ENCODED
secure automated payments

Encoded Ltd
Spectrum House Beehive Ring Road London Gatwick Airport
Gatwick West Sussex RH6 0LG

t 01293 229 700
e sales@encoded.co.uk

www.encoded.co.uk

PCI Compliant
Level 1 PCI-DSS Service Provider

About Encoded

Encoded is a Level 1 PCI DSS compliant, UK company founded in 2001 to offer affordable, pay-as-you-go IVR and payment solutions to small and large businesses. Hundreds of contact centres now rely on Encoded secure automated payments for their PCI DSS compliance requirements. Today the company's software supports many of the UK's leading brands including Virgin Holidays, Mercedes-Benz FS, BMW FS, Green Star Energy and Anglian Water Business.

All of the company's services are designed to fulfil three key objectives:

- Reduce costs by automating card payments
- Increase security around payments and reduce PCI DSS compliance scope
- Improve customer service by maximising resource efficiency.

Solutions include:

- Agent Assisted Card Payments
- IVR Phone Payments
- Mobile App
- SMS Chat and Customer Engagement
- Virtual Terminal Payments
- Web Payments.

For more information please visit **www.encoded.co.uk**

The truth about PCI DSS compliance in contact centres

ENCODED
secure automated payments

A collection of blogs from Robert Crutchington, Managing Director, Encoded Ltd

Contents

Introduction 1

The five most common myths about contact centres and PCI DSS 2

Five things you should know about PCI DSS but are too afraid to ask 4

What every card-accepting contact centre should know 6

Wise up on PCI DSS and Save a Fortune 10

Why PCI de-scoping saves you money 12

Save money by de-scoping with tokenisation 14

Why your customers should know about PCI DSS 16

Five reasons why every contact centre should have a PCI DSS Compliance Programme in place 18

ENCODED
secure automated payments

Correct on compilation for v3.2 of the Payment Card Industry Data Security Standard (PCI DSS)

Introduction

Despite being over 10 years old, the Payment Card Industry Data Security Standard (PCI DSS) remains shrouded in mystery and worse, confusion.
This is a disturbing phenomenon considering payments by credit and debit card are now the norm and the real-life consequences of security leaks and data breaches can be disastrous.

With Financial Fraud Action UK reporting an estimated one in every ten people having fallen victim to financial fraud and 1.5 million incidents in the UK in 2015, the question of fraud prevention in contact centres has never been more relevant.

What is more, the pressure is on contact centres that accept card payments. Research from phone operator Syntec[1] claims "75% of consumers believe contact centre managers should do more to prevent credit and debit card fraud" yet only 10% are confident that the organisations they buy from over the phone will keep their personal or card details safe and secure. With tech savvy consumers demanding technology solutions to prevent fraud, where does this put today's contact centre and how can they help?

There are many verified ways that organisations can achieve PCI DSS compliance and our own experience proves that one size does not indeed fit all. At Encoded, we generally find that agent processing of card details is still the preferred method of payment and offers the best customer service.

In this booklet, I hope you can find answers to the many questions you might have about PCI DSS compliance and that you pick up a few coping strategies along the way.

Look out for:

- The most common myths surrounding contact centres and PCI DSS – for organisations and for consumers;
- The five essentials every card-accepting contact centre should know;
- Who is responsible? Who is liable for fines when things go wrong?
- It's a fallacy that technology can be PCI DSS compliant – why not and how can you avoid falling into the marketing trap?
- Easy tips and technical know-how that help save you a fortune;
- What is de-scoping and tokenisation?
- Don't talk about it, just do it: make sure you have a well thought-out process and proper PCI DSS programme in place to minimise fraud risk in the contact centre.

The latest item is easier said than done. Almost a third of medium sized contact centres have no compliance programme in place. This is typically due to lack of time, resource and understanding. The cost of achieving PCI DSS compliance can be prohibitive when compared with the revenue obtained.

What is clear is that you cannot do it alone. All contact centres, regardless of size, should look to work with a trusted partner in terms of secure telephone and web card payments to reduce PCI DSS scope and the subsequent cost of compliance.
Happy reading!

Robert Crutchington
Managing Director - Encoded Limited

The five most common myths about contact centres and PCI DSS

Although Visa®, MasterCard®, JCBInternational®, Discover® and American Express® created the Payment Card Industry Data Security Standard (PCI DSS) in 2007 it remains surrounded by myth and confusion. Many organisations with contact centres do not appreciate that PCI DSS covers the entire trading environment including all third-party partners and vendors that handle card data and all must comply before full PCI compliance is achieved.

Here are the five most common myths when it comes to contact centres and PCI DSS:

Myth 1

Card Payment software solutions can be PCI compliant. There is no such thing. Many solution providers make the mistake of marketing their products as PCI DSS Compliant. To advertise this claim is to miss the very thing that PCI DSS is trying to achieve, which is to maintain a unified security standard to which merchants have to adhere to. Only companies, legal entities, can be PCI compliant not software.

Myth 2

It doesn't apply to us! Yes it does. Since 1 October 2010, all contacts that accept card payments over the telephone are required to comply with PCI DSS. This includes the smallest to the largest, irrelevant of transaction volumes or values or industry sector.

Myth 3

Myth three – No-one ever gets fined. That may well be the case but the threat of a fine is always there and remember the "buck stops" with the merchant and its contact centre. The cost of data breaches cannot be measured in fines alone. Lost revenue and reputation damage can wipe millions off the value of publicly quoted companies while additional audit fees can damage even the smallest operation. Ultimately banks and card providers can withdraw a merchant's ID resulting in the inability to take card payments over the telephone or in any other way.

Myth 4

Calls including card details can still be recorded. Again not true. PCI DSS prohibits the recording or storing of any CAV2, CVC2, CVV2 or CID codes after authorisation even if the recording is encrypted. The standard states, "It is a violation of PCI DSS to store any sensitive authentication data, including card validation codes and values, after authorisation even if encrypted."

Myth 5

All card payment solution providers are created equal. Not so. Contact centres typically use multiple technologies so it is becoming increasingly important to understand just who does what in the process and who needs to be PCI compliant. The only way to be truly sure whether a third-party vendor is PCI compliant is by checking the VISA Europe Merchant Agent Weblisting.

The Visa Europe Merchant Agent Weblisting has two levels of organisation with very different validation procedures.

To achieve the top level of compliance, Level 1, an Attestation of Compliance (AOC) is needed and this level only applies to organisations that store, process and/or transmit more than 300,000 Visa transactions per year. For Level 2 registration organisations do not require an onsite security assessment by a QSA and are able to submit an annual self-assessment questionnaire including the Attestation of Compliance without reference to a QSA. Level 2 applies to smaller providers involved with less than 300,000 Visa transactions annually.

So think again when it comes to PCI DSS, it applies to every contact centre whatever the size that takes card payments over the telephone and not all third party payment suppliers are created equal. Ensure you know you are dealing with and their PCI DSS credentials.

ENCODED
secure automated payments

Five things you should know about PCI DSS but are too afraid to ask

Although the first revision of the Payment Card Industry Data Security Standard (PCI DSS) was back in December 2004 the standard remains surrounded by confusion and misinformation. For example many contact centres do not appreciate that PCI DSS covers the entire trading environment including all third-party partners and vendors that handle card data and all must comply before full PCI compliance is achieved.

Here are five lesser known but important PCI facts:

1 Responsibility

When the standard came into force all suppliers of payment services were instructed to include a full list of all 258 controls in contracts clearly showing who is responsible for each control. This can be the client, the supplier or both. In the event of lost data and a subsequent audit identifying where the breach in security occurred, the contract will form the basis of accountability. Potentially this is the first step towards holding suppliers accountable for lost data, which historically has always been with the responsibility of the merchant or client.

2 VISA will never fine a merchant

VISA cannot fine a merchant for card data loss because its contract is not with the merchant but the Acquirer (the bank or financial institution that processes debit or credit card payments on behalf of merchants). It is the acquiring bank's responsibility to make sure its merchants are compliant and as such it is the bank that will issue fines, increase charges for non-compliance and impose compulsory PCI programme costs. The revenue raised is used to fund the compliance programme. VISA will, however, fine the Acquirer if its merchants are non-compliant.

3 There is no such thing as a PCI DSS compliant product

Products are often incorrectly marketed as PCI DSS compliant. To advertise this claim is to miss the very point that PCI DSS is trying to achieve i.e. to maintain a unified security standard to which merchants must adhere. Only companies and other legal entities can be PCI compliant, not products or software.

4 Misinformation is perpetuated by procurement and marketing departments

The belief that solutions can be PCI compliant is often the result of procurement and marketing people who do not really understand the premise of PCI compliance and ask solution providers in tenders whether the solution is PCI compliant? This is an incorrect question but many suppliers are happy to go along with this misconception in order to win business. So the PCI DSS cycle of confusion continues.

5 Only select suppliers that appear on the VISA Merchant Agent Website List

Not all payment solution providers are created equal. Contact centres typically use multiple technologies so it is becoming increasing important to understand just who does what and who needs to be PCI compliant. To be certain whether a third-party vendor is compliant it is important to check the VISA Europe Merchant Agent Weblisting which has two levels of organisation with very different validation procedures.

Level 1, the top level requires an Attestation of Compliance (AOC) from a Qualified Security Assessor (QSA) and applies to organisations that store, process and/or transmit more than 300,000 VISA transactions per year. Level 2, applies to smaller providers with less than 300,000 transactions and can be achieved by completing an annual self-assessment questionnaire.

Finally, remember that PCI DSS applies to every contact centre that takes card payments over the telephone whatever its size. It is also important to know who you are dealing with and the status of their PCI DSS credentials.

ENCODED
secure automated payments

What every card-accepting contact centre should know

It is fair to say that most card-accepting contact centres understand the importance of protecting customer data from fraud and cybercrime. However, it might be news to many that in the event of a security breach they will be the ones fined. The buck stops with the merchant. Costs and expenses can quickly add up with payment network fines and assessments, forensic fees associated with a compliance audit of the merchant's business environment and legal fees. Not to mention the damage to reputation and lost sales.

A recent report* based on a survey of 2,035 online consumers stated that nearly half (45%) of respondents saw contact centres as the biggest security risk and the starting point for fraud. Findings also showed that many millions of consumers have been stopped from making purchases over the telephone when interacting with a contact centre.

But surely the Payment Card Industry Data Security Standard (PCI DSS) takes care of all of this? When Visa®, MasterCard®, JBC®, Discover® and American Express® created a standard made up of 12 requirements designed to secure business systems that store, process or transmit card holder data it was meant to protect consumers and merchants against security breaches. However, what many organisations with contact centres do not appreciate is that because PCI DSS covers the entire trading environment, all third-party partners and vendors that handle card data must also comply before full PCI compliance is achieved.

**Sabio and Avaya commissioned Davies Hickman Partners, an independent research consultancy, to complete a nationally representative survey (excluding NI) of 2,035 online consumers in January 2013.*

Visa Europe Merchant Agents List

So which third-party partners and vendors are fully PCI DSS compliant? Payment schemes are building lists of registered Third Party Vendors that can demonstrate adequate levels of data security and acceptable business practices.
For example VISA has its VISA Europe Merchant Agent Weblisting and merchant services organisations such as Elavon are insisting that only organisations which appear on this list are used by customers. This means any company involved in accepting transactions, interactive voice response (IVR) payments, internet payment gateways and any other service or product that is directly or indirectly involved in data transactions must register and appear on the list. Contact centres typically use multiple vendors for their technology so it is becoming increasingly important for management to understand just who does what in the process and who needs to be PCI compliant to avoid fines and lawsuits in the event of the unthinkable happening and customer card data being stolen.

Not all PCI third-parties are created equal

The Visa Europe Merchant Agents list has two levels of organisations that provide services to merchants. These two levels have very different validation procedures. To achieve the top level of compliance, Level 1, an Attestation of Compliance (AOC) is needed and this level only applies to organisations that store, process and/or transmit more than 300,000 Visa transactions per year.

To achieve Level 1 status an Attestation of Compliance must be completed by an independent Qualified Security Assessor (QSA) along with a Report on Compliance. QSAs cost money and have very exacting standards. The high cost of going through full PCI DSS accreditation with an external QSA is leading to some vendors claiming to be compliant when in fact they have not been through the whole process and therefore do not have Level 1 status. This is putting merchants at risk.

For Level 2 registration organisations do not require an onsite security assessment by a QSA and are able to submit an annual self-assessment questionnaire including the Attestation of Compliance without reference to a QSA. Level 2 applies to smaller providers involved with less than 300,000 Visa transactions annually.

As Matthew Tyler, CEO of Blackfoot explained, "Payment schemes such as Visa and merchant service providers like Elavon are getting tough on organisations taking card payments. Many merchants don't even realise they will be ones fined in the event of a data breach as they believe their bank or 3rd party supplier will be accountable. Some acquirers are even threatening to terminate Merchant Service Agreements if merchants fail to work with third-parties that appear on the Visa list. Organisations with call centres are seen as particularly vulnerable and should do everything in their power to work with only Level 1 vendors such as Encoded who have gone through extensive measures and inspections to achieve PCI DSS compliance."

As recent research shows card security is important to consumers and they are becoming increasingly aware of both the technology and standards around payments. For contact centres to build trust and confidence only the best technology from third-parties with Level 1 Visa clearance ▶

ENCODED
secure automated payments

is good enough for customers. It can take years to rebuild a reputation after high profile data breaches such as those at Sony, Lush and the parent company of TK Maxx but it only takes a few minutes to check whether the vendor you are working with appears on the Visa Europe Merchant Agents list, has achieved full PCI DSS compliance and Level 1 status.

Whose responsibility is it anyway?

The Payment Card Industry Data Security Standard (PCI DSS) was originally the brainchild of the world's five largest payment card providers VISA®, MasterCard®, American Express®, Discover® and JCB International®. Today, it is a global framework that provides guidance on how to process, store and transmit information about payment cards and their owners, with the aim of reducing the incidence of card fraud and promoting best practice in information security. Achieving PCI DSS compliance increases trust between an organisation and its partners and suppliers and boosts customer confidence.

PCI DSS affects everyone in the trading food chain

Nowadays, paying for goods and services remotely is the norm and every contact centre that accepts credit and debit card payments over the telephone needs to be PCI DSS compliant. However, what many contact centres don't realise is that PCI DSS covers the entire trading environment, meaning all third-party partners and vendors that handle card data on their behalf or supply services where card data is transmitted, must also comply before full PCI DSS compliance is achieved.

As organisations work hard to achieve and maintain ongoing PCI DSS compliance, they may choose to engage with third-party service providers (TPSPs) to achieve their objectives, for example, companies who store, process, or transmit cardholder data on their behalf or manage components of their cardholder data environment (CDE), such as routers, firewalls, databases, physical security, and/or servers.
Before selecting new TPSPs, organisations should conduct a proper due diligence and risk analysis to establish whether they have the right skills and experience necessary to achieve PCI DSS compliance.
Once on board, making the time to put in place a third-party assurance programme that outlines clear policies and procedures is essential to ensuring that customer card data and systems are fully protected at all times and in a compliant manner.

Contact centres beware!

Coming back to contact centres, many use multiple vendors for their technology so it is becoming increasingly important for management to understand just who does what in the end-to-end card payment process, who needs to be PCI DSS compliant and the exact status of a vendor's PCI DSS credentials. Referring to the VISA Europe Merchant Agent Weblisting is a useful first step to vetting vendors and avoiding fines and lawsuits, in the event of the unthinkable happening and customer card data being stolen.

Responsibility matrix to address the thorny issue of PCI DSS responsibility

At the end of 2014?, when the latest version of PCI DSS was announced, along came the "Responsibility Matrix", a new requirement that makes an attempt to shed light on some of the grey areas surrounding PCI DSS and begins to answer the perennial question: whose responsibility is it anyway?

PCI DSS 3.1 clarifies much of the ambiguity of the previous versions. There shouldn't be anything that affects the day-to-day running of a contact centre. However, service providers are now required to supply a "Responsibility Matrix" which defines which of the many controls are the responsibilityof the merchant and which fall to the TPSP. These responsibilities need to be clearly listed as "the merchant's responsibility," "the service provider's responsibility" or a "shared responsibility."[1]

Remember PCI compliance is not a one-off exercise. It must be revisited every year and that takes time and resource. The best way to minimise future costs as the standard evolves is to reduce exposure to the primary risk areas such as staff and infrastructure. Invest in training and education of the PCI standardin order to have the talent in-house. Unless you have a good understanding of PCI how will you know whether the advice you receive is valid or not?

The buck stops with the merchant

Most card-accepting contact centres understand the importance of protecting customer data from fraud and cybercrime. However, many might not be aware that in the event of a security breach they will be the ones fined. Costs and expenses can quickly add up with payment network fines and assessments, forensic fees associated with a compliance audit, of the merchant's business environment, and legal fees. Not to mention the damage to reputation and lost sales. Always remember: the buck stops with the merchant.

1. https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf Section 5.3.1 and Appendix B: Sample PCI DSS Responsibility Matrix Page 40.

ENCODED
secure automated payments

Wise up on PCI DSS and Save a Fortune

Every contact centre that accepts credit and debit card payments over the telephone needs to be PCI DSS (Payment Card Industry Data Security Standard) compliant. However the process of becoming and staying compliant can be hugely expensive. The interpretation of the 258 controls often leads to confusion and conflicting advice from PCI Qualified Security Assessors (QSAs).

Information about the do's and don'ts of PCI DSS and its cost and impact on every day business processes can often lead to companies putting off the process or self-certifying unaware of the risks should they then suffer card data loss. For many once PCI DSS has been achieved the expense in time and resource leaves them with very little to show or to shout about.

The answer is to wise up on what compliance really means and what the responsibilities really are. PCI DSS covers a great many areas and touches almost every aspect of an organisation's operations. Compliance in the contact centre should address risk and be achievable for a sensible and realistic cost. To truly understand the best practices for each of the 258 boxes that should be ticked takes a real specialist; however, looking at the key vulnerabilities, namely staff and the choice of third party payments supplier, will result in large reductions in both PCI DSS scope and the price of securing your customers' valuable information.

There is no such thing as a PCI DSS compliant solution

Solution providers can make the mistake of marketing their products as "PCI DSS Compliant" – there is no such thing. It is correct, however, to state that a given solution can help achieve compliance. Any third party payment service provider needs to be able to prove it is PCI DSS compliant. This is because the overall contractual obligation of compliance is always between the merchant and their merchant bank. So the third-party organisation which may include outsourced contact centres, payment service providers or collections companies will not get fined in the event of a breach that results in card data loss or fraud. The buck stops with the merchant.

Get smarter – chose the right payment solution for customer demographics

No one payment solution fits all. Different people prefer different methods of payment. A younger tech-savvy demographic may be happy with mobile payments while more mature customers may prefer to speak to an agent. Therefore think of customer demographics and select a payment solution to suit. This usually results in a requirement for multiple payment methods being implemented but has the overall benefit of reducing frustration felt by customers that would have otherwise been forced to use a payment service they're not comfortable with.

Continuous authority payments (also known as recurring payments) can help to reduce the scope and cost of PCI DSS compliance audits.

Once an initial transaction is verified the card used becomes trusted and any repeat uses will not require details to be taken again. On average 40% of customers will opt to have their card details stored for future use. However, there may not always be funds available on the stored card and therefore payments can be declined. Some suppliers, such as Encoded, have a tokenisation feature to enable card holders to validate and amend stored cards when something goes wrong; avoiding fines, fees and interest charges by self-managing the details held on file.

Tokenisation, recurring and stored card payment solutions mean that organisations with contact centres can vastly reduce the scope of their PCI DSS audits.

Tokens can only be used through specific payment gateways and if they are stolen or written down then the token is completely useless to anyone outside the payment environment. So take the time to wise up on PCI DSS and save money.

ENCODED
secure automated payments

Why PCI de-scoping saves you money

Every business or merchant that accepts payment via debit and credit cards has a contractual obligation with its acquiring bank (or acquirer) to be PCI DSS compliant. The Payment Card Industry Data Security Standard (PCI DSS) was created by Visa®, MasterCard®, JCB International®, Discover® and American Express® and is made up of 12 requirements designed to standardise controls surrounding card holder data and to help protect consumers and merchants against security breaches.

To become PCI compliant the 12 requirements, consisting of 258 controls, must be implemented and the cost of this to a business can range from the tens of thousands to the tens of millions of pounds. To many, the costs involved can be prohibitive but there is money to be saved by undertaking a programme of reducing the scope of the cardholder data environment (or de-scoping).

What is de-scoping?

To be PCI compliant organisations have to demonstrate that they have reached a level of security awareness and competence to a point where the risk of losing debit and credit card data is regarded as less than that of a non-PCI compliant organisation. De-scoping is the process to reduce the number of requirements (tick-boxes) for PCI compliance. This can be achieved by passing the responsibility of handling card data to a third party. As the merchant account agreement is between the merchant and the acquirer, the responsibility for PCI compliance cannot be entirely removed, however the amount of time and work required demonstrating compliance can be dramatically reduced.

How to de-scope

To begin the process of de-scoping it is essential to identify where in an organisation card data is handled. This is usually in the contact centre or wherever card holder data is being processed. There are many options available to organisations that regularly take card payments over the telephone. For example working with an interactive payment solutions company such as Encoded allows organisations to offer either IVR (Interactive Voice Response) or virtual terminal payment options. Automated IVR payments reduce contact centre agent involvement and can be available 24x7x365 days of the year. Virtual Terminal payments allow agents to take payment over the telephone by logging into a secure online virtual terminal interface to in-put card details directly or conferencing in the customer who uses their touchtone telephone to securely enter their card details themselves. Tokenisation is another way of keeping card data safe and out of scope of the PCI process. Tokenisation is the process of replacing card data with random numbers that, when used within a specific payment gateway, reference back to the actual card data without compromising its security. Tokens can be used repeatedly by merchants where payments are regularly made.

Why de-scoping saves money

Taking areas of an organisation's business out of the scope of PCI compliance minimises the cost and complexity associated with PCI DSS standards. As mentioned before a PCI project can cost anything from £10k to several millions of pounds plus there is a requirement for quarterly network scans and an annual audit. External Qualified Security Assessor (QSA) fees are typically £1000 per day which can rule out smaller merchants and can soon add up for larger organisations. By working with a fully Level 1 PCI compliant interactive payment solutions supplier to de-scope, by removing customer card data from the process, means there is less for the QSA to audit. Therefore, by de-scoping PCI compliance can be achieved in less time and with a much reduced price tag.

Remember the buck stops with the merchant to ensure PCI compliance. However, whether customer card data is handled within a contact centre, via web pages or a chip and pin terminal, PCI compliant payment companies such as Encoded, offer solutions to ensure compliance is achieved with minimum cost and maximum security.

ENCODED
secure automated payments

Save money by de-scoping with tokenisation

Tokenisation is a process of replacing sensitive card data with a sequence of numbers that, when used within a specific payment gateway, reference back to the card data without compromising its security. This is particularly useful for organisations that take repeat or subscription payments for example membership fees. This functionality is similar to having a direct debit in place, but instead utilises all the flexibility and benefits of a card payment scheme. Once the initial transaction is verified the card becomes trusted and any subsequent payments will not require details to be taken again until the original card expires.

Another benefit of tokenisation is that if the payment fails for any reason neither the merchant nor the card holder are penalised, unlike with direct debits. Offering customers a new method of making regular payments adds value as well as raises an organisation's customer service profile. There is also a reduced risk of declined payments with tokenised cards, because a successful payment must be made prior to tokenisation.

Using tokenisation the whole payment process is faster, easier and more secure for regular customers while saving on time and resource for merchant organisations.

But how does this help with PCI compliance and save money?

To be PCI DSS* compliant organisations cannot retain customers' card details; however, by working with a PCI compliant payments provider with a tokenisation solution, merchant organisations can reduce the scope of the cardholder data environment (or de-scope).

De-scoping is the process to reduce the number of requirements for PCI compliance. To become PCI compliant there are 12 requirements, consisting of 258 controls, designed to standardise controls surrounding card holder data and to protect consumers and merchants (organisations) against security breaches. The payments provider handles the tokens taking responsibility for cardholder data security. Therefore it is important to work with a Level 1 PCI DSS compliant payment service provider.

By implementing tokenisation (also known as recurring or stored card payments) organisations can vastly reduce the scope of PCI compliance and increase data security. Tokens can only be used by the PCI compliant service provider's payment gateway and if they are stolen or written down the token is completely useless to anyone outside of the payment environment.

The process of tokenisation means that payment card numbers are not stored in databases making it difficult for hackers and reducing the chances of cyber theft. Furthermore if multiple payment methods such as agent assisted card payments, website and automated interactive voice response (IVR) solutions are configured to offer tokens, from a shared token pool, then the collection of card information in the contact centre can be removed completely allowing for only tokenised transactions to be taken by live agents.

Therefore, tokenisation increases security of card holder details while minimising the cost and complexity of PCI compliance. However, not all payment solutions can handle tokens and to get the full benefit of the process it is important that tokens are compatible across all payment methods including IVR, virtual terminal, agent assisted and web payments.

While an organisation's responsibility for PCI compliance cannot be entirely removed, as the merchant account agreement is between the merchant organisation and its bank or acquirer, tokenisation is a great way to de-scope for compliance purposes while improving the security of cardholder data and customer experience.

ENCODED
secure automated payments

Why your customers should know about PCI DSS

If you were to ask shoppers in the street to name an online payment protection process the chances are they would know about Verified by Visa, 3D Secure, Mastercard SecureCode or even Safekey from American Express but most would draw a blank at the mention of PCI DSS. Why is this and why doesn't it come as a surprise?

The Payment Card Industry Data Security Standard (PCI DSS) was created by Visa®, MasterCard®, JCB International®, Discover® and American Express® and is made up of 12 requirements designed to secure business systems that store, process or transmit card holder data and is meant to protect consumers and merchants against security breaches. However, beyond the payment industry including merchants, suppliers, acquirers, VISA and Mastercard what does it really mean to people and why aren't consumers aware of its importance?

Customers need confidence

For customers to transact with an organisation either via a contact centre or online they need to be confident that their payment cards will not be compromised, their personal details are secure and their identities cannot be stolen. By complying with PCI DSS, merchants and service providers meet their obligations to the payment system and build a culture of security that benefits everyone. However, not enough is being done to advertise this fact.

Who pays the fine?

In the event of a loss of data or cards being used fraudulently, fines are passed down the chain from VISA and MasterCard at the top to the merchant/retailer at the bottom. The consumer doesn't suffer financially as measures are in place and assurances given to prevent this happening. The fact remains that something has gone wrong and individuals will be inconvenienced and could suffer from emotional stress at the thought of their details being stolen and used fraudulently. In time this could lead to a reduction in customer confidence in both the method of payment and a reduction in confidence of the retailer who caused the problem. Surely, all those involved in the card payment industry including merchant acquirers have a duty of care to improve public awareness. This in turn would benefit consumers as card processing, security and compliance, fraud, fines and penalties are all part of the 'retail cost structure' which can lead to increased prices.

Some merchant acquirer companies have started to levy a surcharge on suppliers and merchant organisations that are not PCI compliant to encourage them to go through the full process of compliance. This can be an expensive exercise because to achieve the top level of compliance, Level 1, an Attestation of Compliance (AOC) is needed which must be completed by an independent Qualified Security Assessor (QSA) along with a Report on Compliance. QSAs cost money and have very exacting standards. But do the benefits outweigh the costs and time involved?

Matthew Tyler, CEO and QSA at Blackfoot believes so, "Only greater public awareness will prove the real value of PCI DSS and lead to reduced fines and improved security. People will ultimately choose to transact with those organisations they have confidence in and they know are PCI compliant."

Greater public awareness

To achieve this greater awareness some of the money paid in fines and surcharges should be used to promote the advantages of dealing with PCI compliant operations. Once card holders have a greater knowledge and know what questions to ask of their merchants and the payment system as a whole, the benefits will become apparent.

If the public had a clearer understanding of the importance of PCI DSS people would only purchase from those organisations who demonstrate full PCI compliance, therefore reducing the instances of lost data and fraudulent activities. The welcome result of this would be fewer fines, lower prices and less sleepless nights worrying about security.

To my mind it is simple – use the money raised in fines and levies to promote the relevance of PCI DSS so that customers look out for the PCI Sign when making a purchase and paying by card.

This will benefit everyone, improve security and raise the profile of PCI DSS to level it deserves.

ENCODED
secure automated payments

Five reasons why every contact centre should have a PCI DSS Compliance Programme in place

With Christmas fast approaching, contact centres are preparing for an escalation in calls and transactions that the festive season brings. However with payment card fraud continuing to rise and data theft constantly in the news, just look at the recent cyber attack on the Talk Talk consumer website, non-PCI DSS compliant contact centres could be risking more than just a fine.

1 News travels fast

Survey findings from the Contact Babel, The UK Contact Centre Decision-Maker's Guide 2015, worryingly revealed that almost a third of medium sized organisations have no compliance programme in place. With several versions of the standard now available via SAQ (Self Assessment Questionnaire) there is little argument as to why a programme shouldn't be at least road mapped.
In the age of social media, where good news travels fast and bad news even faster can a brand afford for clients' card data to be lost with the resulting PR backlash? Referring to the downloadable VISA Europe Merchant Agent Weblisting before engaging with a trusted advisor is a useful first step to vetting vendors and avoiding fines and lawsuits, in the event of the unthinkable happening and customer card data being stolen.

2 The buck stops with the merchant

Delivering a good customer experience is about more than swift call response times. Paying for goods and services remotely is the norm for consumers and they expect their personal card account information to be kept safe. Every contact centre that accepts credit and debit card payments over the telephone is responsible for safeguarding their customer's information and can be held liable for security compromises.

The Payment Card Industry Data Security Standard (PCI DSS) is intended to protect cardholder data wherever it resides and failure to comply with PCI DSS can result in hefty fines, not to mention the damage to reputation and lost sales. By complying with PCI DSS, merchants and service providers meet their obligations to the payment eco-system and build a culture of security that benefits everyone.

3 PCI DSS Compliance is not a one off exercise

PCI DSS is a change in mind-set, a change in attitude towards the handling of card data. It's not like other industry accreditations where organisations can prepare the night before an audit and scrape a pass. It is the implementation of security procedures that will underpin the company's behaviour when dealing with payments as well as how networks are designed, plus how access is granted and logged.

PCI DSS compliance must be revisited every year and that takes time and resource, it is effectively a full time job. Employing a compliance officer, who has the complete support of the contact centre management and the authority to update the status quo, ensures the required changes are driven through.

4 Awareness is increasing

The Payment Card Industry Data Security Standard (PCI DSS) was originally the brainchild of the world's five largest payment card providers VISA®, MasterCard®, American Express®, Discover® and JCB International®. Today, it is a global framework that provides guidance on how to process, store and transmit information about payment cards and their owners, with the aim of reducing the incidence of card fraud and promoting best practice in information security.

In the event of a loss of data or cards being used fraudulently, fines are passed down the chain from VISA and MasterCard at the top to the merchant/retailer at the bottom. The consumer doesn't suffer financially as measures are in place and assurances given to prevent this happening.

However, if something goes wrong, consumer brand loyalty can quickly fade. Customers transact with an organisation because they feel confident that their payment cards will not be compromised, their personal details are secure and their identities cannot be stolen.

In the event of a security breach individuals will be inconvenienced and could suffer emotional distress at the thought of their details being stolen and used fraudulently. This could lead to a reduction in customer confidence in both the method of payment and the retailer who caused the problem. ▶

ENCODED
secure automated payments

Reactive contact centres could find themselves quickly playing catch up as their customers vote with their feet.

5 Becoming and remaining PCI DSS compliant

Every contact centre that accepts credit and debit card payments over the telephone needs to be PCI DSS compliant. However, what many contact centres don't realise is that PCI DSS covers the entire trading environment, meaning all third-party partners and vendors that handle card data on their behalf or supply services where card data is transmitted, must also comply before full PCI DSS compliance is achieved.

The latest version of PCI DSS introduced a new requirement compelling service providers to supply a "Responsibility Matrix" which defines who is responsible for each of the 258+ PCI controls; namely the client, the supplier or both. It is worth stating at this point that PCI is not intended to trip up organisations or waste time; it is intended to secure cardholder data. Achieving PCI DSS compliance increases trust between an organisation and its partners and suppliers and boosts customer confidence.

The best way to minimise future costs as the standard evolves is to take good advice in the first place. Minimise exposure to the primary risk areas such as staff and infrastructure. Invest in training and education on the PCI DSS standard in order to have the talent in house and work with payment organisations that are themselves Level 1 PCI DSS compliant. Remember there is no such thing as a compliant software solution.

The moral of the story is - put a checklist in place, work with the right payment solution provider, get a compliance programme underway and have a safe, secure and profitable future.

ENCODED
secure automated payments