

White Paper On



PCI DSS Compliance
And Voice Recording Implications

PCI DSS within the UK is becoming a hot topic of conversation, with many contradictions and confusions being issued by suppliers and professionals alike.

We would like to share with you the information we have collated on this topic, together with direct feedback from some of our clients who have recently passed the PCI DSS compliance audits

So, What is PCI DSS?*

The **Payment Card Industry Data Security Standard (PCI DSS)** is a worldwide information security standard defined by the Payment Card Industry Security Standards Council. The standard was created to help organisations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to **all organisations which hold, process, or exchange cardholder information from any card branded with the logo of one of the card brands.**

Validation of compliance can be **performed** either **internally or externally**, depending on the volume of card transactions the organization is handling, but regardless of the size of the organization, **compliance must be assessed annually**. Organisations handling **large volumes of transactions** must have their compliance assessed by an **independent assessor** known as a **Qualified Security Assessor (QSA)**, while companies handling smaller volumes have the option of self-certification via a Self-Assessment Questionnaire (SAQ). In some regions these SAQs still require signoff by a QSA for submission.

Enforcement of compliance is done **by the bodies holding relationships with the in-scope organisations**. Thus, for organisations processing Visa or MasterCard transactions, compliance is enforced by the organisation's acquirer, while organisations handling American Express transactions will deal directly with American Express for the purposes of compliance. In the case of **third party suppliers** such as hosting companies who have business relationships with in-scope organisations, **enforcement of compliance falls to the in-scope company**, as neither the acquirers nor the card brands will have appropriate contractual relationships in place to mandate compliance. **Non-compliant companies** who maintain a relationship with one or more of the card brands, either directly or through an acquirer, **risk losing their ability to process credit card payments and being audited and/or fined.**

* Source : From Wikipedia, the free encyclopaedia.

What are the main areas that are assessed?

The PCI DSS assessment specifies **12 requirements** for compliance, **organised into six** logically related **groups**, which are called "**control objectives.**" Version 1.2 is the most current version of the standard.

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

By looking at the standards, the main focus is for organisations to protect and monitor all access to data appertaining to credit card transactions, by using consistent, secure processes and procedures in-house. This will prevent unauthorised access to the information at all times, as well as restricted access to the data internally too.

I use voice recording technology in our operation, is this technology also included in the scope of PCI DSS?

Yes, voice recording technology is considered within an PCI DSS audit and the method of access, playback and data capture is assessed.

There has been a recent update announced by PCI DSS , relating to the capture of cardholder data and/or authentication data. The response can be seen below. The original source can be found via the PCI DSS Security Standards Council website, **under FAQ** <https://www.pcisecuritystandards.org>

Question: *Are audio/voice recordings containing cardholder data and/or sensitive authentication data included in the scope of PCI DSS?*

This response is intended to provide clarification for call centres that record cardholder data in audio recordings, and applies only to the storage of card validation codes and values (referred to as CAV2, CVC2, CVV2 or CID codes by the payment brands).

It is a violation of PCI DSS requirement 3.2 to store any sensitive authentication data, including card validation codes and values, after authorization even if encrypted. It is therefore prohibited to use any form of digital audio recording** (using formats such as wav, mp3 etc) for storing CAV2, CVC2, CVV2 or CID codes after authorization if that data can be queried; recognizing that multiple tools exist that potentially could query a variety of digital recordings.

Where technology exists to prevent recording of these data elements, such technology should be enabled.

If these recordings cannot be data mined, storage of CAV2, CVC2, CVV2 or CID codes after authorization may be permissible as long as appropriate validation has been performed. This includes the physical and logical protections defined in PCI DSS that must still be applied to these call recording formats.

This requirement does not supersede local or regional laws that may govern the retention of audio recordings.

PCI DSS section 3.2 stipulates :-

3.2 *Do not store authentication data subsequent to authorisation (not even if encrypted): Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3*

3.2.1 *Do not store the full contents of any track from the magnetic stripe (located on the back of a card, in a chip or elsewhere) This data is alternatively, called full track, track 1, track 2, and magnetic stripe-data. Note: in the normal course of business, the following data elements from the magnetic stripe may need to be retained:*

- *The cardholders name*
- *Primary account number (PAN)*
- *Expiration Date*
- *Service code*

To minimize risk, store only these data elements as needed for business.

** This does not mean that you cannot use a Digital recorder in your operation.

3.2.2 *Do not store the card-verification code (three-digit or four digit value printed on the front or back of a payment card used to verify card not present transactions. (e.g., CVV2, and CVC2 data))*

3.2.3 *Do not store the personal identification number (PIN) or encrypted number block.*

PCI DSS 3.4 is also relevant, as it appertains to storage procedures and would include voice recording storage too. It reads:

3.4 *Render PAN at minimum, unreadable anywhere it is stored, (including on portable digital media, backup media, in logs) by using any of the following approaches*

- *One way hashes, based on cryptography*
- *Truncation*
- *Index tokens and pads (pads must be securely stored)*
- *Strong cryptography with associated key management processes and procedures*

The MINIMUM account information that must be rendered unreadable is the PAN

What Does ComputerTel suggest to assist companies that operate voice recording technology and who wish to be PCI DSS compliant?

As far as we are aware to date, there does not appear to be a fully compliant PCI DSS voice recording solution, accredited by PCI DSS, currently on the market. Companies have looked at ways of complying to the guidelines issued by PCI DSS, but we are unaware that PCI DSS have issued any companies a compliance status.

ComputerTel suggest that any sensitive authentication data information appertaining to a credit card CVV code that is issued over the telephone **must not** be stored after it is issued, in order to comply with PCI DSS requirements. The CAV2/CVC2/CVV2/CID may not be stored after authorisation in any format.

Our suggestions to meet PCI DSS compliance, as well as other compliance issues that conflict, like FSA compliance issues on recording calls, are as follows:-

- **Look at a possible Business process change – do not record card transactions by default**
- **Do not record card holder details**
- **Record card holder details but not CAV2/CVC2/CVV2/CID**
- **The only ways to achieve a workable solution, in our opinion, is by integrating your CRM/Credit card payment system with the recording solution Application Programming Interface (API). This will allow calls to be muted whilst taking sensitive material of the credit cards and resume once the details have been given. Alternative solutions involve transferring credit card transactional calls to a non recorded telephone line or IVR line.**

How do I Integrate My Recording Solution Effectively?

We suggest that you consider following these recommendations.

- A link is required between the screen context, agent, agent phone and current recording
- Using the link, recording must be controlled through integration with all the systems
- The level of integration will determine the required compliance level
- Manual stop start recording or muting is not a recommended solution. A method of using a phone pad to create DTMF tones may be PCI DSS compliant, but it will not be FSA complaint either. DTMF tones can be decoded, so, in the case of a Best Practice Insurance or Banking related Contact Centre, FSA regulations, Sarbanes Oxley regulations etc. also need to be considered too.

So what other tips can you offer us to help with our PCI DSS audit?

Treat PCI DSS as an important project.

Companies often try to fit PCI DSS around existing projects. If they have different priorities or more intense projects occurring simultaneously, PCI DSS may be fitted around these. That means the compliance deadline is tied to that of the main project. The main project roadmap may be up to three years, but as long as the company can show that key areas are being addressed, such as encryption of credit card numbers, restriction of access to information etc., then subject to assessment guidelines and acceptance, this could be acceptable.

Look at the way you currently work, analyse current methods and procedures, then review and implement new or revised processes and procedures that are necessary to reduce the scope of the PCI DSS programme.

Companies should adopt more control over the movement and usage of credit card data. . One of the best ways to tackle PCI DSS is to restrict the number of areas where card data is allowed to go. By limiting where card information can be obtained within an organisation, it is possible to reduce the threat of a breach, and also to cut down the job of compliance. So in effect, if you don't need it, don't share the information, or allow access to it.

In order to achieve this, look at each department that **has access to** credit card details, then look at which departments **need** access to Credit card details, which will then let you look at ways that you can restrict access. Processes and procedures should then be created, or amended that can be followed by the entire organisation.

It is imperative that all departments involved in helping to meet PCI DSS compliance are involved in the planning, managing and implementing of processes and procedures to obtain compliance. Sharing this information and monitoring progress, implementing internal consequences if this is breached and making it a matter that affects the entire organisation, will help make this an acceptable method of operation.

Focus your PCI DSS efforts.

Some companies believe the standard needs to be applied across the whole infrastructure in the same way. In reality, you can apply stricter controls in important areas, and be less stringent in other part of the systems. However, if you follow the previous suggestions and make it a way of operation across the board, then all areas will be working in the same way.

Compliance is not enough.

Ticking all the boxes to become PCI DSS compliant may still not guarantee that you are secure, and one Qualified Security Advisor (QSA) may interpret the standard differently from another.

PCI DSS is not a complete solution, especially on internal security; it is not a bulletproof solution. Like with everything, if there is a way to bend or break the rules, breach security or act inappropriately, there are ways to be compromised. Don't stop once you have achieved compliance. There is always more that a company can do. Treat it as an exercise in continual improvement and keep trying to improve it.

A final Helpful tool – “Risk Prioritised Approach”

Another helpful tool is the "risk prioritised approach," a set of best practices issued by the PCI Security Standards Council on where to address the most serious PCI DSS risks.

(The guide is downloadable at

<https://www.pcisecuritystandards.org/education/prioritized.shtml> .)

About ComputerTel

ComputerTel is a well established Telecommunications Company specialising in the supply of Call Recording and Quality Monitoring solutions, as well as Speech Analytics, PC Screen Recording and E-learning solutions. All these systems have been designed to improve call quality and productivity within the Contact Centre and Service Industry market.

During ComputerTel's 21 year existence, the company has continued to develop and grow, winning several awards on the way. Having mainly started as a supplier to the financial markets, where recording of telephone calls is essential, the company has successfully expanded into the Contact Centre and Service Industry serving nearly 300 customers, many well known, such as National Express, lastminute.com, Epson, Hillary's Blinds, South African Airways to name but a few.

Contact Details:

ComputerTel Ltd., CTL House, 52 Bath Street, Gravesend, Kent. DA11 0DF.

Tel: 01474 561111 Email: info@computertel.co.uk Web: www.computertel.co.uk