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 contact centre and multi-channel payments

ENCODED

secure automated payments

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

Contents

ENCODED
secure automated payments

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

Introduction

As the saying goes, the only constant is change and this has never been more so than in the payments industry today. PCI DSS Compliance, General Data Protection Regulation (GDPR), the abolition of credit and debit card surcharges and new technologies all conspire to produce a challenging environment for payment taking contact centres.

GDPR is now with us which means companies will be required to review existing data policies and practices to comply with how data is kept. As well as GDPR, new legislation under the Payment Services Directive (PSD2) now makes it illegal for merchants and retailers to charge customers more for using a credit or debit card in the EU. While it is not clear who will really benefit from this change, the good news is that for merchants and contact centres already working with a secure payment service provider (PSP), making the changes to their card payment processing system can be easily accommodated.

Payment technology continues to be a discussion point. The 15th edition of ContactBabel Contact Centre Decision-Makers' Guide (DMG) revealed that for almost three-quarters of the survey respondents, software and/or payment technology is still the single largest cost associated with PCI DSS compliance, causing many organisations to rethink how they take card payments and the technologies they use.

Partnering with a technology provider which has invested in Level 1 PCI DSS compliance and has tokenisation technology can help to simplify the payment process, as well as protect customers against major security threats such as fraud and cybercrime.

New challenges also emerge as we see the new fourth card type, the Deferred Debit Card, becoming more prevalent in the UK. While consumer awareness is in its infancy, it falls on the merchants and PSPs to manage and provide clear feedback to customers.

In this collection of blogs I have attempted to dispel some myths and provide ways to approach these compliance, payment process and technology issues. The last blog picks up on the cloud debate. The 2017 edition of Call Centre Helper's Research Paper, What Contact Centres are Doing Right Now states that cloud uptake is set to rise rapidly, with over a quarter of respondents planning to implement cloud technology.

While not all organisations are ready to make the switch to cloud just yet, working with a cloud-based payment solution provider can help to increase security and de-scope data for PCI DSS compliance purposes – both priorities today.

Enjoy the read and feel free to get in touch if you would like to discuss any of these topics further.

Robert Crutchington
Managing Director - Encoded Limited

GDPR Compliance – Take a lead from PCI DSS in your contact centre

With the General Data Protection Regulation (GDPR) taking effect on 25th May 2018, many organisations need to consider what it means to them. Overriding national data protection laws and including new and more detailed protection legislation for personal data, GDPR necessitates a review of data policies and practices that companies have in place to ensure that they comply with how data is kept throughout the organisation.

GDPR is more than just payment card data

Many see the introduction of the new legislation as a positive step. It encompasses how data is managed, processed and deleted by concentrating on ensuring that it is lawfully and fairly protected by documented and verifiable security measures. It includes all of a company's data dealing with EU citizens, such as that held in marketing, sales and finance, not just CRM systems in contact centres.
It also contains a raft of new rights for individuals i.e. data subject rights, these include the right to data portability, the right to be forgotten and a strengthening of access to their data or data access requests.

In essence this regulation aims to achieve two things:

- A single set of rules applying to all EU member states, creating a single digital marketplace
- Moving the rights of data to the data subject or individual

Organisations that fail to comply with the legislation face punitive fines of up to 4% of their annual global turnover or €20m, whichever is greater, not to mention reputational damage. So what does this mean for contact centres?
The good news - PCI DSS principles apply Contact centres have always been focused on security of card payments, ensuring that customer card data is stored, transmitted or processed securely. Now the process needs to apply to all personal customer data – or Personally Identifiable Information (PII).

The good news is that if your contact centre is already Data Protection Act (DPA) compliant then typically you will be a long way to being GDPA compliant. In addition, the Payment Card Industry Data Security Standard (PCI DSS) is intended to protect cardholder data, which means that by complying with PCI DSS, you can be sure you meet legislation, security requirements and the burden of proof of compliance (which falls on the call centre), by demonstrating adherence to a recognised security standard. Plus, if you are already working with a PC1 DSS Level 1 supplier, which is also DPA compliant, this further ensures you meet the regulations for your payment data.

De-scoping makes it easier to manage
To be PCI DSS 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 DSS compliant organisation.

Therefore, PCI DSS principles are a good place to start when thinking about personal data. Companies can apply a process of 'de-scoping' to reduce the number of requirements (tick-boxes) for PCI compliance. This same method can be applied to personal information, where business processes can be 'de-scoped' from sensitive personal data, by the use of data anonymization, similar to the tokenisation solutions widely used to take repeat card payments without having access to sensitive card details.

Businesses attempt to reduce their PCI DSS scope by limiting the number of places where card data is present in a variety of ways including; removing redundant and obsolete storage facilities and applications, using technology solutions like tokenisation (unique identifiers that retain all the essential information about the data securely) and outsourcing elements of card handling, storage and processing to PCI DSS compliant third parties. As well as taking a risk based approach to justify proportionate controls and eliminate disproportionate costs.

Choose your partners carefully

If you do choose to work with partners it is a requirement of PCI DSS, to draw up a responsibility matrix, outlining compliance and competencies.
This can help to set out what needs to be done and who is responsible to ensure data is secure. It's also important to draw up a data breach plan, to identify what needs to happen in the event of a data breach – what actions need to be taken, regulatory disclosure, communications to stakeholders and customers, as well as forensic investigation.

Improve processes and agent training
Compliance with any legislation, whether PCI DSS or data protection, is not simply about implementing a piece of technology, it involves people and business processes as well as systems. ▶

ENCODED
secure automated payments

One of the biggest risks in any organisation relating to data is staff - not necessarily from fraudsters, but laxity of people in taking proper care of data. The relatively low cost of training and education of the risks involved can go a long way in making staff vigilant to perils such as phishing emails and fraudulent representation. Phishing emails can mean that innocently staff allow hackers to enter the system, and is a bigger risk than a rogue staff member writing the odd card number down.

A Trusted Partner takes away the headache

Taking areas of an organisation's business out of the scope of PCI DSS compliance minimises the cost and complexity associated with many of the standards. Working with a Trusted Provider (one that is PCI-DSS Level 1) for your payment data ensures that you are compliant in the contact centre for payments data and is a good place to start on data protection. The Information Commissioner's Office (ICO) has also published guidance[1] for companies preparing for GDPR to help plan an approach and identify what needs to be done.

Like PCI DSS compliance, the responsibility for GDPR cannot be entirely removed from the contact centre, however, the effort required can be dramatically reduced by following a similar approach to that of de-scoping.

Remember that the buck stops with the merchant to ensure PCI DSS compliance and the same is true for GDPR. Responsibility cannot simply be handed over to a third party – an organisation must also identify itself how data is to be managed.

However, taking a lead from PCI DSS and working with the right people can go a long way to sleep filled nights and compliant days.

This article was co-authored by Rob Crutchington, managing director of PCI DSS Level 1 payment service provider Encoded and Matthew Tyler, director of information security specialists, Blackfoot.

About Blackfoot

Blackfoot specialises in cyber security, data protection and compliance, helping clients make informed pragmatic decisions in an increasingly complex and regulated world. Blackfoot's risk based approach ensures focus is applied to what's most important to their clients.

For more information please visit: www.blackfootuk.com

[1] https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Agent Assisted Payments

Agent assisted payments and stored card payments improve customer service and reduce the cost of PCI DSS compliance. Other secure automated payments from Encoded include IVR, Virtual Terminal Payments and Automated Recurring Payments.

Keep it Simple – Keep it Secure

Talk to Encoded to discover a more engaging and cost effective route to payments

www.encoded.co.uk

01293 229 700

ENCODED

secure automated payments

PCI DSS: 3 Surprises from latest contact centre report

Taking a closer look at contact centre payments

The UK Contact Centre Decision-Makers' Guide (DMG) revealed several surprises in terms of PCI compliance and card fraud reduction in its 15th edition. This major report studying the performance, operations, technology and HR aspects of UK contact centre operations is produced annually by analyst ContactBabel. Taking a random sample of the industry, 218 contact centre managers and directors answered a detailed structured questionnaire during the summer of 2017.

In the PCI DSS* Compliance and card fraud reduction section of the report there were 3 main surprises highlighted by the research:

- Pause and resume or "stop-start" recording which aims to prevent sensitive authentication data and other confidential information from entering the call recording environment remains consistently the most popular method of compliance with 60% of respondents using this method
- The number of respondents using DTMF tone suppression, the often promoted alternative to pause and resume, fell from 22% last year to 14% this year
- The cost of compliance is causing organisations to rethink how payments are taken in contact centres, with 7% of respondents no longer accepting payments in this way.

What do these surprises mean?

Increasingly at Encoded we are seeing that the requirements and costs associated with payment technology, processes and training outweigh the benefits of taking payments by phone in contact centres. However, there are ways to reduce these costs and the complication often associated with PCI DSS compliance.

For almost three-quarters of survey respondents software and/or payment technology is the single largest cost associated with compliance (particularly in small and medium-sized operations). While in the largest contact centres, training staff in card fraud prevention techniques and processes is the greatest cost in 36% of cases.

Ringing the changes for how card payments are taken

It would appear the cost of compliance is therefore causing many organisations to rethink how they take card payments. We find an agent processing card details is still the preferred method and offers the best customer service, but there is confusion around the need for tone suppression (whereby DTMF tones are captured and altered making them unidentifiable), and this in particular is pushing up the cost of technology to support card payments.

However, one of the other surprises of the report was that the use of DTMF tone suppression was down this year from 22% to 14%. While price and reliability may be contributing factors to this decline, there is the added problem of discrimination and a potential legal and social media backlash. By restricting the contact centre to only accept card data via DTMF tones could mean that some people are effectively being discriminated against by not being able to make a payment or have increased difficulty to do so, particularly if they are either elderly or disabled in anyway.

Therefore, it was good to see "pause and resume" still performing well. Despite some commentators claiming pause and resume is dead, ContactBabel's Report shows that it remains consistently the most popular method of compliance and used by over 60% of respondents. It is typically far cheaper to implement than almost any other option and offers the highest level of customer service.

Other less expensive options for compliance

It was also good to see other less expensive options for maintaining PCI DSS compliance mentioned in the report for example:

- Improving agent processes and training – according to the report, this is the second-most widely used method by contact centres. The relatively low cost of training and education of the risks can go a long way in making staff vigilant to safeguarding data. Regular training including the perils of phishing emails, often a far bigger risk than a rogue staff member writing the odd card number down, can prove vital to securing data.
- IVR Payments – although used by only a few, especially large contact centres, automated IVR process to take card details from the customer cuts the agent risk out of the loop entirely. ▶

ENCODED
secure automated payments

- Third-Party Cloud-Based Payment Solution - no cardholder data is passed into the contact centre environment, whether infrastructure, agents or storage. As such, this can de-scope the entire contact centre from PCI compliance, but does rely on the security processes and operational effectiveness of the service provider.

Before implementing any new technologies or processes relating to achieving compliance, it's important to consider the level of risk, the time and effort required to complete self-assessment questionnaires (SAQs), the cost of technology and the effect on customer experience.

Whatever solution a contact centre decides to employ, the fact remains that if compliance is being achieved at the expense of customer service, then maybe it's time to think again.

Copies of the full report The UK Contact Centre Decision-Maker's Guide 2017-18, The PCI Compliance chapter can be downloaded from the Encoded website, www.encoded.co.uk

**Payment Card Industry Data Security Standard (PCI DSS) – the creation of five of the largest card providers: VISA, MasterCard, American Express, Discover and JCB International.*

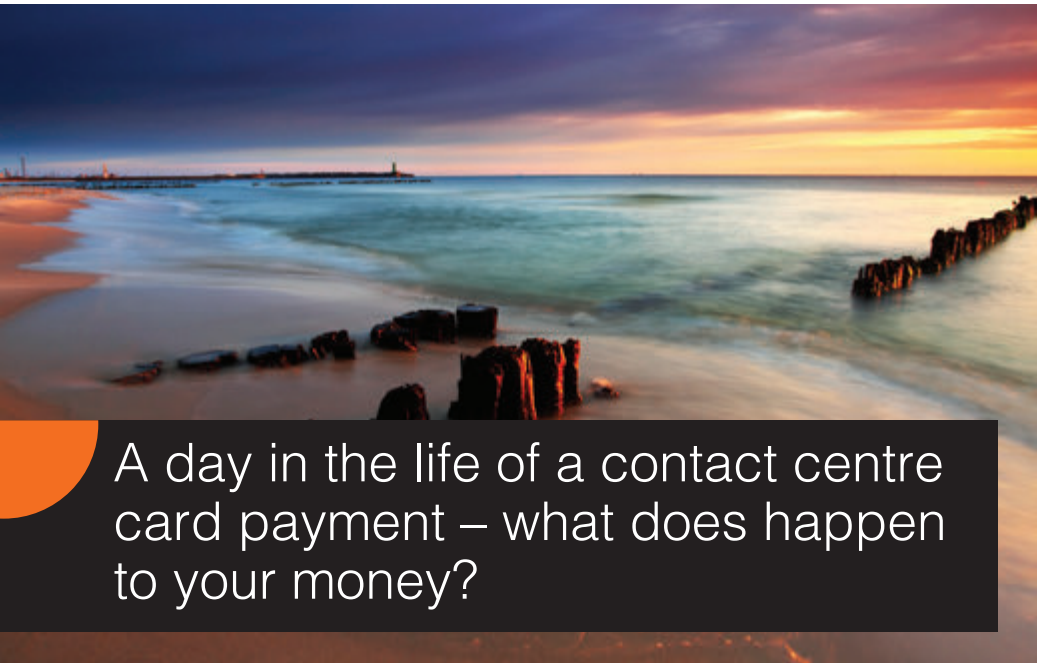
SMS Customer Engagement

SMS is widely accepted as a non-intrusive, convenient method of communication. Encoded offers a feature rich, highly secure customer engagement messaging solution. As well as SMS and Voice, Encoded's solution also integrates with many other messaging services such as Facebook messenger.

Keep it Simple – Keep it Secure

Talk to Encoded to discover a more engaging and cost effective route to payments
www.encoded.co.uk
01293 229 700

ENCODED
secure automated payments



A day in the life of a contact centre card payment – what does happen to your money?

Have you ever thought about what happens once you enter your debit or credit card details into an automated system or read them out to a contact centre agent? The answer isn't easy but it is more straightforward than many would like you to believe, so stay with me as I take you through a day in the life of a payment.

Payment Method

There are a variety of payment methods available. These may include online purchases, Chip and PIN terminals, contactless or over the phone payments with an agent but whichever method used the underlining process of authorising the card issuer to allocate your money against that transaction in order to pay for the product or service is roughly the same. After all, you're not actually handing over cash, and the merchant (the company or person you're paying) isn't actually getting paid; they're really just requesting an authorisation code which assures them, but crucially does not guarantee, that their merchant account will be credited with the agreed amount.

Payment Service Provider

Once card details are taken they begin their journey towards a payment gateway which is hosted by a Payment Service Provider (PSP) Encoded is a good example of a PSP, where merchants can utilise multiple payment methods from a single supplier, regardless of which company provides their merchant account. The card details are checked for errors. If these all pass, then the payment is forwarded on to the payment gateway, such as those provided by Mastercard, Barclaycard, First Data or Cardstream. These payment gateways have relationships with acquirers, which is another name for a Merchant Bank such as Streamline, Cardnet or Barclays Merchant Services (BMS). At this point the acquirer identifies the Merchant Account by way of the Merchant Identification Number (MID) which is the merchant's account number.

Authorisation

The next important step sees the acquirer recognising your card's long 16 digit permanent account number (PAN) as one that it deals with i.e. from a card issuer that it recognises. At this point your card's 16 digit PAN number, the merchant's identification (MID) number and the transaction amount are sent via the card scheme to the card issuing company. The card scheme for example could be VISA, Mastercard, AMEX or a host of others that card issuers are able to work with. Once the card issuer, Barclaycard for example, has checked that there is enough credit or balance available to fulfil the purchase an authorisation code is generated which reserves the money against the transaction and is passed back up the chain to the payment service provider (PSP) to notify the merchant or service of the transaction outcome. Ideally the transaction has been authorised but if it's been unsuccessful then the merchant is also informed and the transaction declined. However, even with an accepted payment no actual money has been moved yet. The payment is still held by the acquirer and hasn't gone any further.

Final Settlement and Payment

The final step is settlement for the agreed transaction; this is carried out at midnight, every night. This is when all the acquirers settle authorised payments between themselves in one large transaction to avoid multiple payment fees with the banks. At the same time reconciliation information is issued. It is the duty of each merchant to negotiate a payment term with their acquirer. This is typically measured in days (not hours) and it is finally the actual movement of money from the acquirer to the merchant for the goods sold. Charities for example might be paid within one day whereas gambling operations and furniture merchants could have to wait 5 and 30 days respectively before they get their hands on your cash. Furniture is often delivered damaged and is subject to refunds and therefore the settlement term could be longer. On the whole payment periods are determined by the merchant's industry sector or standard industrial classification (SIC) code. Some merchants may even delay delivery of goods until settlement has been confirmed.

Failed Settlement

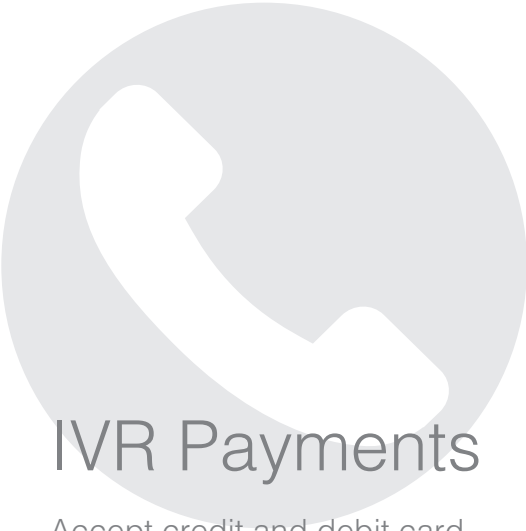
It is possible for an authorised transaction to fail settlement. In the event of a failed settlement, for example where a customer has reported their card lost or stolen within the same day as having made a purchase either in store, by phone or online, an authorisation code will have been generated but the payments made that day on that card will be stopped at settlement. ▶

ENCODED
secure automated payments

This is to prevent fraudulent transactions from being processed after the card was reported lost or stolen. Encoded encourages its customers to do reconciliation against a settlement report and not to rely on the transaction log they receive – just in case a transaction failed to settle. It's better to be safe than sorry.

As you can see it really is at least "a day in the life of a payment" if not longer. What may appear to be a simple case of an amount being taken from your card and a debit appearing on your statement the following month really involves far more than is at first evident.

Add to this the complications of Payment Card Industry Data Security Standard (PCI DSS) compliance and you soon realise why card accepting contact centres are wise to work with a Level 1 PCI DSS secure, automated payment service provider (PSP) to remain compliant and maintain maximum security.



IVR Payments

Accept credit and debit card payments by an IVR phone service to improve customer service, reduce operational costs and cut PCI DSS compliance costs.
IVR payments save on agent time and increase security with proven return on investment (ROI).

Keep it Simple – Keep it Secure

Talk to Encoded to discover a more engaging and cost effective route to payments
www.encoded.co.uk
01293 229 700

ENCODED
secure automated payments

Scrapping Card Fees – A Bureaucratic waste of time or a benefit to consumers?

According to the Treasury, in 2010 the total value of surcharges for debit and credit cards was an estimated £473 million[1] but the news is that this is set to change.
From 13th January 2018 new legislation under the Payment Services Directive (PSD2)[2] made it illegal for merchants and retailers to charge customers more for using a credit or debit card in the EU.

The original purpose of splitting out card's fee was to make the cost of using a card transparent to the card holder. Often credit cards incur a greater fee than debit cards. For example, with theatre and concert booking sites, airlines and take-away food apps typically adding an extra charge to any purchases made using a card.
As do some local councils and government agencies.

Why the surcharge?

Businesses argue that they face extra charges when someone pays by credit or debit card and so the rationale was that they could pass on the costs for processing card payments.

Typically banks charge companies higher rates to process a credit card, therefore businesses have been allowed to add a surcharge accordingly. In fact, many smaller shops and businesses often have a minimum spend of £5 or £10 for payment by card, this can now be overcome by switching to contactless payments.

What does this change mean for merchants?

Adding surcharges will be illegal under the new directive, however, as consumers switch away from using cash many merchants and retailers will not want to risk losing their business and will need to reconsider their practices.

It's a difficult decision. Under the Consumer Rights Act[3], businesses can only pass on charges that genuinely reflect their costs and it will be up to Trading Standards officers at local authorities to act if they receive complaints about those merchants who continue to impose card surcharges after the act came into force.

However, Trading Standards has limited resources and it may be that many small retailers used to imposing card surcharges under the current rules may continue to do so after the new deadline. It's also likely that since smaller retailers are often local, customers are happy to pay a premium price for convenience. For bigger, national retailers, online merchants and card accepting contact centres it's a different challenge. They will probably need to be more upfront to consumers about their pricing policy and practices if they are to avoid criticism.

How does this new ruling benefit the customer?

It's difficult to see whether this is a benefit to consumers or not. In the past the surcharges were transparent and enabled customers to see what they were being charged (and opt out of using their card if they choose).

With this new legislation prices may go up as merchants attempt to recoup some of their costs. In this case, consumers will have no way of knowing how much they are being charged for using their card. Since the fees are a legitimate cost, then the likelihood is that consumers will continue to be charged. Businesses cannot afford to swallow merchant charges and so they will still pass them on, plus maybe a bit extra, because 'now they can'.

It's not all bad news for merchants

The good news is that for merchants and contact centres which are already working with a secure payment service provider making the changes to their card payment processing system can be easily accommodated. It's a simple configuration that can be managed easily and one that at Encoded we will administer at no cost.

As to whether anyone will really benefit from the new legislation – the jury's still out.

[1] https://www.gov.uk/government/news/rip-off-card-charges-to-be-outlawed
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L2366&from=EN
[3] http://www.legislation.gov.uk/uksi/2012/3110/regulation/4/made

ENCODED
secure automated payments

It's time to simplify the card payment process! Take the first step by ditching the three-digit CVV code

Paying for goods and services with a debit or credit card is now so commonplace that those wielding a fist full of bank notes are often regarded with suspicion. Card payments make life easy but the process behind making them happen is a lot more complex than you might think, with verification taking place every step of the way. We're all familiar with giving our card details by telephone or entering them online but what happens next? There are 14 steps in card authorisation and settlement*, involving merchants, payment service providers, payment gateways, the merchant's bank, card schemes and finally the customer's own bank and this whole process can take a minimum one day and often far longer.

Authorisation is essential but how much information is really necessary?

For those paying online or over the telephone there is often one more step required in the authorisation process. They are asked for the card verification value (CVV) code or three-digit number on the back of their MasterCard or Visa card (four-digits if paying by Amex).

The rationale behind the CVV code is that it is further validation that the customer physically has the card in their presence. But is this true and is it absolutely necessary?

Time to dispel the myths around CVV codes
There are several rumours in the industry which relate to why merchants seem to think the CVV code is necessary.

One thing is for sure it cannot be retained once a transaction has been processed. Keeping it would contravene the very foundation of the Payment Card Industry Data Security Standard (PCI DSS) which prohibits the storage, hand-written or in computer files, of a customer's confidential card data. The two most common myths around CVV codes are:

Myth 1 Merchants benefit from reduced interchange fees by using CVV codes in transactions

Many merchants believe that by insisting on CVV codes, they can benefit from a reduced interchange fee based on the transaction being deemed "secure". The interchange fee is the amount charged by Card Schemes such as VISA to the acquirer for using their services. However, as of the 1st of March 2015 VISA capped the rate at 0.2% for debit card transactions and 0.3% for credit card transactions across the EU irrespective of whether the transaction included the CVV or not. All mail order telephone order (MOTO) transactions are deemed as non-secure.

Therefore, it is not true that there is any financial benefit from requesting the CVV and given the huge importance PCI DSS places on the CVV, Encoded's advice is to simply not request it in the first place. What is true is that by including the CVV code should a dispute or chargeback occur, when a merchant submits a transaction for authorisation, the processor and/or card brands will reduce their fees on the dispute or chargeback. However this small business cost is dwarfed by the PCI DSS costs of protecting it, if accepted.

Myth 2 Merchants conducting repeat transactions need to submit the CVV for the original and all subsequent transactions

Again, this is a myth. There are two ways to conduct such recurring transactions. The easiest way is to use a payment service provider that supplies a reference number from the original transaction and then processes all subsequent transactions using the same number or token. The other option is for an organisation to store the cardholder's name, account number and expiration date, providing, of course, these details are stored securely either by encrypting them if on a computer, or if using a manual system they are physically secure.

Is it time to ditch CVV codes?

Interestingly, in a country that is often at the forefront of data protection and security, the United State of America does not use CVV codes and we should follow suit. Until recently VISA Europe and VISA Inc. were two separate organisations. However, in November 2015 VISA Inc. bought VISA Europe for $23.4bn. As such we can all expect changes in the European payments market to follow the US way of handling card details. In actual fact all that is really required is the 16-digit card number and this can be stored provided it is encrypted and "deemed" unreadable as per sections 3.3 and 3.4 of v3.1 the PCI DSS requirements. ▶

ENCODED
secure automated payments

This latest development is good news because, from a PCI DSS compliance perspective, storing cards and making use of automated recurring payments will be much easier. Eliminating the need to provide CVV codes and partnering with a technology provider which has invested in the top level of PCI DSS compliance and tokenisation technology will go a long way towards simplifying the payment process for customers and protecting them against major security threats such as fraud and cybercrime. There really is no time to lose to get the right levels of security in place while ditching the three-digit CVV code.

**https://www.encoded.co.uk/day-life-contact-centre-card-payment/*

Web Payments

Give customers the option to pay securely by telephone or online. Integrate contact centre and web transactions with a 3D secure payment solution from Level 1 PCI DSS accredited Encoded.
Make regular transactions easier with Automated Recurring Payments.

Keep it Simple – Keep it Secure

Talk to Encoded to discover a more engaging and cost effective route to payments
www.encoded.co.uk
01293 229 700

ENCODED
secure automated payments

Deferred Debit Cards

A headache for Merchants and Payment Services Providers

Merchants and Payment Services Providers (PSPs) generally deal with three main types of card these are Debit Cards, Credit Cards and Charge Cards. The rules and processes surrounding each of these card types, has for the most part been clear, and consumer understanding of the differences between them, especially the distinction between Debit and Credit Cards, has been strong.

However, a fourth card type is becoming more and more prevalent in the UK - the Deferred Debit Card. And it's starting to cause headaches for consumers, merchants and PSPs alike.

A Deferred Debit Card is linked to a banking current account, similar to a traditional Debit Card, but where the value of a transaction is not debited from the current account's balance immediately. Instead, the total money for all transactions processed is deducted at a certain date, usually the end of the month, similar to the way that a Charge Card works. This can provide advantages for certain customers, especially those with large current account balances who may benefit from a longer period of interest accrual.

However, for merchants and PSPs there are three main factors which are likely to cause issues in the near future due to the increased adoption of Deferred Debit Cards in the UK. These include Financial Conduct Authority (FCA) guidance, interchange rates and a lack of consumer understanding.

When is a debit card not a debit card?

Visa and MasterCard both apply Credit Card interchange rates to purchases processed using a Deferred Debit Card. This makes processing a transaction on a Deferred Debit Card more expensive than a traditional Debit Card. Many merchants in the UK already add surcharges to Credit Card transactions to cover any additional expense, and most likely will expect their PSP to do the same and apply surcharges for transactions processed with Deferred Debit Cards. If a PSP is not currently adding an equivalent surcharge to Deferred Debit Cards transactions, this could result in an awkward conversation if the merchant identifies a discrepancy between surcharge income from their PSP and the Merchant Service Charge from their Acquirer.

Merchants who offer financial products and services and who are regulated by the FCA, will often request that their PSP does not allow customers to settle credit with a secondary credit line. This helps customers to avoid spiralling into worsening debt issues. The FCA Handbook, which sets out rules and provides guidance for all regulated companies, defines a credit line as "...payment card such as deferred debit or credit card..." Because of this, all PSPs providing payment services to merchants regulated by the FCA for the purpose of settling outstanding credit, should identify and **reject** Deferred Debit Cards as it could be seen as a secondary credit line.

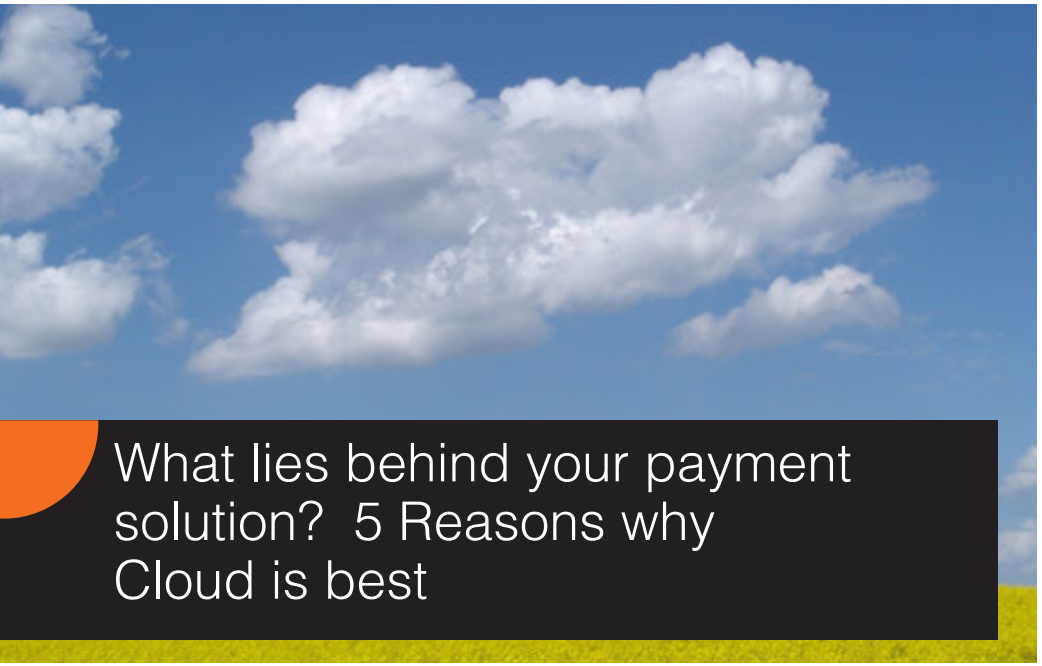
Whilst these two factors directly affect how merchants and PSPs should be handling Deferred Debit Cards internally, the issue is further exasperated by poor consumer understanding of the product and a lack of clarity from the industry.

Clarity required

Card Issuers often do not clearly explain the limitations to consumers before providing them with a Deferred Debit Card, and from a consumer perspective there is little to physically distinguish a Deferred Debit Card from a standard Debit Card. Cards look very similar, the branding is identical, with both card types displaying the traditional Visa Debit/MasterCard Debit logos. This undoubtedly results in confusion for consumers when, having been asked to pay a credit card surcharge or told that they cannot make a payment on their outstanding credit with a credit card, they look down at the card in their hand and see the Visa Debit logo looking back at them. Therefore, the situation can become very confusing.

Until consumer awareness of the terms and limitations of Deferred Debit Cards increases, it is the responsibility of the merchants and PSPs to provide clear feedback to customers. This can be achieved by ensuring that all messaging, both visual and audible, includes appropriate instruction and feedback for Deferred Debit Cards.

ENCODED
secure automated payments



What lies behind your payment solution? 5 Reasons why Cloud is best

Contact centres are often seen as the front line service of a business. They are at the forefront of customer service and therefore the long-term profitability of any organisation. Contact centres need to encompass every aspect of the customer experience, including providing information, solving problems, securing sales, processing payments and capturing data. In fact, they play a pivotal role and the latest technology is required to support them and maximise efficiency.

Taking a look under the bonnet

Payment solutions are often cited as the engine of the contact centre as they provide a way to complete a transaction and drive business forward. In terms of payment solutions security is a top priority and 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. While there is no such thing as a PCI DSS compliant payment solution it is wise to understand just what lies behind your system and whether the provider is PCI DSS compliant as an organisation. Working with a cloud-based payment solution provider can help to increase security and de-scope payment data for compliance purposes.

Here are five key reasons why a cloud-based approach to payments is best for business:

1 **Improved security / PCI DSS compliance** - when personal and card details are involved there is no room for error, secure handling of payment data is paramount. Working with a Level 1 PCI DSS cloud-based payment service provider reduces both the operational cost and management issues around compliance. Cloud suppliers typically have more security in place that many organisations have the skill or resource to deploy.

This is also good news with GDPR around the corner, which means a review of data policies and practices to ensure compliance with how data is kept throughout an organisation. The PCI DSS Standard is intended to protect cardholder data, therefore by complying with PCI DSS, contact centres are more likely to meet the new legislation and the burden of proof of compliance by demonstrating adherence to a recognised security standard.

2 **Improved scalability** - one of the key benefits of a cloud solution is the ability to scale up or down easily, without capital expenditure. For example, a Virtual Terminal Payments Solution, enabling contact centre agents to process payments over the phone, is suitable for multiple users which can be increased or decreased as required, all done in the cloud. Accessible from any location, agents can work from home or different sites and this flexibility means businesses can adapt to busy times without costly overheads.

3 **Supports disaster recovery planning** - in the event of any disruption to a company's own IT infrastructure, for example, flooding or a cut cable, contact centre operations supported by a cloud-based payment solution will still be able to take payments. Lost revenue, dropped calls and negative customer experience are avoided as a result of business continuity.

4 **Increased functionality offers a range of payment options** - for today's time pressured customers offering a variety of ways for them to pay speeds up the process and frees agents to handle more complex enquiries. Providing integrated online payments into a company's website, enabling recurring payments (repeat and subscription payments), or accepting credit and debit card payments via interactive voice response (IVR), allows customers to make payments quickly and accurately, reducing agent handing time and the associated costs.

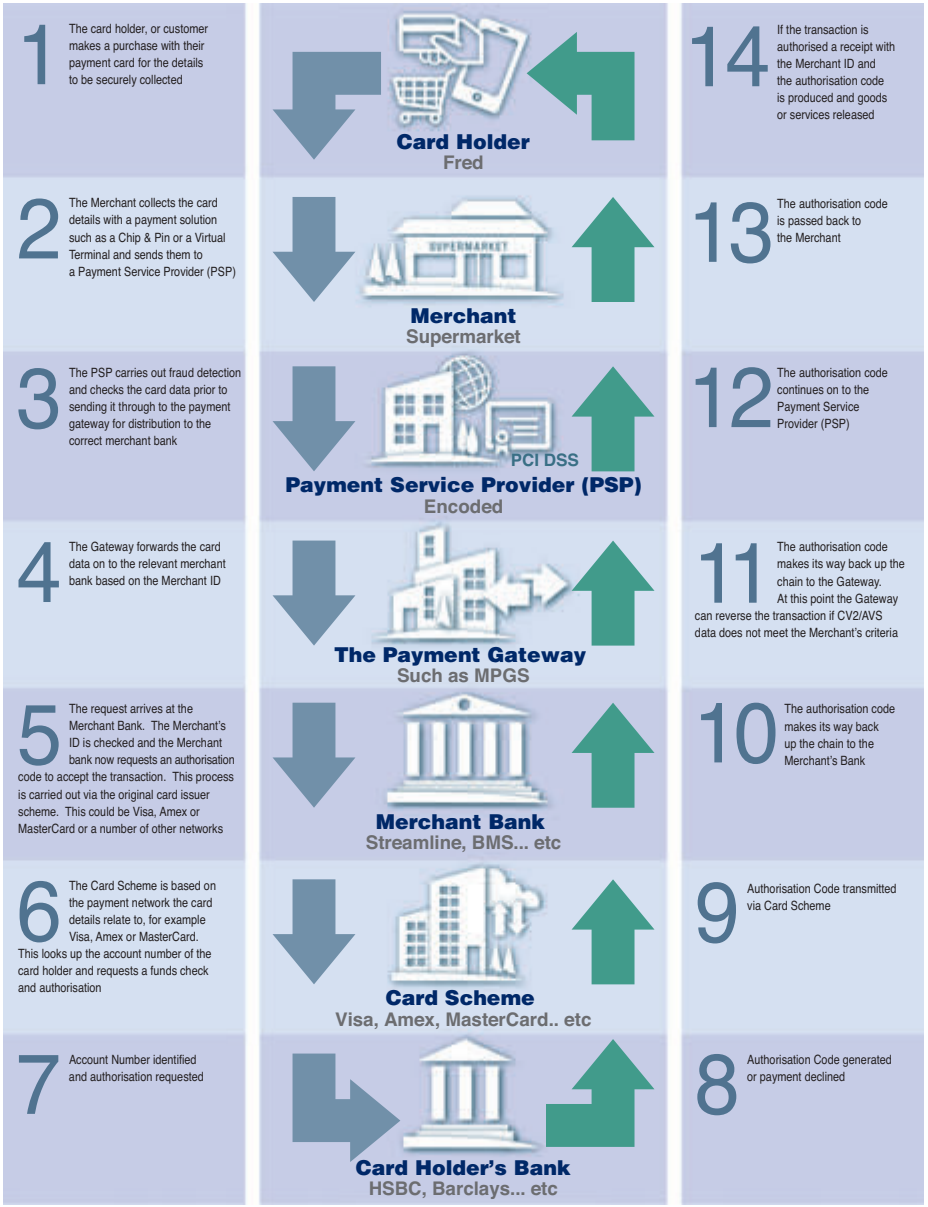
5 **Reduced capital expenditure and pressure on IT resources** - often cited as a key benefit of the cloud, the ability to add agents as required is a popular reason for choosing a cloud provider. Cloud-based payment solutions avoid costly upfront expenditure or the need for additional IT resources which makes handling the transition to cloud easier and more cost effective.

The 2017 edition of Call Centre Helper's Research Paper, What Contact Centres are Doing Right Now states that cloud uptake is set to rise rapidly in the near future with over a quarter of the 380 respondents having put plans in place to implement cloud technology. An additional 11% are reported to be considering the cloud within the next six to 12 months. While not all organisations are ready to make the switch to entirely cloud-based contact centre technology just yet, there is every reason to take a closer look under the bonnet of cloud-based payments right now.

ENCODED
secure automated payments

Lifecycle of a Card Payment

ENCODED
secure automated payments



The moral of the story is – work with a cloud-based payment solution provider to increase security and de-scope data for PCI-DSS compliance, both priorities today and in the future.

ENCODED
secure automated payments