ENCODED
secure automated payments

Telephone card payments and PCI DSS

White Paper

A look into card payments taken over the phone, industry requirements and the merchant's responsibilities.

- What are the real threats and what can be done to mitigate risks?
- What products are available and can service providers be trusted with a merchant's responsibility?
- Who is ultimately responsible for the loss of card data?

Includes – The four things you probably don't know about PCI DSS.

Author: Robert Crutchington
Contributors: Mary Phillips, Matthew Tyler

Contents

Executive summary

Making payments via a credit or debit card is now largely common place. With 55.6 million[1] credit cards issued in the UK alone and with over 90%[2] of the adult UK population carrying a debit card it's inevitable that payments will be carried out over the phone either directly with a merchant or via an automated system. It is convenient and in the most part, safe. With the introduction of 3D secure for online payments a decline of fraudulent transaction has been seen. Even so, in 2012 according to FFA, UK fraudulent transactions totalling £245.8m[3] were processed via mail order/telephone order (MOTO) card not present (CNP).

Currently there is no equivalent to chip and pin or 3D secure for payments made over the phone. It's the Achilles heel of the industry and many fraudsters will use automated phone systems to test recently stolen cards with small transactions to identify active cards prior to making larger purchases.

Businesses and organisations need to manage reputational risk and have a duty of care to their clients to ensure that card details taken for payment are not misused, lost or stolen. The introduction of the Payment Card Industry Data Security Standard (PCI DSS) compliance attempts to tackle this and aims to bring merchants up to an adequate security level that should minimise the risk of card data being abused or going missing. The first revision of PCI DSS was back in December 2004[4] when it became mandatory for merchants to adhere to it. However, recognition of its importance and necessity has been slow; 9 years on and only a handful of merchants responsible for losing card data have been fined. In the early days a lot of its principles directly conflicted with requirements issued by the FCA, which had more industry weight and legislation behind it. With the recent release of version 3 in November 2013 the message is finally gathering momentum that PCI DSS is to be taken seriously, the benefits and teachings of the standard should be evident. But is it?

Achieving level 1 PCI DSS is hugely expensive and the interpretation of the 258 controls often leads to 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 project to become PCI compliant or simply self-certifying compliance, 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 shout about.

Why is it that the general public are largely unaware of PCI DSS which sets out to protect them?

Accepting card payments over the phone is a processing method which is here to stay, either by automated system or by agent.

- So what are the real threats and what can be done to minimise the risks to the card data and the organisation taking the details?
- What products are available to merchants and can the service providers supplying them be trusted with a merchant's contracted responsibility?
- Who is ultimately responsible for the loss of card data if the requirement is outsourced?

This white paper attempts to answer these questions and empower the reader to enable them to start asking the right questions.

[1] Reference http://www.theukcardsassociation.org.uk/welcome/index.asp
[2] Reference http://www.payyourway.org.uk/special-focus/payments-counter/
[3] Reference http://www.financialfraudaction.org.uk/downloads.asp?genre=retailer Fraud the Facts 2013 PDF
[4] Reference http://searchsecurity.techtarget.com/feature/The-history-of-the-PCI-DSS-standard-A-visual-timeline

1 Taking Payments from within a contact centre – understanding the risks

Direct debit is by far the most popular method of bill payment in the UK. With over 2/3 of all household bills[5] being processed by Direct Debit this is a tried and tested, not to mention trusted method of transferring funds. However, when faced with the situation of requiring immediate payment, or if a Direct Debit has failed, then it usually falls back to processing a payment via a credit or debit card. Current standard practice is for a contact centre agent to request the client's card details and for these to be verbally given to the agent; upon receipt the agent manually processes the transaction and confirms the transaction with an authorisation code. It all sounds simple enough and for many years this has been sufficient. However, one of the most fundamental principles of PCI DSS compliance is that card details are not recorded, written down or retained by the merchant or its staff. So if the contact centre uses call recording, a common feature, then the card details are inadvertently captured and stored. Even without call recording procedures are required to ensure data is not written down or stored at any point in the payment process.

1.1 Identifying the primary risk to your card data

In recent years there have been some high profile cases of card data theft. These include TK Maxx[6], Target[7], The PlayStation Network[8] and Lush[9]. In some cases poor IT implementation and insufficient security allowed cyber criminals to hack databases. However, many security consultants consider that staff members themselves are a significant threat to data security. In many cases an organisation's security is only as good as the honesty and integrity of its staff. So what can be done to minimise the risk?

Prevention is better than cure; carrying out Criminal Records Bureau (CRB) checks on new staff is a good first step and is suggested by PCI in section 12.7, along with reference checks and credit history. Following this up with security awareness training sets the expectations of new staff members that security is taken seriously and that handling customer card data is not to be taken lightly.

In the 2013 Data breach investigation report by Verizon it is stated that in 2012 the majority of breaches as a result of company employees came about because people were careless with their access details rather than them maliciously steeling data. This carelessness was then exploited by a third party to gain access and commit the theft. Installing Malware for example attributed to 40%[10] of breaches. This threat can be reduced with training and policy controls. However the report also found that a huge amount of data breaches occur from external attackers exploiting vulnerabilities in company systems and networks. This Verizon report is an excellent read from which companies can draw comparisons to their own data environments and heed the advice offered.

[5] Reference http://www.payyourway.org.uk/special-focus/payments-counter/
[6] Reference http://news.bbc.co.uk/1/hi/business/6508983.stm
[7] Reference http://www.bbc.co.uk/news/technology-25681013
[8] Reference http://www.bbc.co.uk/news/technology-21160818
[9] Reference http://www.theguardian.com/money/2011/jan/21/lush-website-hack-customers-fraud
[10] Reference http://www.verizonenterprise.com/DBIR/2013/

1.2 Selecting and evaluating the right secure payment solution

There are many different solutions available to merchants that operate contact centres or require payment over the phone. The primary goal of any solution is to make it as simple yet secure as possible. The following is a selection of the more common phone payment solutions available. Each listed with a description and an ease of implementation, pros and cons of each and its knock on effect to PCI DSS compliance:

Fully automated IVR payments

Fully automated IVR payments services have been common place for many years now. They typically require authentication information from the caller to return an outstanding balance and then accept and process the payment card details. If designed correctly they are relatively simple to use and most importantly operate 24hr a day without having to speak to an agent.

Pros	Cons
Usually cheap and quick to implement.	There will always be a demographic that hates automated services.
Can be accessed directly without having to go through the company PBX. Ensures no card data is logged and reduces telephony resources.	Can lead to considerable frustration if the data entered by the caller isn't recognised or fails validation.
Can be used as an option to redirect the caller through to at the point of sale, this reduces average handling time (AHT) by about 1 minute.	If used in conjunction with speech recognition promotes the verbal broadcasting of sensitive card holder data.
Can be used with card tokenisation for repeat or frequent callers which can reduce the overall call duration by approximately 30 seconds.	
Can be used 24 hours a day 7 days a week.	
Removes telephony infrastructure and agents from PCI DSS scope.	

Virtual Terminal used by Contact Centre staff in conjunction with Pause and Resume call recording

This is by far the most common method of accepting card payment over the phone. This is where the merchant logs into a web based payment form and manually enters the customer's card data.
The transaction is processed and the authorisation code can be read out to the caller. This is the preferred method of payment for most people that like the "human" touch. Maintaining the conversation enables for free dialogue to be sustained. If no call recording is utilised then this method of accepting payment would be the simplest to implement, providing staff have been trained not to write down or retain the card data.

Pros	Cons
Keeps the personal touch.	Increases the average handling time of a call.
The pause and resume of call recording can often be automated. This is an excellent option which complies with both PCI and FCA regulations.	Some call recording systems don't allow for automated integration with the payment form which then relies on the staff member to manually pause and resume the call recording. Human behaviour would suggest that this will sometimes be missed.
Can be tailored to fit with existing CRM systems and business processes. Often simple to implement.	Usually more expensive than a fully automated option and involves staff training if a new payment form is required.
	Leaves telephony infrastructure and agents within PCI DSS scope.

Virtual Terminal with Dual-Tone Multi-Frequency DTMF tone suppression

This is a new spin on an old technology which has attracted a lot of attention; Suppressing DTMF tones has been around for many years, but to use this feature in conjunction with card payments enables call recording to be maintained throughout the call. Depending on the method of implementation it also has the added benefit of removing large parts of an organisation's infrastructure from PCI DSS scope. The implementation method is an important consideration as each has its own drawbacks and benefits. Options include having the service hosted in the cloud or installed locally (CPE Installation).

Pros	Cons
Enables the contact centre agents to maintain the conversation whilst the customer enters their own card details using touch tone keypad.	Currently extremely expensive to implement.
From the point of implementation onwards DTMF tones are not flowing through the network reducing the scope of PCI DSS compliance.	Increases the average handling time of a call.
	Adds an additional layer of potential failure into the telephony infrastructure; which could result in total loss of call traffic.

1.3 Telephone Systems – Logging

Confusion still remains for contact centres around call recording and transmission of Voice over Internet Protocol (VoIP) networks. Very little official guidance has been issued in relation to telephone payments, mainly because telecommunication solutions vary widely from geographic region to region.

Call recording is covered by the PCI Security Standards Council (SSC) in its 2011 guidance of call recordings, Sensitive Authentication Data (SAD) and PCI Compliance. However this did not cover the transmission of VoIP networks.

Costs scale with the scope of compliance, for example a 500 seat contact centre with 500 agent terminals for payment purposes would see all 500 still in scope. However, PCI SSC guidance only deals with any call recording aspects[11].

1.4 The Future – where the industry is going – Tokenisation and recurring payments

It could be argued that one of the most significant advances within the payments industry in recent years is the introduction of the Tokenisation of card payments. Tokenisation is the process of creating a meaningless number that references back to the genuine card details. By allowing organisations to retain card details in a secure way it minimises the risk of data loss but offers the merchant all the benefits of the continued payment authority available with Direct Debits.

Suddenly merchants can offer payment schedules for services such as clearing off variable balances at the end of each month; or recurring payments which are generally regular set payments of the same value, such as subscriptions or membership fees. Tokenisation can also be used to remove card data from the contact centre altogether. This sees customers Tokenise their card details either online or via an Interactive Voice Response (IVR) service. The resulting Token can then be used by the agent to authorise payments or set up payment schedules without having visibility of the original card details.

There are now services being developed which aim to maximise the use of Tokens. These include services such as SMS payments, mobile phone applications and near field communication (NFC) solutions. However, whilst these services will undoubtedly offer merchants new methods of payment, to make sure they are received well by card holders they need to include easy methods of changing details, stopping and suspending their use. It would be simple for less honourable industries to capitalise on the relative freedom the merchant has to make a payment on a Token. There are controls and legislation to protect account holders with Direct Debits but currently nothing is in place to protect the card holder. It is up to the merchant to adhere to a policy of responsible collection to avoid the negative PR that would result from abuse of such as service and the risk of charge backs.

[11] Reference https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf

2 PCI compliance

Recent news headlines have included stories of thieves stealing huge amounts of card data from high profile organisations. The public's reaction to this is usually… so what. Mainly because any theft of funds from stolen cards is insured and the money is promptly returned to the card holder's account. However, VISA and MasterCard have had enough. It stands to reason that if the merchant account owner had sufficient security in place then maybe the theft couldn't have happened or at least it would have been very difficult for the card data to be obtained. PCI DSS was the result of this belief. PCI DSS compliance became a contractual obligation that merchants – often unknowingly – signed up to when a merchant account was opened. As a result merchants could be fined for each card number stolen and used maliciously.

2.1 Understanding what PCI DSS really means and a merchant's responsibility

As security policies of the working environment are updated to meet with the requirements of PCI DSS compliance, payment service providers are constantly evolving their solutions to keep up with best practice. Some are more effective than others but it's important to bear in mind that there is no single solution that makes an organisation PCI DSS compliant; only solutions that help merchants achieve compliance. The most effective method of this is to de-scope the responsibility and exposure of card data away from the working environment.

Many solutions providers make the mistake of marketing their products as "PCI DSS Compliant". There is no such thing. To advertise this claim is to miss the very thing that PCI DSS is setting out to achieve, that is, to maintain a unified security standard to which merchants themselves adhere to. It is correct however to state that a given solution can help achieve compliance, or that by outsourcing the payment processing responsibility to a third party no card data is handled; but the merchant then has to prove that the chosen third party they are using is PCI DSS compliant. This is because the overall contractual obligation of compliance is always with the merchant and not with any third party.

2.2 The PCI DSS skills gap; a little knowledge is a dangerous thing

There remains a grey area within PCI DSS about what is acceptable to be compliant or what is not. Especially amongst merchants that choose to self-certify compliance. Even between Qualified Security Assessors (QSAs) that audit organisations there is a level of difference about what will pass and what will not. And then there are the many compliance officers, IT staff and finance managers who all have their own opinions on what is "needed" to become compliant. It's no surprise that once all of this confusion reaches the procurement department it results in incorrectly worded tenders and product requirement documents. These are then dutifully responded to by sales and marketing teams who respond with the same sound bites. This cycle then pollutes the industries understanding of the subject and starts a cycle of misinformation and confusion.

PCI DSS covers a great many areas and touches almost every aspect of an organisation. To truly understand the best practices for each of the 258 PCI DSS boxes that are required to be ticked takes a real specialist. However, oddly the payments security industry seems to have no shortage of people and organisations claiming to be PCI DSS experts. It's inevitable that like so many other aspects of life it can come down to one person's interpretation of what PCI DSS demands to achieve compliance.

Contact centre compliance is often viewed as a long and expensive project with the significance of cloud-based telephony often missed. PCI DSS Compliance by the contact centre should address risk and be achievable for a sensible and realistic cost. Looking at the subject of security as a whole and including the key vulnerabilities namely staff and the choice of third party supplier should, if carried out correctly, always result in large reductions in both the PCI DSS scope and the price of securing valuable information.

The PCI DSS Cycle of confusion

"A little knowledge is a dangerous thing"

2.3 Selecting the right payment partner – the VISA Merchant Agent List and its benefits?

Outsourcing the PCI DSS requirement to a third party is clearly the cheapest and most efficient way of achieving compliance. But how can merchants decide who to entrust their clients' card data with? VISA Europe manages a list of outsource partners involved in the payments market; these range from hosting companies, payment service providers, call centre providers, managed service providers and others connected to the industry.

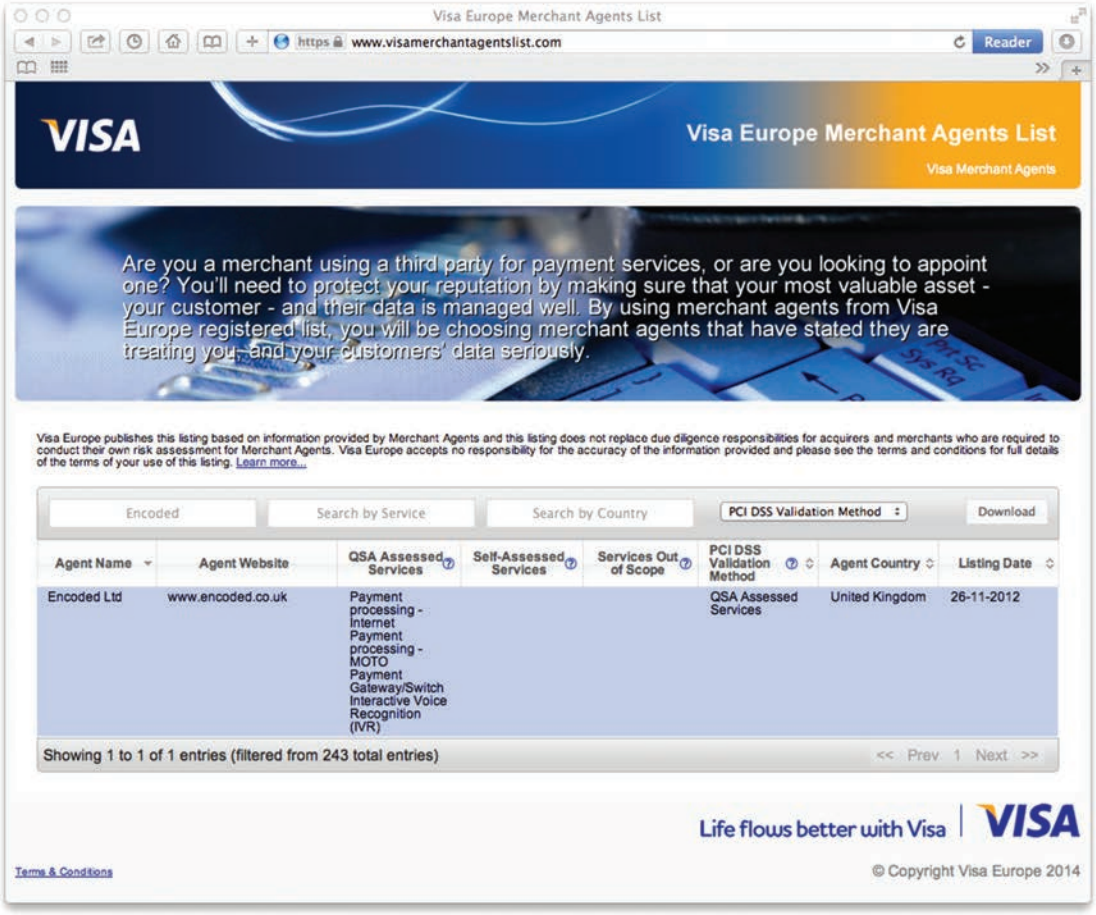
The list is designed to guide merchants when selecting an outsource partner and working only with companies on this list is likely to become a compliance requirement of merchants within the EU.

The list details what each company does, whether it has been externally audited or is self-assessed for compliance, whether it processes over or under 300,000 VISA payments annually. Finally the list includes what a company is validated to do for clients.

www.visamerchantagentslist.com

The VISA Merchant Agent list is simple and easy to search for your service provider, and if they are not listed then it's time to start asking some serious questions. At the time of publishing this white paper it was not mandated to be listed in the VISA merchant agent list, but it's in the pipeline.

But why choose a company on the list over one that isn't? Simple; because all members of the Visa Merchant Agent List have contractually agreed under section 4.1[12] of VISA's T&C's of list inclusion that if a breach of card data is reported that VISA has the right to audit their network and request any information relating to the breach. If a supplier is not on the list then neither VISA nor the merchant has the contractual right to investigate the breach outside of their own network. As such if the payment supplier does not feature on the VISA list then the merchant is solely and directly responsible for any card data loss regardless of where is originated.



[12] Reference https://www.visamerchantagents.com/terms-conditions.pdf

3 Conclusion

Therefore in answer to the questions posed at the beginning of this white paper:

- So what are the real threats and what can be done to minimise the risks to card data and the organisation taking the details?
- What products are available to merchants and can the service providers supplying them be trusted with a merchant's contracted responsibility?
- Who is ultimately responsible for the loss of card data if the requirement is outsourced?

In reverse order:

- Merchants are ultimately responsible for the loss of card data even if payment solutions are outsourced to a third party supplier. However, to many this comes as a surprise – the buck stops with the merchant. By entering into a contract with a bank, VISA or MasterCard in the event of a security breach the merchant is the one that will be fined.
- There is a myriad of products available to merchants to take them out of scope of PCI DSS. Solutions such as IVR payments or Virtual Terminal payments. However, the only way to establish whether the service provider supplying the solution is to be trusted with a merchant's contracted responsibility is by reference to the VISA Merchant Agent List to check a supplier's level of compliance.
- As with most security breaches the real threats are human ones. A rogue employee with a desire to steal or discredit an organisation is difficult to legislate against, however by working with a Level 1 fully QSA certified PCI DSS compliant payment provider the risk is mitigated and the chances of large fines significantly reduced.

Four things you probably don't know about PCI DSS

Although Visa®, MasterCard®, JBC®, Discover® and American Express® created the Industry Data Security Standard (PCI DSS) in 2004 it remains surrounded by confusion and misinformation. Many organisations with call 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 compliance is achieved.

Here are four PCI DSS lesser known but extremely important facts:

1 Responsibility

In December 2014 version 2 of the PCI DSS standard will be retired. All PCI DSS compliant companies must meet the levels laid out in Version 3.
On the whole version 3 isn't too problematic and just clarifies responsibility. To this end all suppliers of payment services must include in their contract a full list of all 258 controls clearly showing who is responsible for which control. This can be the client, the supplier or both. If a breach is reported and the subsequent forensic audit discovers where the breach occurred the contract will form the basis of accountability.
This potentially takes the first step towards holding suppliers accountable for lost data, which currently solely lies with the merchant.

2 VISA will never fine the merchant

It is a common misconception that VISA fines merchants for card data loss.
This is not the case. VISA would not and cannot fine a merchant for card data loss. This is because VISA does not have the contractual relationship with the merchant, but does with the Acquirer (the bank or financial institution that processes card payments on behalf of merchants).
It is the Acquirer that a merchant has a contractual relationship with and not VISA. It is the responsibility of the Acquirer to make sure its merchants are compliant. As such it is the Acquirer that issues fines, increases transactions charges for non-compliance and imposes compulsory PCI program costs on to merchants and not VISA. None of this revenue makes its way back to VISA but is used to fund the compliance program. VISA will fine the Acquirer if its merchants are not compliant.
If a breach is reported and a merchant is found to be either non-compliant or compliant but negligent, fines are collected from the merchant's account in the form of withheld revenue. Settlement of payments resumes once the fine value has been collected.

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

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. Only companies and other legal entities can be PCI compliant, not software. However, this misconception is perpetuated by 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 the misconception in order to win business. So the PCI DSS cycle of confusion continues.

See diagram on page 7.

4 Only Select suppliers that feature on the VISA Merchant Agent List website

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 Merchant Agent List which 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 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 on site security assessment by a Qualified Security Assessor (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 who you are dealing with and their PCI DSS credentials.

About the Authors and Encoded

Robert Crutchington, Managing Director, Encoded

Robert Crutchington was a founding director of Encoded Ltd, the secure automated payment solutions provider, and is still involved with the company on a day-to-day basis. Launched in 2001 Encoded is fully PCI DSS Level 1 accredited which applies only to organisations that process and/or transmit more than 300,000 transactions per year. Rob is a computer science graduate who began his career as a systems engineer specialising in ATM (Asynchronous Transfer Mode) protocols combining audio, data and video for several of the country's major infrastructure organisations.

Mary Phillips, Head of Marketing, Encoded

Mary Phillips has been involved in the contact centre world for over 20 years. Mary sold her first telemarketing company to multi-national contact centre outsourcer Sitel in 1997, where she remained as marketing director until starting her second company PRA in 1999. Since then Mary has worked with contact centre solution providers including Q-Max Systems, Intelecom and Encoded. Mary is passionate about standards and security in contact centres and regularly writes on behalf of her clients for the contact centre press.

Matthew Tyler, CEO, Blackfoot

Matthew Tyler has 25 years experience working with some of the largest brands in strategic risk, security and compliance. In the mid 1980s Matthew worked for the fledgling Financial Services Authority (FSA) in the UK, specialising in Securities Trading and Investment Management. Matthew then worked for a string of international Finance organisations including Standard Chartered and Lloyds of London. Matthew formed his own wealth management company; which he sold in the early 1990s. After a year of world travel Matthew settled in Australia where he started a couple of small IT Security businesses focusing on regulatory compliance.

When Matthew returned to the UK he set up several IT businesses ranging from Deep Packet Inspection, SEO analytics through Risk Management to founding Blackfoot UK in 2008. Blackfoot is now a leading Information Security, Risk and Compliance consultancy helping some of the largest retail brands, financial institutions, insurers, manufacturers and industry associations manage Security, Risk and Compliance. Matthew's expertise lies in both 'grasping the big picture' and assisting large organisations commercialise opportunities. Blackfoot's mission is to enable its clients to understand and mitigate the real world risks they face.

Encoded

Encoded is a leading PCI DSS compliant provider of interactive contact centre payment solutions. Encoded Ltd was founded in 2001 to offer affordable, pay-as-you-go solutions to contact centres both large and small. In 2011 the company went through full PCI DSS Level 1 accreditation with an external Qualified Security Assessor (QSA) and was awarded the top level of compliance and an Attestation of Compliance (AOC). This level of compliance only applies to organisations that store, process and/or transmit more than 300,000 Visa transactions per year.

Encoded operates as a long-term consultative partner with many of its customers which range from major enterprises to more boutique SME businesses in the UK and Internationally. Encoded's established network of partners means it can provide flexible cloud-based or customer premises equipment (CPE) solutions at competitive prices.

Encoded Solutions Include:

- Interactive Voice Response (IVR) Payments
- Virtual Terminal Payments
- Agent Assisted Card Payments
- Online Payments
- Self-Service Recurring Payments
- Recurring (stored cards) Payments

Notes

Automated Card Payment Solutions

Encoded specialises in solutions that reduce costs, increase profits and improve customer experience.

Encoded solutions include:

Interactive Voice Response (IVR) Payments
Virtual Terminal Payments
Agent Assisted Card Payments
Online Payments
Self-Service Recurring Payments
Recurring (stored cards) Payments

For more information about how Encoded solutions can help your business or contact centre please speak to one of our payment experts on 0845 120 9790

ENCODED
secure automated payments

Encoded Ltd
1 Stanley House Kelvin Way Crawley
West Sussex RH10 9SE United Kingdom

t 0845 120 9790
f 0870 830 1945
e sales@encoded.co.uk

www.encoded.co.uk

PCI Compliant
Level 1 PCI-DSS Service Provider

About Encoded

Encoded is a leading provider of interactive voice response solutions and automated payment solutions. All the company's services are designed to fulfil three key objectives:

Reduce costs by automating business processes
Increase sales by offering new fulfilment channels
Improve customer service by maximising resource efficiency

Encoded was established in 2001 to offer affordable, pay-as-you-go solutions to the growing telecommunications requirements of small and large businesses. Today, the company's software regularly supports 30 million customers and 10 million calls globally and automates £60 million of secure payments without operator intervention.

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