, 8 and 10 are all functions of the customer network infrastructure and the features implemented by the system integrator. You should make sure that your networking infrastructure is configured with the following features to address these requirements:

- VLAN segmentation (Requirement 1)
- 802.1x authentication (Requirements 7 and 8)
- Encrypt access to the switches using Secure Shell Protocol (Requirement 2 and 8)
- Restrict and log access using built-in authentication techniques (Requirement 2 and 8)
- Implement timed session terminations (Requirement 2 and 8)
- Track users through integrated, hardware-enabled Cisco NetFlow to audit network usage (Requirement 10)
- Users (e.g. Homeworkers) utilise a IPSEC/SSL VPN over any public network (Requirement 4).

Requirements 5, 6, 11 and 12 must be addressed through implementing the required business processes – ask your systems integrator to ensure they are met.

What does all this mean in terms of the technology used in my contact centre?

The key issue for contact centres when meeting PCI DSS compliance revolves around the recording of calls. Many call centres want to voice record calls in order to gain business insight and as a training and improvement tool. However, any stored recordings of customer payment data break PCI DSS rules. Traditionally, two main methods have been used to address the challenge where calls are recorded:

1) **Encryption of call recordings**: Many organisations believe that encrypting their call recordings will manage the risks of storing sensitive card data. However, according to PCI rules, the CVC2/CVV2 security code should not be stored under any circumstances, even if it is encrypted.

2) **Stop/Start application controlled call recording**: Pausing the call recording at the moment a payment is being taken is often suggested as a way for call centres to comply with PCI DSS. But with this method, both the agent and the desktop they are using are still within scope for PCI DSS, as the sensitive data passes through them. Also, errors can be made – for example if the customer gives their details at the wrong time, or if the agent notes down some of the details to help with the transaction.
Be warned!

If you are using either of these methods, additional safeguards are required in terms of accessing the recordings that are stored. Vocalcom’s Hermes.Net software provides role-based access whereby certain users have privileges for access to certain recordings. Users must be configured and licensed by an administrator prior to being given access. This could involve specific solutions such as user ID assignment, first time passwords, user termination, time limited accounts, password strength requirements, time limits, and lockouts.

How can I be sure I am meeting PCI DSS requirements?

Many organisations and compliance officers would say that the only effective way to ensure you are meeting the requirements is to remove the contact centre completely from the scope of PCI regulations. This ensures customer security and compliance with PCI standards, as well as avoiding the ongoing cost of securing your infrastructure. Typically, this has been done using a third method:

3) Automated IVR payment solutions: Using voice recognition or keypad entry, these systems allow payments to be taken without the card details being recorded.

Be warned!

Although this third option is viewed as a compliant methodology, the conversion rate of completing payments may be lower when compared to dealing with an agent.

The perfect solution?

The Vocalcom Hermes Software suite is able to provide both method 2) “Start/Stop Recording” and method 3) “Automated IVR” payment solutions (Vocalcom considers encryption of call recordings a non-compliant methodology).

However, Vocalcom believes there is a more compelling solution where an agent is present on the call during an automated IVR Payment. The agent simply conferences an IVR application developed in Vocalcom’s Interface designer environment into the call with the customer. The IVR application goes through the relevant prompts requesting card details which a customer types in using their DTMF keypad. The DTMF tones are masked in the application so that the agent cannot hear them. However, the agent is able to coach the customer through the transaction or restart the IVR application should an error or mistake be made.

In order to be compliant with transmission of card details utilising DTMF, Vocalcom enables customers to use TLS/SRTP encryption technologies. Standard secure Webservices encryption methodologies can then be used to communicate the card details to a payment gateway provider of the customer’s choice.

This enables full PCI compliance within the application, with no storage of card details on voice recordings, whilst maintaining the conversion rates of dealing with an agent directly.

About Vocalcom

For almost two decades, Vocalcom has been helping clients to maximise proactive customer contact through their innovative contact centre application suite. Founded in 1995, Vocalcom is a privately owned global company that has consistently grown by 20% each year.

We are 100% focused on contact centres. We have created a highly competent team that combines contact centre operational management experience with a unique understanding of how to leverage technology to improve performance.

Our award-winning and market-leading contact centre application is developed in both Europe and North America, helping us to create a truly world-class solution that is focused on and reflected by local requirements.

Our goal is the constant improvement of our contact centre application suite that enables organisations to transform the way they interact with their customers – our ability to do this is proven by the fact that Vocalcom is being used by over 600,000 agents within 4,500 organisations across 40+ countries.

To find out more about Vocalcom, please visit our website www.vocalcom.com