



Payment Card Industry (PCI)
Compliance for Call Recorders in a Contact centre

A White paper by Steve Donovan

Xarios Ltd

0845 3736880

steve.donovan@xarios.com

Contents

Payment Card Industry (PCI)	1
Contents	2
Introduction	3
Regulations, Rules and Regulations!	4
UK Law	4
The FSA.....	4
Data Protection.....	4
OFCOM	5
Who or What is PCI SSC?	6
What is the DSS?.....	6
So what must not be recorded?.....	6
The dilemma for Call Recording.....	10
PCI Compliance v Dispute Resolution.....	10
What are the various technical solutions to the problem?	11
DTMF tones over the call.....	11
CTI Software Application.....	11
What are the problems with these two methods?	11
What about speech recognition?	12
Is it possible to automate Stop/Start?.....	13
What is PCI-Mute?.....	13
Web Service	13
Xarios CTI software application.....	13
OCX control.....	13
.NET DLL	14
Remoting	14
Conclusion.....	15
About Xarios Ltd	16

Introduction

www.xarios.com

Call recording equipment in contact centres is subject to a range of government legal and regulatory constraints driven on the one hand by the need to record financial advice given to consumers required by the Financial Services Authority (FSA), and on the other hand by The Regulation of Investigatory Powers Act which provides a business with the right to record calls to monitor staff activities.

In addition to these regulations that say "You must record calls" there are regulations designed to prevent credit card fraud that say "Do not record calls"

This white paper seeks to explain what can and can't be recorded, what the regulations say and how to get more detailed information on the regulations.

However the primary objective of this document is to explore the practical and technical issues on the call recorders themselves raised when the regulations conflict (i.e. when one regulation says "record" and another says "don't record")

PCI compliance presents a business with a range of technical headaches. Xarios has the ability to provide solutions to these problems for the voice technology in your contact centre.

The Xarios call recorder can handle sites from 8 to 800 trunk lines with or without the compliance module delivering a range of features designed to address a call centre's requirement to comply with the various regulations surrounding call recording

Regulations, Rules and Regulations!

With the primary objective of protection for the consumer, the government has established several regulatory bodies that impose the regulations covering a range of issues including telephone call recording.

UK Law

There are in fact two main aspects of call recording:

1. The physical act of recording and monitoring of calls and
2. The storage and handling of the resulting recordings (the data)

[The Regulations of Investigatory Powers Act](#) was passed in July 2000. This is the legal framework covering the recording and monitoring of telephone calls. It states requirements with Lawful Business Practice Regulations are complied with on behalf of sender and recipient.

[The Lawful Business Practice Regulations](#) came into force in October 2000. This identifies situations when an organisation may record a conversation. It shows how a business provides evidence of a transaction that is used to meet quality standards or check that targets are being met.

For more details see:

http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1

<http://www.opsi.gov.uk/si/si2000/20002699.htm>

The FSA

The Financial Services Authority regulate "financial markets" but have a stated aim to "help retail consumers achieve a fair deal"

See the following for more detailed information:

http://www.fsa.gov.uk/pubs/policy/ps08_01.pdf

These regulations set out the rights and requirements of businesses and individuals to record calls but once the call is recorded, and depending on the content of the conversation, the resulting "data" stored electronically may be subject to the Data Protection Act

The FSA also state that call recording must be "easily accessible"

Data Protection

When a call has been recorded it is covered by the [Data Protection Act, 1998](#). The recorded call comes under the form of private data stored electronically (Part II of the Data Protection Act 1998 section 7 - Rights of Data subjects and others).

See the following for more detail:

http://www.ico.gov.uk/what_we_cover/data_protection.aspx

OFCOM

[OFCOM](#), the independent regulator and competition authority for the UK communications industry states: "you have to take reasonable steps to ensure both parties are aware that the call may be monitored or recorded to demonstrate, if required, that you have done so."

"Reasonable steps" are not defined by legislation or by OFCOM. It must be decided by the company what is reasonable. In practice it would make sense to inform both parties in a clear and precise manner and understand the policy of what is recorded and under what conditions (Part II of the Data Protection Act 1998 section 7 – Rights of Data subjects and others).

It is not illegal to make a recording or listen to it as long as you have taken the "reasonable steps" to let both parties know that a recording is taking place. This does not cover employers recording private calls made by employees.

Steps should be taken to notify customers that a recording is taking place. Customers can be notified by a simple message at the beginning of the call (e.g. "calls may be recorded for quality and training purposes") or a statement on a brochure or website.

See the following for more detail:

<http://www.ofcom.org.uk/>

So far we have addressed that calls *can* be recorded and that when we record calls we have a duty of care to *protect* the playback of these calls from unauthorised access.

But what if there were regulations that insisted that, based on the content of the call, either the entire call or worse still only *part* of the call must not be recorded at all?

Well its no surprise that such regulations exist but in this case the regulations are driven by not only consumer protection, they are driven by a commercial imperative to prevent cash losses – Credit Card Fraud

At the time of writing and notwithstanding the introduction of chip and pin technology, Credit Card Fraud in the UK is estimated at over half a £1BN per annum.

The losers are Consumers, the banks but also the traders i.e. the contact centres taking payment card details over the phone.

Not surprising then that the latest regulation to affect our industry is from the Payment Card Industry itself.

Who or What is PCI SSC?

The "Payment Card Industry Security Standards Council" was setup and is enforced by the founding members consisting of:

VISA
Mastercard
American Express
JCB International
Discover Financial Services

What is the DSS?

The PCI "Data Security Standard" (current version 1.2) is a set of guidelines issued by the PCI SCC that if followed will minimise if not eradicate credit card fraud and cover a range of measures to protect card data once stored but also sets out what can and can not be recorded electronically in the first place.

Its states that sensitive card data should be encrypted when stored and that there should be clear rules and security measures taken to prevent unauthorised access to the data. In simple terms this can mean a controlled password is required before the data can be seen but can also include specific measures to maintain firewall protection to segregate database servers from a network that could pose a threat (apart from the obvious one – the public Internet)

So what must not be recorded?

The following table is lifted from the DSS guidelines and sets out what can and can not be recorded electronically. **The key thing to remember is that the customer's 3 digit Card Verification Value (CVV) code – i.e. the last three digits on the signature panel on the back of the card, must not be recorded anywhere.**

That includes in a database or in a recorded telephone call.

Guidelines for Cardholder Data Elements

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name ¹	Yes	Yes ¹	No
	Service Code ¹	Yes	Yes ¹	No
	Expiration Date ¹	Yes	Yes ¹	No
Sensitive Authentication Data ²	Full Magnetic Stripe Data ³	No	N/A	N/A
	CAV2 / CVC2 / CVV2 / CID	No	N/A	N/A
	PIN / PIN Block	No	N/A	N/A

For an overview of the PCI SSC and the DSS see:

<https://www.pcisecuritystandards.org/>

Jan 2010 DSS update

In January 2010 the PCI SSC issued a clarification to its guidelines making explicit reference to call recording in contact centres. Here is the verbatim wording of the clarification:

“PCI SSC FAQ’s are designed to provide merchants, assessors, acquirers and other Council stakeholders with clear and timely guidance on PCI standards. They are a critical two way communication channel from which the PCI SSC draws valuable market feedback and insight, and is able to share this with the industry. On January 22 2010, as part of the online FAQ feedback and submission process, the regular review of FAQ language, and inquiries from Participating Organizations the SSC sought to clarify its position on call centre audio recordings.

The updates to the FAQ language were intended to eliminate any inconsistencies in implementations of audio recordings in call centre environments by providing a higher level of specificity in FAQ guidance. The Council’s position remains that if you can digitally query sensitive authentication data (SAD) contained within audio recordings - if SAD is easily accessible - then it must not be stored. As a result of additional market feedback, on February 17, 2010 the SSC modified the new language to further clarify its position on audio recordings.

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”

Interpretation

The statement repeats the primary point made above. Namely that it is a clear violation of the Payment Card Industry Data Security Standard (PCI DSS) to store the 3 digit CAV2, CVC2, CVV2 or CID code even if encrypted. In fact it explains that the statement refers "only" to the 3 digit code.

Therefore by implication it confirms that it is NOT a violation to store the other card data although access to that data must be restricted and encrypted.

Therefore if you operate a contact centre that takes credit card payments over the phone AND you ask the customer to tell you the 3 digit CVV code on the reverse of the card, you must not store that data in the call recording (i.e. you must pause/resume the call)

I would make the case that using a DTMF (Tone Dialling) solution to take the CVV code is technically a breach of the guidelines. Despite the fact that the data may be encrypted and awkward to decipher (it is possible to use a DTMF decoder downloaded for free onto an iPhone for example), the fact that the CVV code is being stored is what constitutes the breach.

Conversely if you operate a contact centre that takes payments over the phone where it is not required to take the CVV code, it is not necessary to employ technology to mask or pause/resume the card data. It is however necessary to follow the remaining guidelines to encrypt and password protect the data.

It goes on to say that "where technology exists to prevent recording, such technology should be enabled"

Since most policy statements make a concerted effort to be ambiguous, this one makes a valiant attempt by adding the following point:

"If these recordings can not be 'data mined' storage of the CVV code may be permissible"

This means that there must be no means by which these recordings are easily accessible. So if for example you recorded the call then immediately removed the call recording from the call recorder's database so that it could not be found and played back by a supervisor or team leader and the data was placed in a secure location, it "may" be permissible to record the CVV code.

Since this would effectively render the call recorder useless for the normal purposes of quality control and dispute resolution, I would rule this out as interpreting the statement as a relaxation of the requirement to employ technology that can pause/resume or mask the CVV card data.

What does "Data Mining" mean?

Well it's sufficiently complex to need its own Wiki page! ...

http://en.wikipedia.org/wiki/Data_mining

In this context it means the ability to use a search method to for example find all the call recordings containing a CVV code and that a typical call recorder user interface can't do that.

Some call centre manager may interpret this to be a loophole but I disagree

Do call recorders with speech analytics breach PCI compliance?

I believe this is irrelevant since you should not store the CVV code in the first place

If its possible to use speech analytics to search for all the calls containing the phrase "What's your credit card number?" then I would say that speech analytics could be interpreted to constitute "data mining" and this would I believe breach PCI compliance for call centres that store the credit card number but do not have to store the CVV code

In which case make sure your speech analytics module contains a phrase exclusion list to enable you to bar searching for phrases that might return multiple calls containing "what's credit card number?"

The dilemma for Call Recording

There are some clear technical and practical issues created by the conflict between opposing regulations. The dilemma for contact centres is how to comply with all the regulations in a reliable way not only technically but also practically.

The fundamental dilemma is that one set of regulations say "record the call" and another set of regulations say "don't record the call"

Before we get into the technical issues there is inevitably going to be some trade off and the task can only be to minimise the impact to the business for a failure to comply.

PCI Compliance v Dispute Resolution

One way to comply with PCI is simply not to record calls for agents who handle credit card payments.

However if the contact centre chooses not to record any calls handled by staff taking credit card payments they forfeit their Dispute Resolution capability.

Even if the contact centre finds a way to pause the call recording at the precise moment and resume the recording after the CVV code is spoken there could still be a scenario where the dispute itself pertains to the credit card data and clearly there is no solution that could deal with this.

What are the various technical solutions to the problem?

If the problem is defined as "How do we record all calls but stop recording when the CVV code is requested and re-start recording when that data has been collected", there are various methods

DTMF tones over the call

One way call recorders can stop a recording is set up a dial string that the agent keys into their phone during the call to stop the recording and a different dial string to restart the recording.

For example when the agent reaches the point when a caller is about to divulge the CVV code the agent could dial say **3 over the call. The agent would then listen to the CVV code, enter the code into the merchant payment software and then dial say **4 to restart the call recorder.

DTMF tones as a means to collect the card data

Some solution providers support the ability to ask the customer to enter their card data using the keypad on their telephone so that the agent can not immediately understand and supervisors can not later play back the information

As described above, this is OK if there is no requirement to collect the CVV code but any scenario where the 3 digit CVV code "stored" (even if encrypted) is a violation of the standard

CTI Software Application

It is possible for a Computer Telephony Software application to display the current state of the call recording and show the agent say a red light when the call is being recorded.

This software can also be designed to have a button the agent can click or a keyboard function the agent can key that stops and starts the call recording

What are the problems with these two methods?

1. Both are open to abuse.

A rogue agent could decide to abuse the caller and stop the recording at any time during the call

2. Both are susceptible to human error.

The agent could simply forget to stop the recording or alternatively an agent who is not so IT competent could get finger trouble flipping between software applications or dial the wrong DTMF tones and the process would fail.

What about speech recognition?

Some vendors use speech recognition to detect when a caller or agent say words that could imply that a CVV code is about to be spoken. In theory you could program the recorder to detect "can I have your CVV code please?"

This should cause the recorder to stop the recording the call and it will then be necessary the program a restart "trigger" phrase such as "OK thanks for your CVV code"

The problem with this method is similar in that it relies not only on accurate speech recognition of thousands of different accents let alone foreign language contact centres, but it also relies on the agent to say the correct phrases and they could either forget to say them or intentionally choose not to.

Is it possible to automate Stop/Start?

Yes! As well as the other methods discussed above Xarios have developed a CTI software component that can detect where in the agents screen or software the current focus is and can automate the task of stopping and restarting the call recorder.

What is PCI-Mute?

PCI-Mute is the brand name of the PCI compliance component for the Xarios call recorder and is available in various forms.

The idea is to remove agent intervention and connect the logic of the call recorder start/stop function to the logic of software that collects the credit card data.

Typically the credit card data collection application provides a browser user interface but there are various other ways to handle the problem

Xarios have developed a CTI software program Application Programming Interface (API) that runs in a Microsoft environment that detects the software status and provides a command to start and stop the call recorder automatically based on what software the agent is currently running on on their computer

Web Service

The web service API will allow any credit card collection software user interface running in a browser to call a function to stop the recorder and for example would support a web page written in ASPX

Xarios CTI software application

This involves installing a software application onto the user's computer that detects Microsoft forms and can be configured to automatically stop the call recording when a user loads a specific form in any software application that is used to collect the CVV code.

When the user moves away from that form to another, the call recording can be automatically restarted.

OCX control

If the software application that takes the card data is written in Visual Basic (VB) or Visual Basic for Applications (VBA) such as Microsoft Access database, it is possible to use the Xarios API in the form of an OLE Control Extension (OCX).

In the same way as the web service, the developer can automate the process of stop/start

.NET DLL

The latest software development environment from Microsoft is .NET and the API can be used by embedding the Xarios .NET Dynamic Link Library (DLL) component inside the users software application.

.NET Remoting

.NET Remoting is the term for calling an API method within a .NET environment that uses a secure connection to a server application to pass data

Command Line Argument

Use a Command line argument that calls our .NET remoting feature. If the software environments fail to provide a compatible way to embed a component to perform the task, the last (and sometimes the only) option is to simply "shell" a command line.

For example the software developer could call a shell command line such as:

```
C:\Program Files\Xarios\PhoneManagerCTI.exe /Stop_Rec
```

Conclusion

This whole thing is a complex and difficult subject but the key issue is that PCI compliance is here stay and the technology exists to be compliance whilst still meeting obligations to record calls

Having five different ways to use the API for the Xarios call recorder to automate the process of stop/starting call recording, contact centres can comply with ALL the conflicting regulations surrounding compliance in the UK.

The Xarios professional services team can help your contact centre with the integration project and take the headaches away from your compliance issues.

About Xarios Ltd

Xarios Ltd is an independent software development company specialising in telephony oriented software applications.

The Xarios call recorder can handle sites from 8 to 800 trunk lines with or without the compliance module delivering a range of features designed to address a call centre's requirement to comply with the various regulations surrounding call recording.

With development offices in Manchester, and Beijing and support offices in Phoenix USA, the company is a Microsoft Gold Partner and has attained the ISO 9000-3 quality standard for software development as well as accreditation for API integration to various PBX manufacturers.

Standard products include Call Recording, CTI and CRM integration and Progressive diallers.

The company also designs a range of bespoke applications such as IVR and custom CRM integration.

See www.xarios.com for more details