AKJ Associates

PCI DSS:
Case Studies in Excellence

pci WINNER

Awards for Excellence 2018

PROVE IT

2018 events

PROTECTING DATA
e-crime & cybersecurity
CONGRESS
MANAGING RISK

6th & 7th March 2018
London

e-crime
FRAUD FORUM

7th March 2018
London

PROTECTING DATA
e-crime & cybersecurity
CONGRESS
MANAGING RISK

20th March 2018
Dubai

PROTECTING DATA
e-crime & cybersecurity
FRANCE
MANAGING RISK

11th April 2018
Paris

PROTECTING DATA
e-crime & cybersecurity
GERMANY
MANAGING RISK

19th June 2018
Munich

pci
LONDON

5th July 2018
London

PROTECTING DATA
e-crime & cybersecurity
CONGRESS
MANAGING RISK

19th September 2018
Abu Dhabi

SECURING
THE LAW FIRM

20th September 2018
London

Securing
Online Gaming

2nd October 2018
London

PROTECTING DATA
e-crime & cybersecurity
MID-YEAR
MANAGING RISK

18th October 2018
London

PROTECTING DATA
e-crime & cybersecurity
SPAIN
MANAGING RISK

22nd November 2018
Madrid

PROTECTING DATA
e-crime & cybersecurity
NORDICS
MANAGING RISK

27th November 2018
Stockholm

PROTECTING DATA
e-crime & cybersecurity
BENELUX
MANAGING RISK

6th December 2018
Amsterdam

To sponsor,
please call Robert Walker on +44 (0)20 7841 2926
or email robert.walker@akjassociates.com

PCI DSS: taking the pain out of GDPR?

The advent of more comprehensive national and international regulation, especially the EU General Data Protection Regulation (GDPR), may seem to reinforce the idea that PCI DSS is becoming less relevant. But is it?

By February 1, 2018, version 3.2 of the PCI DSS will set new standards for safeguarding payment data. GDPR is imminent, and its arrival in May will make businesses more accountable – and more liable – than ever before. Call centres will be obligated to let callers know just how their data is being handled, stored, processed and used. Compliant payment security is now a key priority.

To effectively manage this period of transition, PCI specialists need the support of the right partners. For solutions providers, there is a valuable opportunity to prove themselves, and differentiate from the rest of the market.

And as issues of data loss, fraud and cybersecurity become an integral part of operational risk infrastructure, their clients are looking for the right support to move their programmes onto the agenda of senior management, clients, and budget holders. Because while times change, some things remain the same.

And one of those is the need for a detailed set of guidelines to define a clear framework around which companies can build their data security programme, as it evolves from voluntary cybersecurity measures to legally mandated regulations.

While organisations prepare for the onset of regulatory change, they are looking for a familiar set of standards that has benefited from continuous evolution, and is supported by a large number of enterprises across all sectors and at all points in the payment chain. This is, and will remain, PCI DSS.

Amanda Oon
Editor

Editor and Publisher
Simon Brady
e: simon.brady@akjassociates.com

Design and Production
Norma Kelly
e: normaewart@me.com

Forum organiser:
AKJ Associates Ltd
27 John Street
London
WC1N 2BX
t: +44 (0) 20 7242 4364
f: +44 (0) 20 7831 2175
e: amanda.oon@akjassociates.com

Printed by: Method UK Ltd
Baird House
15–17 St Cross Street
London
EC1N 8UN
e: hello@thisismethod.co.uk

Articles published in this magazine are not necessarily the views of AKJ Associates Ltd. The publishers and authors of this magazine do not bear any responsibility for errors contained within this publication, or for any omissions. This magazine does not purport to offer investment, legal or any other type of advice, and should not be read as if it does. Those organisations sponsoring or supporting the PCI Awards for Excellence 2018 and/or the PCI London 2018 bear no responsibility, either singularly or collectively, for the content of this magazine. Neither can those same organisations either singularly or collectively, take responsibility for any use that may be made of the content contained inside the magazine.

Contents

The cybersecurity customer knows best

Choosing a security vendor is one of the hardest tasks for companies seeking cybersecurity. These case studies are part of the process of increased transparency that will aid choice and make the business case for compliance and security more obvious.

For years, frustrated CISO's and senior IT security professionals have struggled with lack of engagement from senior management, board members and those who hold influence and budget.

Times are finally changing. Cyber-threats are among the top concerns cited by CEO's, not least as a result of the wave of attacks and data breaches reported in the mainstream press over the course of 2017. Cybersecurity has become a household talking point.

In addition to these highly-publicised cyber-crimes, businesses are also facing profound disruption from digital rivals and are responding with their own attempts at digital transformation. These inevitably create new cyber-risk exposures or at least increase organisations' attack surface.

And the oncoming array of regulatory change means that board members, clients and stakeholders are recognising data loss, fraud, and cyber-risk as real threats to the business that require their attention.

As a consequence, investment in cybersecurity solutions and staff is on the increase: the worldwide spend on cybersecurity is expected to climb to $96 billion in 2018 and ever higher beyond that. However, that figure hides an uncomfortable question. How can vendors and end-users prove their value in an opaque and changing market?

How to prioritise spend?

The other way to frame this question is, "How can potential purchasers of cybersecurity solutions choose from the vast range of products currently being marketed?"

With less than half of boards actively participating in their companies' overall cybersecurity strategy, the CISO (when there is one) still faces challenges. And one of the most significant is that he or she still lacks the definitions and risk metrics that senior management demands in order to allocate resources appropriately. There may be budget, but how do you prioritise spend?

Now that CISOs and their programmes are in the spotlight, they need to prove that they can deliver business efficient security, at the right price, and communicate its ROI in a language that their board will understand.

It is impossible to achieve this without the support of the right partner, who will deliver solutions on time, within budget, and prove the value of securing information and protecting data as a critical business asset.

Over the course of 2017, AKJ Associates has spoken to hundreds of end-users to uncover their perspective on the solutions market in general and the complexity of the vendor ecosystem, and to gauge their main priorities when choosing such a partner.

Through our events, and a series of detailed market research polls that we are continuing to develop in 2018, we have gained exclusive insights into the procurement process and into the key qualities and product variables that help vendors stand out from the crowd.

Prove your performance

Throughout all of these exercises, the main and recurring theme told to AKJ by end-user after end-user remains: prove it. That is, prove that your solutions work for relevant companies. Prove that they do what they say they do, that they can be implemented cost effectively, that they are supported and that they are scalable.

At last year's PCI awards, decision-makers at end-user companies were starting to challenge the lack of data in the cybersecurity marketplace and to demand an increased level of validation from their existing and potential solution providers.

This year, with new products continuing to flood the marketplace, and with new technologies being hyped as the latest catch-all, the competition is greater than ever, and so is the need to show you have real life expertise in addressing your clients' specific business needs.

The smart vendors have noticed this trend. Increasingly they have abandoned the claim that they cannot reveal clients for reasons of confidentiality or security. Increasingly their websites emphasise not just the quantity but the quality of their clients. And more and more vendors are using case studies combined with genuinely informative thought-leadership to demonstrate their expertise and experience. They understand that they need to show that they are more focused on their target buyers' key priorities than the competition.

Real testimonials needed

The most effective way to do this is to show that they have experience in solving similar problems for their prospective clients' peers. With a lack of clear metrics to differentiate and value the merits of solutions providers, end-users are looking for real-life testimonials.

These can help vendors prove their credentials and show that they can answer the following questions:

- How did implementation go: on budget, on time?
- Did the product deliver the outcomes it promised?
- What measures of performance and value can you share?
- What are your experiences of this solution/vendor in terms of scalability, ease of integration, ease of use, ease of update, service and support?

With our content, AKJ Associates have always emphasised the importance of such case studies to demonstrate the value and help prove the ROI of a service, and to reward those vendors who have achieved real success in their market.

When high-profile attacks and their financial and reputational consequences dominate the media, sharing success stories is not only a refreshing break from

FUD. It is also a valuable commercial advantage.

Most end-users now understand that they need to prove their own commitment to cybersecurity to their customers, shareholders and other financiers and insurers. They also recognise that the most effective way to do this is to work with an established vendor who has a background in addressing the problems they need solving.

Demonstrating value

PCI DSS – and the regulatory framework it provides – forms an important foundation on which companies can base their key priorities for protecting cardholder data, and providers can tailor their solutions to address these needs.

Whether it is moving to the Cloud, de-scoping phone payments, or building a customised, tailored PCI DSS network, the changes that the new version PCI DSS 3.2 will bring in February have created a specific set of business challenges and demands for any company that manages payments and card data.

The vendors featured here have all risen to these challenges. They have gained validation from their clients themselves, as these have rated them as the go-to solution for their PCI DSS challenges.

Their stories prove not only the vendors' expertise, but also the importance of sharing real life examples as a way to justify business value and to stand out from the crowd.

Vendors who can prove, through detailed case studies, that their products have been installed on time and on budget, and work as advertised, will be the clear winners in the market. These are the solution providers who are likely to win the battle for new business.

This was proven with our inaugural PCI awards, which showcased the highest standards in preventing fraud, protecting card data, and integrating PCI DSS regulations alongside business efficiency.

Following its success, our second annual awards ceremony reflects how the market, its main players, and their stories, have evolved. Our winning suppliers have shown how they have been able to implement security solutions that are commercially efficient, reliable, and scalable without additional costly hardware and software requirements.

Real-life projects, real achievements

Each award is presented for a real-life PCI DSS project, successfully implemented for an individual client. They have been chosen as exemplars of PCI DSS best practice on the part of both solutions provider and buyer.

To stand-out, these case studies had to demonstrate clinical interpretation of client needs, flawless implementation, flexibility of deployment and strong after-sales service and support.

Above all, they demonstrate that, as threats become more sophisticated and clients become more discerning, the leading vendors will rise to their demands – and to the top of clients' preferred supplier lists.

These case studies showcase products that have provided great functionality and value for money, and they stand out for the business benefits they provide to clients. In today's opaque and oversaturated vendor ecosystem, your last success can be the best tool to winning your next opportunity. ●

Armor: Securing hybrid Cloud, complying with PCI DSS

Moving to the Cloud is a big step for any organisation. For a credit union with 200,000+ members needing access to their data and the assurance that data is safe, it is a particular challenge. Armor Anywhere's security and PCI 3.1 compliant solution lets BCU focus on adding value.

Credit unions in the United States, like other organisations that manage funds around the world, face many challenges when operating online. Unlike traditional banks and other financial institutions, they are not-for-profit entities that provide services for members, as opposed to customers and businesses. Because of this unique relationship, special care must be taken to ensure their members can access financial data easily and securely. Balancing these customer expectations and operational objectives, while maintaining robust security, can be a challenge for even the most security-savvy credit union.

This was the challenge Illinois-based BCU (Baxter Credit Union), with assets of $2.8 billion and more than 200,000 members, faced when seeking a convergence of member satisfaction and cybersecurity while also supporting their hybrid Cloud strategy.

Embracing the Cloud

BCU prides itself on offering members more innovative services than can be found at many other financial institutions. Of course, standing apart from the competition requires thinking outside the box, and in the case of BCU, thinking beyond legacy, on-premises hosting solutions for their sensitive data workloads. To truly differentiate themselves, they needed to hybridise their infrastructure and embrace the public Cloud.

About BCU
The fastest growing credit union in the last 30 years
$2.6 BILLION
200,000 MEMBERS

BCU is regarded as having set new standards for bringing together technology and member service in the fast-changing world of financial services delivery.

For Jeff Johnson, Chief Information Officer at BCU, the potential benefits of fully embracing Cloud hosting were obvious.

"The Cloud in general is a fantastic opportunity to put our time and resources towards non-commodity IT practices," he

ARMOR ANYWHERE - SECURITY ON MICROSOFT AZURE
SECURITY FEATURES
AZURE ENVIRONMENT

says. "Having vendors that can support both physical and Cloud data centres allows for more consistencies in BCU's processes, fewer vendors and contracts to manage, and the ability to form long-term relationships that can meet our strategic security needs. The more automated tools we have, the fewer manual activities that need to be performed, allowing us to free up our professional resources to add great value."

Unfortunately, their existing security provider was not capable of supporting their move to a hybrid Cloud infrastructure, so they began searching for a provider who was.

Addressing Compliance

Similar to the situation they encountered with their own managed security provider, BCU soon discovered that finding the right security partner would not be an easy task. "We found a lot of resistance and hesitation from managed security providers when it came to the Cloud. Even though the systems run the same, they wanted to diminish the services offered just because it was on the Cloud as opposed to being on-premises."

There was the additional complication of BCU meeting their PCI compliance requirements. Any solution they integrated into their Cloud strategy would have to be both agile and secure – that is, flexible enough to adapt to any Cloud infrastructure whilst also capable of meeting the standards set by the PCI Security Standards Council.

Why Armor

A recommendation from a vendor led them to Armor. They were quickly impressed by Armor's managed approach and the level of protection of Armor Anywhere, a PCI 3.1-compliant managed security solution, which provides for workloads on Microsoft Azure. With Armor Anywhere, they have the flexibility and level of control needed to achieve their Cloud-based aspirations.

A better Cloud

Armor Anywhere secures BCU's Microsoft Azure-hosted instances from persistent cyber threats – providing 24/7/365 incident detection and response along with advanced threat intelligence capabilities for their members' sensitive data.

"One thing that intrigued us with Armor versus our other managed security provider was Armor's Cloud aptitude and competency," says Johnson. "Working with the Security Operations Center (SOC) has provided great resource-saving value. The team members are knowledgeable about their clients, as well as security, so there aren't unnecessary escalation events sent to our team to deal with."

Armor's proactive approach to Cloud security services contrasts with other managed security providers the credit union encountered – including their previous Cloud security provider. Armor's focus on expanding its services to support public Cloud infrastructure was also a welcome approach for BCU.

BCU also benefited from Armor's expertise in mitigating online threats, a value that Johnson says is essential to maintaining a secure Cloud environment.

"The first step to overcoming the risks of hosting in the Cloud is having the capabilities to identify abnormal behaviour as it's happening, and then responding instantly to minimise or prevent any damage," he explains. "With Armor Anywhere, we have the detection and prevention tools we need to feel secure in our environment."

Sharing responsibility on Azure

Armor Anywhere also helps BCU manage the shared responsibility model of securing workloads on Azure – ensuring they maximise the value of their public Cloud investment.

This is a core benefit for Johnson and BCU, as they are keenly aware that accountability for the security of their Azure instances falls to them.

"You can't lose focus that, at the end of the day, managing security on Azure is still our responsibility," he says. "You need to make sure that when you move your assets into Azure – just like when you move your assets into a new data centre – you're maintaining security and you're bringing the appropriate security with you as you go to the Cloud."

BCU has seen Armor Anywhere evolve more rapidly than services offered by Armor's more traditional hosting-focused peers. These enhancements include greater vulnerability and patch management, along with enhanced monitoring features such as host-based intrusion protection.

> **"One thing that intrigued us with Armor versus our other managed security provider was Armor's Cloud aptitude and competency,"**
>
> *Jeff Johnson, Chief Information Officer, BCU*

Characterising Armor as "more of a value-added partner," Johnson is optimistic about the relationship going forward: "The responsiveness has been great and so has the evolution of the product. We're looking forward to expanding its usage across our services." ●

CardEasy from Syntec: De-scoping phone payments

CardEasy 'keypad payment by phone' is Syntec's patented DTMF solution for card payments in contact centres. Founded in 1998, Syntec is an independent network operator providing managed contact centre services for merchants in the UK and worldwide. CardEasy is flexible to deploy, and works with any telephony, not just Syntec's.

Background
Syntec's CardEasy 'keypad payment by phone' DTMF touchtone system enables merchants to de-scope their call centre environment and call recordings from PCI DSS, reducing the risk and costs associated with managing card payment transactions in their contact centres, including outsourcers, homeworkers, and disaster recovery sites.

CardEasy increases customer trust in your brand and improves the customer/agent experience, improving average call handling times and reducing mis-keying and lost transactions.

Syntec is a level 1 PCI DSS managed service provider, Visa Merchant Agent and participating member of the global Payment Card Industry Security Standards Council (PCI SSC). Founded in 1998, Syntec is an independent UK network operator, providing a range of telecoms and managed services for contact centres to a wide range of clients internationally.

CardEasy
With the CardEasy PCI DSS solution, instead of callers/customers reading their payment card numbers out to the call centre agent, they are asked to enter them using the keypad of their own phone, live in mid-conversation with the agent (using the DTMF or dual tone multi frequency touchtones to convey the numbers, instead of voice). There is also a customer self-service autopay alternative, which works with interactive voice response (IVR) systems where no agent assistance is required and for 24/7 service.

The encrypted card data bypasses the call centre via the CardEasy Cloud and payment authorisation is confirmed back to the agent's screen in real time. Integration with the Payment Service Providers (PSPs) is at Syntec level. So the sensitive card data is kept out of the contact centre environment altogether and is no longer available to be heard, seen, stored or compromised.

A success story for Staples

Office supply retailer Staples approached Syntec in 2015 to supply a mid-call DTMF payment system for their call centres in Europe, as they wanted to increase data security without compromising customer experience or losing transactions.

Why CardEasy?
Staples were very happy that in the middle of the conversation with agents, using CardEasy, a customer would simply be asked to type their PAN into their phone keypad instead of having to read it out. This is then sent via CardEasy to their Payment Services Provider securely for authorisation in real-time for the agent, without interrupting the usual call flow or having to handle (or store) the card numbers themselves.

The Project
Staples started rolling out CardEasy in their various UK call centres in 2016, deploying the hybrid 'on premises' option with their existing Cisco telephony and various back office systems, and returning a tokenised PAN for repeat-purchase use.

Training support was provided by Syntec and the results went so smoothly that Staples took up their option to roll CardEasy out to other European sites with hundreds of users - a project which has now been successfully completed.

The Results
Staples' call centre environments and any call recordings are covered by Syntec's level 1 PCI DSS service provider compliance, using the CardEasy managed service.

Staples can no longer hear, see nor store sensitive card numbers in their call centres and so cannot suffer a breach or fraud from having card numbers compromised there.

Their staff no longer need to be monitored for PCI purposes and so can concentrate on their customer service and sales jobs, as the card data is no longer there to worry about.

Management can also concentrate on running the commercial side of the business rather than being distracted by PCI concerns in their call centres.

The smooth operations of Staples' call centres have not been interrupted during or after the project.

CardEasy supports their legacy and also new ERP systems. CardEasy also provides Staples with a tailored 'mass tokenisation' service for their major corporate clients for easy and secure use of employees' cards when ordering.

The CardEasy merchant reporting suite allows for monitoring of response times from different PSP's in use; monitoring of agent/customer capture failures; and monitoring PSP transaction failures, amongst other features. ●

"CardEasy 'keypad payment by phone' was the perfect fit to resolve the PCI compliance and data security needs in Staples' major call centres in Europe. This was because of its ease of use mid-call, the breadth of PCI DSS issues it resolves in one go, the flexibility of integration with all our differing systems and the ability for them to meet our tokenisation requirements."

Jurgen van Roon Senior Project Manager – Security, Staples

Miele PCI DSS case study

Miele is a leading premium domestic and commercial appliances manufacturer. This case study explains how it is using Syntec's CardEasy secure 'keypad payment by phone' system in order to de-scope its call centre and call recordings from PCI DSS requirements.

Cloud/hosted CardEasy service

Miele was originally considering a premises-based touchtone payment (DTMF) system to de-scope its call centre environment and call recordings from PCI DSS regulations, with its agents still taking payments from customers in mid-conversation.

The network-hosted version of the CardEasy keypad payment by phone solution turned out to be more attractive for Miele, because there is no equipment to buy and the sensitive card data never enters the call centre environment, thus reducing PCI DSS compliance requirements almost to nil with just a minimal self-assessment questionnaire (SAQ) to complete.

> **"Miele selected Syntec's pioneering, hosted CardEasy system to enrich customer service whilst de-scoping us from large sections of PCI DSS regulations, which otherwise require significant cost and effort to satisfy."**
>
> *Paul Aram, IT Manager, Miele*

Miele

CUSTOMER FEEDBACK

"Oh OK, that's a good idea – it's nice to know my card details are kept safe"

"I wish more companies handled my card security this way"

AGENT FEEDBACK

"Quick and simple, easy to go through with the customer, faster than taking card numbers and more secure"

The hosted CardEasy solution proved quick and easy to trial and subsequently deploy with no new equipment needed (as it integrates with existing phones and payment systems on an SaaS basis)

CardEasy was integrated with Miele's payment gateway for easy trial and rollout (CardEasy is now integrated with all major PSPs on behalf of Syntec's CardEasy clients).

As an Ofcom-regulated telecommunications provider, Syntec was also able to give Miele expert advice on integrating CardEasy into its existing infrastructure.

Results

- Miele achieved PCI DSS level 1 with mid-call secure payment; improved transaction speed and customer service; and with no capital expenditure outlay.
- Miele is so satisfied with the CardEasy system that it has now integrated this with Syntec's AgentCall contact centre management solutions across its operations.
- 95% of transactions went through CardEasy on day 1 of launch, with no age barrier to take up
- Shorter call times due to one less process (of agent taking card numbers before entering them)
- Less mis-keying achieved due to this removed process too

Allied Irish Bank— a customised solution

AIB

Background

In recent years AIB has been dealing with an increased amount of payments that were taken by card over the phone and has expanded its call centre-based staff. AIB needed a secure and user-friendly solution for taking card payments over the phone that put customer security, PCI DSS compliance, and removal of risk at the forefront of its operations.

Why Syntec?

The Syntec CardEasy solution offered AIB the best possible fit when AIB was weighing up potential solutions. Syntec offered AIB an efficient, easy-to-use product that removed all records of card details from its call centre, including call recording, thus increasing customer security and reducing risk.

Results & benefits of CardEasy

- The full card details of the customer do not enter, and are not stored on any of AIB's systems.
- No need to transfer the call to an IVR for payment to be taken. This allows AIB to build a stronger relationship with the customer.
- De-scopes the call centre from PCI DSS compliance.
- Increased customer security and satisfaction.
- Easy to use for agents and customers.
- The platform was easy to scale to other areas of the business.
- The CardEasy implementation was customised to meet the specific needs of AIB.
- CardEasy provides agents with the ability to identify if the card is a credit or debit and make a decision to progress or not based on the procedures in place.

"The driver for CardEasy was that we wanted a solution that increased security whilst decreasing the compliance aspect for us – mainly PCI DSS compliance. The CardEasy solution is now being extended to other teams at AIB as it very easily de-scopes us from PCI DSS compliance and mitigates the risk of any internal fraud happening. The platform is scalable and easy to use and this is a key driver in our decision to expand, along with the confidence we have in Syntec who have been instrumental in a smooth implementation, guiding us and offering insight into the design of our internal call flows and helping us address any issues we encountered. We got great support from Syntec: they helped customise the solution as needed and provided excellent support in its launch and expansion.

The CardEasy solution, being in-call, has enabled us to manage PCI compliance without the need for us to transfer a call to an IVR. This is key for us in terms of engaging with the customer on the phone and building rapport, without transferring the call to an automated system where we are not on the end of the line in support.

Once the agents were used to the change, they too have seen this as favourable. Its ability to flag to us whether a customer is using a credit or debit card before we authorise a payment has also made it far easier for our agents to stay compliant and avoid taking payments by credit card, which has helped them stay compliant and made calls easier to handle."

Eoin Heneghan, Head of Collections, AIB.

In 2015, Charles Tyrwhitt was being pressured by its merchant acquirer to become PCI DSS compliant for card payments by phone in its call centres. Based on its previous experience with Syntec's other call centre services, Charles Tyrwhitt decided to deploy the CardEasy 'keypad payment by phone' DTMF system, which keeps the sensitive card information (PAN and CV2) out of the contact centre entirely and thus de-scopes the contact centre operation from PCI DSS regulations and audits.

"We wanted to further enhance data security in our call centre and decided to use Syntec's secure phone keypad payment (DTMF), as it's important to our customers that our payment solution is safe and easy to use. CardEasy works just as effectively for callers in the USA, Germany and Australia as in the UK."

Simon Kerry, Chief Information Officer, Charles Tyrwhitt

... continued from page 10.

Deployment Flexibility

The CardEasy system can either be hosted in Syntec's network or deployed as a telephony-agnostic, hybrid premises-based version, supporting SIP, ISDN or any mix of the two. If the merchant has SIP-based telephony, they can opt for a fully Cloud-based variant, which removes the need for any premises-based equipment. All versions use the CardEasy cloud for their PSP connections and the hybrid CPE and 'pure Cloud' options work with the merchants' existing telephony.

CardEasy also works with any ISDN or SIP provider globally, and with any payment gateway and/or tokenisation service provider.

Agent control integration options include a virtual terminal launched by the merchant's business system (for example, CRM, reservation/booking/sales system); a SOAP API; an iframe embedded in your web application; hosted payment page integrations; and even a 'light-touch' option to avoid integration at all, used for instance with legacy green screens.

CardEasy is a Syntec managed service offering the merchant full PCI DSS de-scoping of their contact centre operations. In the case of the hybrid premises-based solution, the merchant is responsible only for the physical security of the appliance. Nearly all other PCI DSS controls relating to the contact centre are taken out of scope, including those relating to agents, network and call recordings, effectively eliminating the cost and hassle of PCI monitoring and audits in this environment altogether.

CardEasy is available and installed internationally. ●

Eckoh: Securing relationships through secure data

The challenge for allpay was to find a replacement supplier for their contact centre PCI DSS requirements in time to meet their original dead-line. CallGuard Hosted and EckohPAY for secure telephone payments met all their objectives and helped retain key client relationships.
By Nick Peplow, Bill Payments Director, allpay

Collecting nearly £7 billion a year from more than 67 million transactions, allpay offers the UK's widest range of payment collection solutions and bill payment services, primarily to the public sector. The company strives to offer clients ways to save money through creating modern payment systems that are both cost effective and very convenient for the end consumer.

Its operations now comprise bill payment, prepaid cards, card manufacturing and bureau facilities, print and design, the businesses 24publishing and Herefordshire Live, as well as an online wine retailer.

Work had begun towards PCI DSS compliance as allpay needed to have a Report on Compliance (ROC) to reassure our customers of our commitment to keeping their data secure. It was also important to our customers that they could offer the end user the most secure method of payment and peace of mind.

However, when allpay approached Eckoh, we had already tried to implement another solution for our contact centre PCI DSS requirement. Regrettably, we later discovered that the supplier could not deliver their commitment using a VoIP solution.

One of the key problems was that the internet signal kept dropping during calls and was proving to be so unreliable that we didn't believe we would ever be able to implement it. We therefore decided that we had to look for a more credible supplier.

Having wasted time on another solution we needed to get it right this time as well as meet our original deadline. We were determined to choose the services of a robust and reliable solution provider so we launched a rigorous and highly detailed Request for Proposal (RFP) which we sent out to four other leading providers of dual tone multi frequency (DTMF) suppression solution providers.

What we wanted to achieve was…

- To be able to offer our customers the ability to make repeat payments using an automated phone system at any time of day.
- To have a solution that could be resold to our clients to help them achieve PCI DSS compliance.
- To allow our customer service agents to take payments over the phone without any break in the customer conversation
- To allow our clients to collect payment from their debtors 24/7 using a Self Service Pay Interactive Voice Response (IVR) which was PCI DSS compliant
- To implement the solution within nine weeks of contract signature
- To have a solution that guarantees high availability with no downtime as clients make payments 24/7/365.

We have many clients, some of which we have held for some years. Some of these relationships were potentially at risk if we couldn't demonstrate our compliance to PCI DSS. At the same time, as many of our customers are housing associations they also needed to achieve PCI DSS compliance to be able to take secure payments from residents. In addition to this, as a payments solution provider, we wanted to ensure that risks to data exposure were reduced – significantly. We fully understood the risk to our reputation and the terrible damage that a data breach could cause.

Eckoh's solutions

Integration solution for syndication/ resale to our existing client base
We requested that Eckoh deliver an integrated product that would enable them to syndicate the solution across their client base. As allpay's clients are mostly housing associations, budgets are often tight and through this syndication allpay can help them to achieve PCI DSS compliance at a reduced cost as well as protecting their customers' data. Eckoh could provide this due to the simplicity of the solution, which is not something that alternative suppliers can achieve.

Automated payments in a PCI DSS compliant manner: EckohPAY
EckohPAY is the flagship automated phone payment system for Eckoh. Hosted on Eckoh's PCI DSS Level 1 compliant platform, it keeps all payment data outside allpay's networks and systems. When the customer calls and wants to make a payment, the system identifies them with a personal reference number, linked to their customer billing information on allpay's system.

EckohPAY then uses various IVR prompts to guide the caller through the payment process enabling them to pay any amount they choose.

Agent assisted payments in a PCI DSS compliant manner: CallGuard Hosted
CallGuard is available in several options to suit an organisation's preferences. allpay chose the CallGuard Hosted solution that

removes the entire contact centre (agents, call recordings, telephony, networks and systems) from the scope of PCI DSS. The service enables allpay's agents to remain on the phone with the caller and guide them through the payment process.

When a caller types their card details into their handset, the DTMF tones are intercepted by CallGuard and replaced with monotones, allowing call recording to continue with no implications for PCI DSS. As only masked card numbers are shown on the agent's CallGuard web panel, they can assist the customer in the event of any difficulty. Numeric data isn't seen, heard, transcribed or recorded. Also, agents can stay on the phone with customers throughout each call.

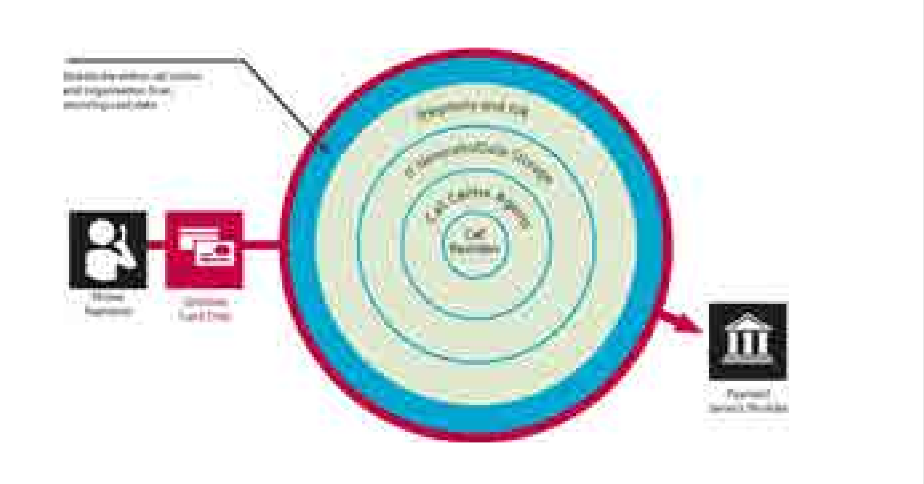
The advantage of delivering both solutions is that if a client falls out of the self service IVR an agent can take a payment.

Why CallGuard Hosted & EckohPAY are the best option on the market for contact centre organisations
allpay's RFP results were heavily weighted in favour of Eckoh's CallGuard Hosted and EckohPAY solutions because they showed Eckoh's solutions to have system resiliency and professionalism. The company had also received excellent feedback from existing customers.

Tony Porter, Head of Global Marketing at Eckoh, says: "Many times over we've been contacted by businesses who have tried to implement alternative solutions but have been unsuccessful. It would seem that these alternatives promise much but deliver little because they are often just too complicated to make work or they require too much integration which can disrupt existing systems and create further problems. The beauty of Eckoh's solution is its simplicity and we're always glad to help anyone trying to achieve PCI DSS compliance."

How does CallGuard Hosted work?
CallGuard completely de-scopes allpay's contact centre.

All incoming calls to allpay's contact centre come through Eckoh's secure platform. When the agent needs to take a payment, the agent's phone and web sessions are linked to a CallGuard ID.



This ID is displayed on the agent's CallGuard web panel and the agent then enters the ID into their phone keypad. Alternatively, the ID can be played down the phone as audio and then the agent types the ID into the CallGuard web panel.

CallGuard allows the caller to remain on the phone with allpay's contact centre agent, who will guide them through the payment process, assist in the event of any difficulty and complete any final tasks.

When a payment is required, the agent asks the caller to enter the details using their telephone keypad, which will generate DTMF tones. CallGuard recognises these as sensitive information and replaces them with flat tones.

Call recording continues as normal. The agent receives visual process indicators on their web panel and remains on the line with the caller, guiding throughout the entire process, and correcting any errors if necessary.

Once the card details are captured, CallGuard processes the payment directly with the payment services provider and returns the transaction information needed, such as Transaction ID, Auth-code and Token.

CallGuard ensures that while cardholder data remains isolated from the contact centre environment, the agent and caller can continue dialogue, providing a seamless customer experience.

How does EckohPAY work?
EckohPAY offers allpay the ability to take secure, automated payments 24/7/365 securing those payments over phone, web, SMS or via a smartphone.

Telephone payments: callers are greeted and guided through the automated service by a professionally recorded voiceover and script. They can choose to interact with the service using speech recognition or touch tone.

Meeting allpay's objectives
Since the solution's launch in September 2016, allpay has taken over 639,171 payments from customers and syndicated its implementation in their contact centre and two housing associations.

"We wanted a secure payment method that would adequately protect our customers' card data when they paid over the phone. We chose Eckoh because of its credentials and references. We have been extremely impressed with the robustness of CallGuard and EckohPAY, and the speed of implementation. It's ticked all

> **"Eckoh was the only business to use its own technology in-house within its own contact centre to process payments on behalf of its clients. This was a clear differentiator for us and we believe CallGuard will be a great answer to many of our clients' PCI challenges. We're extremely excited to share Eckoh's technology and expect a very positive response."**
>
> *Nick Peplow, Bill Payment Director, allpay*

the boxes for us, and for our PCI DSS requirements," says Nick Peplow, Bill Payments Director, allpay.

How Eckoh's solution met allpay's objectives
Eckoh had to meet allpay's very specific goals. With careful and swift project management, we achieved each one using the technology described here.

Goal 1. Remove the entire allpay contact centre environment from the scope of PCI DSS
To allow allpay to complete PCI DSS SAQ A (the compliance checklist in which all payments are outsourced to a third party), Eckoh provided the fully hosted version of CallGuard. This means all of allpay's payment calls are routed through our secure hosted data and telephony platforms and can accommodate allpay's multiple sites and clients: mission accomplished.

Goal 2. Enable any agent, at any time, to handle card payments in a PCI DSS compliant manner.
Any agent can now take payments without being exposed to 'real' card data (just tokens), either visually or audibly at any of allpay's sites, or even working from home. What's more, with the automated, self-service EckohPAY solution, customers can now make payments at any time of day.

Goal 3. Solution should be able to be syndicated/resold across allpay's client base
Because of the simplicity of Eckoh's solution, it was able to be lightly integrated into allpay's 'CallPay' system. This meant that Eckoh's solution could be rolled out to allpay's client base – reducing the cost and ensuring it was delivered in two to three weeks.

Goal 4. Ensure contact centre workflow isn't altered or agent average handling time increased
The great thing about the new system is that there is 100% agent/customer interaction throughout the call and 100% of calls are recorded without any sensitive cardholder data being transmitted. At no moment in the conversation is the customer put on hold or passed to an IVR to take payment. This provides a much better and quicker service for customers.

Our Customer Services department were enthusiastic about the new system but were a little concerned that the new process may increase agent handling time. They weren't sure how the customers would adapt from speaking their card information to keying it in.

Fortunately, their fears were unfounded. The department started reporting a significant reduction in average handling time since the full deployment of the hosted solution.

"Eckoh was the only business to use its own technology in-house within its own contact centre to process payments on behalf of its clients. This was a clear differentiator for us and we believe CallGuard will be a great answer to many of our clients' PCI challenges. We're extremely excited to share Eckoh's technology and expect a very positive response," says Peplow.

Goal 5. Implement the solution within nine weeks of contract signature while meeting allpay's budget and resource limits
The system had to go live by September 2016 which gave Eckoh a challenging time frame of just nine weeks from contract signature to go-live.

Benefits to allpay
Eckoh provided a solution that completely met allpay's requirements and original deadline. Despite losing time to their original supplier, Eckoh implemented the new system quickly and without delay.

Not only is allpay itself taking payments from customers directly, but the company was so impressed with how CallGuard Hosted works that it has entered into a reseller agreement with Eckoh to offer it to their customer base as an additional service.

Payment security is a consistent hot topic with housing associations and local authorities, and allpay can provide them with the same reassurance and trust that allpay receive from Eckoh's technology.

The main benefits that allpay are experiencing with Eckoh's solution are:

- Speed of implementation
- Robustness of the system
- Ease of use for both agents and customers
- Full contact centre de-scoping for PCI DSS requirements
- Peace of mind for themselves and their customers.

Eckoh's CallGuard Hosted solution in particular provides a wealth of real accountable cost and time saving benefits. The speed of integration, flexibility and 'light layering' nature of the solution is where this solution sets itself above competitors.

Why Eckoh should win
Eckoh's solution has once again solved more than just the client's immediate requirements. It delivers well beyond the scope of the contact centre, providing security, peace of mind and reassurance to the immediate customer and the end user.

The important distinction for Eckoh and allpay is the ease with which Eckoh's solution has been packaged to provide a product that allpay can syndicate across its client base to embed cardholder data security into its operations. This has not been possible with other solutions due to their complex design and implementation.

Making things vanish has been a magician's trick for centuries. Now Eckoh has made it happen with sensitive card data – instantly removing a compliance challenge that otherwise threatens to unseat today's contact centres. With a valueless token in its place, there's nothing for thieves to steal, providing unrivalled security that protects sensitive data and business reputation.

With the problem solved, allpay is able to focus on its core business: winning new business, securing its customers' and end consumers' payments – amounting to tens of thousands of customers – and providing new levels of confidence and peace of mind for everyone.

ECSC: The importance of customisation – building a tailored PCI DSS network

Rail franchises, like many organisations, have their own organisational and contract idiosyncrasies. So in PCI DSS, one size does not fit all. ECSC's solution fixed significant vulnerabilities and compliance issues without disrupting the client's normal working arrangements.

The Payment Card Industry Data Security Standard (PCI DSS) is mandated where retail merchants and their third-party service providers store, process or transmit card data. The standard is maintained by the PCI Security Standards Council, set up by the card brands Visa, Mastercard, American Express, JCB and Discover.

For larger organisations, compliance with the PCI DSS is assessed annually by external PCI Qualified Security Assessors (QSAs).

Each retailer has a Merchant Agreement with the bank that processes their payments, and this agreement includes liability for fines in the event of a breach. These fines can quickly run into millions of pounds for large volumes of card data compromised.

The standard contains many technical and process requirements. For most organisations, the best strategy is to segment payment systems to reduce the scope of their compliance obligations. This separation and isolation of payment systems also helps to reduce the number of third parties that might otherwise have to be included in the scope of compliance to the standard.

Where third-party service providers are left either storing, processing or transmitting card data, or they have network access into the card processing environment, they must also be fully compliant with the standard. This is demonstrated by either being pre-certified as a PCI Level 1 Service Provider, or by being included in the merchant's annual assessment.

Client Challenge

For a rail franchise, card payments usually come through one of four routes:

- Online ticket sales
- Automated station ticket machines
- Station ticket counters
- On-train ticket and refreshment sales

The ECSC client had outsourced its online sales to a certified provider, but this still left the remaining payment channels, each of which needed to communicate across the rail company's IT network, including multiple stations.

Unfortunately, investigation by ECSC QSAs showed that there were significant instances of PCI DSS non-compliance within the payment card systems and significant security vulnerabilities. As these were supplied as part of long-standing, third-party management contracts, the ability to make these compliant and secure was going to be difficult and time-consuming, leaving a significant risk of a serious breach.

The UK rail model requires each rail franchise to be run as a separate entity that can be handed over to the next franchise owner. This means that most IT departments are limited in size and security expertise, and don't have the staff to meet the 24/7/365 security monitoring requirements of the PCI DSS.

ECSC Solution

As QSAs, ECSC could understand the technical challenges and detailed requirements of the PCI DSS. Furthermore, as a PCI Level 1 Service Provider, ECSC could build and manage a technical solution.

> **"The ECSC approach is collaborative rather than the more dictatorial style some other QSA providers use in the long term. This gives a better, more robust PCI framebook which is adaptive to change and provides a base from which to deliver a secure environment across a range of deliverables, not just payment card security."**
>
> *PCI Compliance Manager (ISA), Rail Franchise*

This solution involved managing perimeter security devices, including firewalls, an Intrusion Detection System (IDS), and log collection, together with network switch management.

Each device was built and fully documented to the PCI DSS requirements, and ongoing management processes aligned to the standard. This allowed the client to increase their overall compliance level, prevent a serious data breach, and demonstrate compliance progress to their bank.

Each component was then monitored and managed by ECSC's global 24/7/365 security operations centres (SOCs). These currently operate from the UK and Australia, giving 'follow the sun' support.

Key Benefits

- Non-compliant insecure payment systems isolated and protected
- 24/7/365 SOC monitoring and incident response
- System designed by PCI QSAs
- Delivered and managed by a PCI Level 1 Certified Service Provider ●

Mastercard Payment Gateway Services: secure, scalable, future-proof

Securing the payment data that enables commuters to benefit from the latest in ticketing and payments technology is a challenge. Mastercard Payment Gateway Services' P2PE encryption solution helps Scheidt & Bachmann to run its business today and future-proof it for tomorrow.

Background

With over 3,000 employees from nearly 50 countries worldwide and decades of experience, Scheidt & Bachmann are a truly unique, family-owned company, providing innovative mobility solutions such as parking, signalling, petrol station and fare collection systems to thousands of businesses around the globe. In a world where it is no longer sufficient to provide barriers and machines, Scheidt & Bachmann's success lies in the intelligence and breadth of their technology and the highest quality of service.

Mastercard Payment Gateway Services has a long-standing partnership with Scheidt & Bachmann, providing secure payment solutions specifically designed for their train and transit operators in the UK and Ireland.

Business challenge

Having come a long way, evolving from a mechanical engineering company established in 1872 into a leading global systems provider, Scheidt & Bachmann perfectly combines tradition and innovation. With that in mind, the company was determined to team up with a well-known and trusted payments provider, capable of enhancing consumer experience, ensuring the highest level of security and utilising the latest technology and payment innovations.

Overall, the requirements were simple and clear:

- A highly secure and scalable payment processing platform for unattended ticket machines, including omni-channel tokenisation to support tickets purchased online and collected at self-service terminals at train stations
- Fast, reliable and fully managed Point-to-Point Encryption (P2PE) solution to securely remove sensitive payment data from merchants' systems and reduce the cost associated with PCI compliance, whilst providing the best-in-class integration to existing ticket machines and offering flexibility to both operators and consumers
- Integration of innovative solutions, like Apple Pay and contactless
- Quick and efficient implementation across multiple UK locations

By working collaboratively with our client's IT and business divisions, Mastercard Payment Gateway Services was able to meet those requirements and offer a unique solution that not only addressed the customer's existing challenges but also helped to future-proof their business.

Solution

By working collaboratively with our client's IT and business divisions, Mastercard Payment Gateway Services was able to meet those requirements and offer a unique solution that not only addressed the customer's existing challenges but also helped to future-proof their business.

Our PCI-certified P2PE technology encrypts sensitive cardholder data at the point of in-store card acceptance, thus rendering the data useless if it fell into the hands of a cyber-criminal. Once encrypted, cardholder data remains encrypted until it reaches our omni-channel payment gateway environment, where it is decrypted for onward bank processing.

The solution is designed to reduce the burden of PCI DSS compliance, remove sensitive cardholder data from the merchant's in-store environment and reduce operational and compliance costs.

The P2PE standard is comprised of six domains:

- Encryption Device Management
- Application Security
- Merchant Encryption Environment
- Segmentation between Encryption and Decryption Environments
- Decryption Environment
- P2PE Key Management Operations

Mastercard Payment Gateway Services has elected to validate against the requirements of the PCI DSS P2PE hardware/hardware specification and utilise hardware-based encryption and decryption. This means that secure cryptographic devices are employed for both encryption and decryption.

Additionally, our industry-leading tokenisation solution, which converts sensitive card data into secure omni-channel tokens, allows merchants to provide an enhanced consumer experience across different channels, by facilitating the increasingly popular Click & Collect model. That removes the need to store the card data within the merchant's environment and further reduces their PCI scope.

To make the payment journey even more convenient, consumers who make their purchases at physical locations/train stations, as opposed to online, can benefit from the speed and efficiency of the contactless technology,

using either their card or mobile phone/smart watch to complete the payment with a simple tap.

Implementation and results

Each stage of the implementation was carefully planned and executed, ensuring that the following phase of the project was being prepared to go live at the same time. Our teams worked with the client to agree specific criteria to not only outline what the pilot would include, where it would be completed, and how long it would last, but also to clearly identify at the end of this timeframe whether the pilot had been successful.

The full P2PE encrypted traffic went live during the summer of 2017 and currently includes the following services:

- Processing authorisations, settlement and Point-To-Point Encryption
- Deployment of Verifone's UX series unattended PIN pad devices into customer locations for readiness of P2PE rollout
- Using Scheidt & Bachmann's in-house developed payment client application, operating on Verifone's UX series devices and consuming our gateway on a "host to host" basis, ensuring consistency and the highest quality of service
- Implementing contactless technology into most transit operations and seeing significant uplift in contactless transactions – with approximately 20% to 25% of card payments currently being made via a contactless enabled device
- Supporting cardholder present transactions to over 75% of all the UK and Ireland's major transit operation companies
- Processing more than 50 million transactions per annum, a significant rise from 2016

Throughout the partnership, we have continuously expanded our services for additional client projects:

- Maintaining a highly flexible contract, with continuously evolving requirements to ensure all of the latest industry standards and consumer demands are met
- Supporting Scheidt & Bachmann's customers through numerous mandate changes, including the mandate to support contactless payments in an unattended environment

With our specialist Acquirer Certification team, we worked proactively to ensure that we remain ahead of these mandated requirements, and we were one of the first payment system providers to gain contactless approval with the acquiring banks.

Summary

Mastercard Payment Gateway Services' unique technology combined with Scheidt & Bachmann's unrivalled systems enabled merchants to benefit from a secure omni-channel payment solution, which proved to deliver exceptional results, whilst utilising the latest innovations and significantly reducing the PCI scope. ●

Pay360: Delivering PCI DSS compliance – ERYC's 3.2 journey

When East Riding of Yorkshire Council looked at what it would need to comply with the Payment Card Industry Data Security Standard (PCI DSS) 3.2, it realised it needed help. In Pay360 by Capita the Council found a suite of solutions that has improved services, saved them £1 million and ensured full PCI compliance.

Councils cannot risk public funds. That was the position of East Riding of Yorkshire Council (ERYC) in April/May 2016 when the future requirements of PCI DSS 3.2 were published by the Payment Card Industry Security Standards Council (PCI SSC), giving notice that 3.2 would become 'the standard' on 1st Feb 2018.

As ERYC was an existing customer of Pay360 by Capita, James Hewson, the account manager responsible for the ERYC account, was on hand to support. Hewsons' challenge was to ensure ERYC achieved the right balance between customer experience and cost, whilst at the same time meeting the overall requirements of PCI DSS 3.2 and delivering business-as-usual.

PCI DSS first appeared on ERYC's radar at one of the Pay360 annual user group meetings, over five years ago. It became apparent that PCI was beginning to take centre stage in the security segments.

"At that point, we knew very little about PCI, other than it was assumed that it was automatically adhered to by IT. Additionally, our merchant bank began its own phased programme of mandating compliance, which complemented the information triggered by the user group meetings," explains Patrick Woodhead, ERYC Senior Technical Officer.

"Having become aware of what PCI was and the implications for non-compliance, it was quickly realised that not meeting PCI requirements was a substantial financial risk to the Council. Furthermore, not only would a breach be extremely costly to tax-payers' funds, it would inflict terrible damage on the Council's reputation. Our customers expect us to protect their data. Losing that confidence and trust was unthinkable."

Having realised that PCI compliance was a significant business risk, ERYC established a working group to assess its situation and compliance status. At that time, version 3.2 of the PCI DSS code was in the pipeline but not yet launched. The working group consisted of representatives from IT, Finance and general business administration.

Significant work needed for 3.2

The investigation confirmed that while existing measures for PCI DSS compliance were sufficient, for version 3.2, it was

> **"As part of our preliminary investigations we had realised that typing card numbers into a keyboard to enable telephone payments would require a full separation of the network, since telephone payments via Pay360 Paye.net were taken across the whole authority."**
>
> *Patrick Woodhead, ERYC Senior Technical Officer*

apparent that significant new work was needed, in particular on the non-IT control and monitoring mechanisms that 3.2 imposed, but also with the much more rigorous demands of full point-to-point encryption that were on the horizon.

There were also concerns about full network segmentation, a key feature of version 3.2. Geographically the authority covers a large area with diverse operations, each taking card payments through a variety of methods.

Version 3.2 of the PCI standard raised the bar considerably. ERYC engaged a Qualified Security Assessor (QSA) and asked them to conduct a full PCI assessment to the relevant SAQ standards that version 3.2 was about to impose.

Says ERYC's Woodhead: "They confirmed that all our chip and pin devices needed to incorporate full P2PE (point-to-point-encryption). We had a multitude of different devices at various stages of their product life cycle, some better than others (some worse!) but all, apart from a handful, that would fail under version 3.2 of the standard. Not addressing the chip and pin problem was not an option.

The QSA report also provided a highly useful insight into our telephone card payments. As part of our preliminary investigations, we had realised that typing card numbers into a keyboard to enable telephone payments would require a full separation of the network, since telephone payments via Pay360 Paye.net were taken across the whole authority. This brought the entire network into scope. And whilst a full segmentation was possible, the cost (at over £1 million) was prohibitive."

At this juncture, the QSA report was invaluable. It recommended that, instead of trying to segment the whole network, since all of it was in scope due to telephone-based payments, the telephone payments be taken off the network completely.

Various options were explored thoroughly, including a dedicated and network-isolated telephone payments team, contracting-out the telephone payments to a third service provider, and implementing mini-segmentation by only allowing certain staff members in each office to take phone payments.

However, the best option that emerged was Pay360's CallSecure product. CallSecure allowed ERYC to lift telephone payments off the network. At a stroke, this solved the complex and thorny issue of network segmentation. CallSecure allows the Council to handle a telephone call by regular staff as normal.

Phone payments are usually, but not exclusively, a result of the call itself; booking a service – querying and then paying a bill for example. The payment portion of the call is the final action. At that point, the member of staff transfers the customer to Pay360's CallSecure function where payment is taken.

None of the card data traverses the Council's network; none of the Council's servers or other IT architecture is utilised; Pay360's own PCI-approved and certified IT infrastructure handles the card payment on the Council's behalf, whilst still allowing the full access by customers to the Council's staff and services. Minimal changes to working practice were required, the biggest being a slight amendment to the call handling procedure to ensure that all areas of the call had been dealt with prior to transferring the customer to CallSecure to make the payment.

Operational and implementation challenges

The Council uses Paye.net to process payments for a multitude of services. These range from 'standard' payments such as Council Tax and housing rents to more complex service requests that require payment to have been made prior to the service being delivered.

ERYC currently has over 400 Paye.net users, the majority of whom take payment over the telephone. There are approximately 30 users who offer a face-to-face payment facility utilising Pay360 supplied chip and pin devices.

"We have deployed Paye.net since 2002. Paye.net was the obvious choice as it enables our service delivering departments to take payment at the point of order. This reduces costs as it removes the need to raise an invoice, improves cash flow and allows service managers to better monitor income. Paye.net is also used to help drive down arrears by allowing departments to take payments whilst they have customers engaged on the phone – i.e. no more 'The cheque's in the post'," says Lee Parker, Collection and Transactional Team Leader, ERYC.

Easy to implement?

CallSecure has been very simple to roll out. The ability to 'switch' existing Paye.net users instantly either individually or by department has allowed the Council to implement a phased roll-out whilst not suffering any loss of payment processing facilities.

Existing users have transferred seamlessly to the CallSecure option. This is due to the fact they retain their existing user details and the only alteration to their previous practice is to select a different method of payment. Once this has been highlighted the work process is smooth and transparent.

The benefits of CallSecure

The major benefit of using CallSecure is that it takes the call taker, and all the infrastructure that supports them, out of PCI scope. This is due to the fact that the user no longer has access to the customer's card details, which are handled by Pay360's secure data centre. The Council investigated an option of segmenting the network for each user but this was discounted due to cost. It was estimated that it would cost approximately £1 million to segment the network completely for its 400 users.

With this cost in mind, CallSecure was the obvious option to allow PCI compliance and allow the Council's departments to continue offering payment services. Reduction of these services was not an option. "CallSecure has also delivered reductions in call handling times allowing call centre staff to move on to the next customer more quickly," says Lee.

ERYC is continuing to roll CallSecure out on a department by department basis.

Supporting ERYC's transition to the Cloud

ERYC have been using Pay360's Income Management product suite including AIM, ACR & Paye.net for over 15 years. Two options were considered when they upgraded from v8 to v9. These were to remain 'on-site' using Council-supplied servers or move to the hosted Pay360 Cloud solution.

After a costing exercise it became apparent that savings could be achieved by moving to the Cloud. By having the system hosted by Pay360, the Council bypassed the need to purchase a new server as well the inherent costs of keeping the server secure and up to date.

Cloud also promised to make any upgrade of the product suite far simpler, requiring very little in the way of input from ERYC's own IT department.

Who are Pay360

Pay360 are the specialist payments business within Capita plc. Our aim is to offer one payment system and service that does everything you'll ever need it to do, irrespective of the complexity, size and scale of your business operations and transactions. To give you an idea of scale, we support over 6,000 merchants offering 40 plus technology products that deliver over 225 million card payments annually with a value of over £9.5 billion. As well as card payments, we manage or support an additional £40 billion per annum of 'other' payment types including cash, cheque and direct debit. Pay360's focus and reach extends to both the public and private sectors.

"The transfer to Cloud was a smooth transition. We had expert help in the shape of a dedicated project manager and an engineer who both understood the requirements of the Council and was on hand to investigate and resolve any issues we had. This support continued through testing and implementation in the live environment, ensuring we had minimum downtime on the day of transfer," says Parker.

The major benefit to moving to the Cloud is that Pay360 is now responsible for maintaining both the software and the hardware. This cuts out having to decide whether issues are the responsibility of ERYC's own IT department or a Pay360 issue. Any issues are now reported to the Pay360 helpdesk and resolved quickly.

ERYC's PCI DSS challenges solved

Says Parker, "Through Pay360's Paye.net and CallSecure solutions we have been processing on average 5,000 payments a month via our call centre with an average value of £170. Introducing this system has saved us £1 million and given us the peace of mind that we are fully PCI DSS compliant.

The main deliverables to us operationally have been:

- Fully integrated to our existing call centre front end
- Reduced operators' time on the call by up to 50%, freeing us up to answer calls more quickly
- Removed all telephone payments infrastructure from PCI scope
- Reduced ERYC's risk significantly and reduced the security burden on our teams by having no spoken payment card data in our call centres
- Provided us with flexibility and options around our customer journey, returning a customer to the original agent, telephone hunt group or any nominated extension

More to come in 2018

Pay360 is not resting on its laurels. As Stephen Ferry, Managing Director, Pay360 by Capita, explains: "Historically Pay360 has focused on technology development and payment services delivery, and as you can see from Lee and Patrick's responses, there's still plenty of scope for our well-established solution sets to deliver cost savings for ERYC. However, when I joined the business at the end of last year, I believed that was not enough and our teams have been working hard during 2017 to make us better.

That has resulted in us developing two new offerings to support our merchant and acquirer communities. We identified the need for larger merchants (Levels 1, 2 and 3) to have more insight into their payments risk, to have the ability to exert greater control over the risks they took, and from that, to increase the conversion rate between customer contact and successful payment outcomes, and deliver that across all their customer communication channels. We describe that as our 'Optimise' offering.

More specific to PCI DSS compliance is our second new offering that we plan to formally launch in January 2018, that is Pay360's 'Secure'."

'Secure' arises from work with the PCI SSC and from analysis of the market.

Says Ferry, "We know too well that merchants today want to 'get more with less', so building the business case for additional spend is not an easy one. We also recognise that helping merchants understand how to get the right balance between people, process and technology, so that payments compliance does not impact needlessly on business-as-usual, is not an easy task either.

"Pay360's CallSecure has delivered reductions in call handling times, allowing staff to move on to the next customer more quickly."

Lee Parker, ERYC Collection and Transactional Team Leader

"We fully support the PCI Security Council's mantra of 'getting risk off the table' and 'devaluing data' and at the same time, Pay360 is committed to helping our merchants by fully supporting our acquirer community's recent acceptance that all merchants of Level 3 and above can now certify PCI DSS compliance on a channel by channel basis. That means Pay360 is aligned with our 250-plus acquirers and the PCI Standards Council to help reduce merchant risk, and reduce the merchants' burden of compliance.

"However, keeping PCI DSS on the merchant agenda has not been easy for us this year as the merchant community works to cope with the requirements of GDPR, and we recognise those struggles won't go away during 2018 or even 2019.

"So, putting merchants in a position where they can de-risk their journey through GDPR and PCI DSS, as well as take full advantage of 3D Secure 2 and the Payment Services Directive (PSD) 2, by providing them with the right guidance and tools to do the job, that's what our 'Secure' offering is going to be all about in 2018." ●

PCI Pal: Providing AllSaints with a joined-up, compliant payment solution

AllSaints is a global fashion brand based in East London, which operates in twenty-seven countries, with over two hundred stores globally. Since implementing PCI Pal's solution, the company has seen a two-thirds reduction in how long it takes to process a phone sale.

The compliance challenge

The AllSaints customer experience team were facing a number of problems in creating a seamless customer journey. Realising that the payment journey was time-consuming for both agent and customer, AllSaints needed to join up their various systems and provide a payment solution that would be smooth and painless for both parties.

AllSaints' customers are typically quite tech savvy, so the company needed a convenient secure payment solution that would make customers feel at ease and secure when ordering on the phone.

As Sarah-Jayne Grabiec, Global Head of Customer Experience and Brand Protection at AllSaints, explains: "We are a 24/7/365 customer contact centre and also a brand protection team. We have an extremely international clientele – we speak 15 languages – and we needed a solution that made them feel comfortable and confident calling us and placing phone orders. We are a global digital business operating on a number of different platforms. We wanted to make sure that we ticked all the boxes in terms of legislation."

How PCI Pal solved the problem

PCI Pal offers a series of Level 1 PCI DSS certified solutions built around clients' contact centres and processes. The aim is to introduce compliant and secure payments solutions that are customisable, scalable and reliable, with 24/7 global support and 99.999% uptime. PCI Pal is compliant, and will remain compliant, with the latest versions of the Payment Card Industry Data Security Standard.

The Agent Assist solution replaces the traditional payment process, in which a contact centre agent asks a customer to read out their credit card details. Instead they ask that they enter them on their telephone keypad. PCI Pal's secure Cloud captures the tones entered, masks them with a monotone beep and displays asterisks on the agent's screen. Crucially, the voice path between the customer and agent remains open, so they can communicate should there be a problem.

PCI Pal's deployment models do not require any kind of integration with existing telephony providers. And integration with payment providers is straightforward as the majority of payment providers now have modern APIs that allow easy integration with secure Cloud services. Payments made via PCI Pal are processed by the provider at the same speed as (or quicker than) using their virtual terminals directly.

Says Grabiec: "PCI Pal advised us on a best practice solution for a PCI compliant payment system and on how to protect our customers' details for all of our contacts within our existing customer experience. The only difficulties we faced were probably at our end and not PCI Pal's. We worked in partnership with them to iron those out and they delivered on time and within budget."

The result

Since implementing a PCI Pal solution, AllSaints have seen a two-thirds reduction in how long it takes to process a phone sale, which means they can handle more calls and take better care of their customers.

"We certainly put it to the test over our busy Black Friday and Christmas peak period," says Grabiec.

And, importantly, the solution is able to grow and adapt with the business. "PCI Pal are also very good at working with us whenever we make any internal changes within the business. Having PCI Pal on board has enabled us to allow our customers to shop with confidence, knowing that their details are secure, that they could call us at any time if they had difficulty placing an order online or if they just wanted one of our personal stylists to support them in a transaction.

> **"Here at AllSaints we would certainly recommend PCI Pal. Not only are they digital and safe and secure but they are also very forward thinking so great for any retail e-commerce business,"**
>
> *Sarah-Jayne Grabiec, Global Head of Customer Experience and Brand Protection at AllSaints*

They understand we are a 24/7 business and they're very proactive. So often they contact us first if they anticipate any bumps in the road and should we have a problem they are easy to get hold of. They provide a root-cause analysis and then assure us for business going forward. They don't expect us to adapt to their business but they go out of their way to adapt and evolve with us."

Customers can now shop with confidence, safe in the knowledge that their cardholder data and personal details are secure. An improved telephone order system also means customers can call the AllSaints team at any time if they're having difficulty placing an online order, or if they'd simply like agent support with a transaction.

"The PCI Pal team are very proactive and easy to get hold of. They've always gone out of their way to adapt their solutions as our business needs have evolved. We would certainly recommend PCI Pal, as not only are they digital, safe and secure, but they're also very forward-thinking, which is great for any retail e-commerce business," says Heather Gibson, Brand Experience Director, AllSaints. ●

SecurityMetrics: When PCI DSS is mission-critical

If you provide PCI P2PE certified solutions to merchants who want your help in reducing their PCI DSS scope and maintaining PCI compliance, then your own compliance credentials must be second to none. For IPS this meant using SecurityMetrics.

IPS was founded in 2013 to help merchants accept payments across multiple countries, in multiple currencies, through a single platform. The company offers a comprehensive service that bundles terminals, POS software, payment gateway and professional services to enable its customers to accept, secure and process payments. Its mission is to make securing payments simple for its customers.

> **"Because PCI is always changing and P2PE is so new, education of all parties has been crucial."**
>
> *Delia Pedersoli, Sales Director, IPS*

IPS provides an omni-channel payment service to international merchants, enabling them to interact with their consumers to accept and process payments across multiple channels, in multiple currencies and countries, in a safe and secure way.

The company enables merchants to dramatically reduce the cost and scope of achieving PCI DSS compliance through the use of its PCI P2PE certified solution. Merchants also benefit from a significant cost reduction in achieving and, very importantly, maintaining PCI DSS – a cost reduction that is achieved through centralisation, standardisation, and simplification of the merchant's complete payment landscape.

Clearly then, as specialists in domestic and international PCI and P2PE accredited payment solutions, International Payment Services (IPS) takes their security and compliance very seriously.

Challenges IPS faced with PCI compliance

In the past, IPS has had problems with various third-parties in the pursuit of its compliance needs. Says Delia Pedersoli, Sales Director, IPS: "We have had a number of issues working with our hardware manufacturers, Key Injection Facilities (KIF), the Point Implementation Manual (POI), and P2PE apps. We were unsure of the challenges of validating a P2PE solution, as it was not only our first time, but it was also so new in the industry. And we did not know where to start developing policies and procedures for our P2PE solution."

Resolving challenges with SecurityMetrics

Companies face many challenges in PCI compliance, particularly in their choice of vendor and/or QSA. QSAs can establish schedules/timelines, which they fail to meet, resulting in clients missing key compliance deadlines.

Project managers can fail to communicate exactly what is required of the client, create audit schedules they do not follow, and fail to meet commitments to help clients maintain PCI compliance over the year.

It is critical for clients that their solution providers clearly communicate schedules, where clients are in the process, what is needed from the client to keep progressing, and expectations of when each task would be completed.

And clearly clients need a thorough assessment from a QSA with an in-depth understanding of PCI scope, requirements, compensating controls, and security in general.

SecurityMetrics combines this expertise with the knowledge that clients have goals and deadlines and their QSAs make themselves available to answer questions. Clients cite this as a key reason to select them for audits.

The QSA team realises the importance of helping clients understand the requirements of the standards, develop policies and procedures for staff, and work with the PCI Council to get their solution listed.

> **"As a leading provider of payment card data security, we at SecurityMetrics strive to help organisations comply with financial mandates such as the Payment Card Industry Data Security Standard (PCI DSS)."**
>
> *Chase Palmer, CISSP, Senior Program Manager at SecurityMetrics*

As Pedersoli explains: "Because PCI is always changing and P2PE is so new, education of all parties has been crucial. The SecurityMetrics team has been very helpful in this regard. SecurityMetrics employees volunteer to help us through conversations with potential customers and presentations at conferences to explain how our P2PE solution reduces overall PCI scope."

Goals achieved

Pedersoli has partnered with SecurityMetrics for two PCI audits and two P2PE audits, and previously for six PCI and two P2PE audits at European Payment Services (EPS). The following goals have been achieved from these audits:

- While at IPS, SecurityMetrics conducted the world's first successful P2PE audit
- The firm successfully listed multiple solutions with the PCI Council
- SecurityMetrics helped IPS understand requirements, process, gaps, and how to resolve issues that were discovered.
- Found a lasting partner and expert in PCI, P2PE, and data security

The four steps to follow to reach PCI compliance

1

Identify Your PCI Scope

To discover your own PCI scope and what must be included for your PCI compliance, you need to identify anything in your organisation that touches cardholder data. Ask yourself, “What devices do we use to store process, or transmit cardholder data?” We have a tool and agents who help you in this process and make identifying your scope a simple task.

2

Complete an SAQ

All merchants are required to complete a Self-Assessment Questionnaire (SAQ) for PCI compliance. Your specific questionnaire is determined based on how you handle payment card data (your PCI scope). Our agents are always standing by ready to assist you with any questions you may have about your SAQ.

3

Achieve a Passing Scan

Merchants that process, store or transmit cardholder data online are required to have external network vulnerability scans performed by an Approved Scanning Vendor (ASV) on their network or domain. Scans should be conducted quarterly and discovered vulnerabilities should be patched immediately. As an ASV, SecurityMetrics is qualified to conduct these scans, provide you with detailed reports on your results, and remedy any issues that are found.

4

Report Your Compliance

Once PCI compliant, merchants are required to report their compliance to their merchant processor. Don’t worry if you feel unsure of how to validate your compliance because SecurityMetrics will do this for you as part of our service.

By following these four steps you can reach PCI compliance for your organisation, and more importantly, you will be creating a secure environment for your customers’ data. SecurityMetrics makes PCI compliance a simple task for any organisation with 24/7-based support at your disposal.

“In addition to all the help they already provide, SecurityMetrics employees volunteer to help us through conversations with potential customers and presentations at conferences to explain how our P2PE solution reduces overall PCI scope. I trust the team at SecurityMetrics as my go-to experts for all things PCI and P2PE,” says Pedersoli. ●

Semafone: Boosts AO's call handling capacity and keeps sensitive customer payment data secure

Achieving PCI DSS compliance can be a challenge for many organisations. The key is choosing the right partners.

About the Organisation

On a mission to become the best electrical retailer in Europe, online electricals retailer AO.com operates at the forefront of online retail innovation.

Offering 4,000 products and serving more than 1.3 million customers, AO has experienced exponential growth since it was first founded in 2000. Today it has become a multi-country business, with operations in 18 locations across three territories – the UK, Germany and the Netherlands.

Committed to giving customers the best shopping experience possible, AO's call centres are of crucial importance to the business. Over 400 call centre agents are on hand at any one time to help online customers with their order placement or delivery queries.

It is a highly dynamic environment in which thousands of incoming calls, live web chats and email queries are all handled simultaneously – and where agents following up with customers can generate up to several thousand outbound calls a day.

The Challenge

The sheer number of calls handled by AO's call centres can jump dramatically during peak retail times like Black Friday, Christmas, long weekends and seasonal sale periods. But AO's legacy ISDN lines were hampering its ability to cope with these demand spikes. And that meant long hold times, abandoned calls and a poor experience for customers.

But that wasn't all. Trust and transparency are at the foundation of everything AO does and it wanted to ensure that expansion of its inbound and outbound call lines wouldn't compromise customer payment security.

With new EU GDPR data protection legislation due to come into effect in May 2018, AO was determined to take every step possible to ensure that customer payments taken over the phone were

> **“Semafone and 360 Solutions went beyond the call of duty to ensure we were able to maintain continuity of service for customers during the implementation phase. Our agents have found the system really easy to use and feedback from customers has been very positive.”**
>
> *Adam Warne, IT Director, AO*

secure. As a trusted customer brand, protecting customer data and minimising any risk that sensitive customer information could be compromised is of paramount importance to AO.

The Solution
To overcome these challenges, AO chose Semafone and 360 Solutions. Implementing Semafone’s solution would ensure that all over-the-phone payments would be PCI DSS compliant, and that customer data would be kept safe. Meanwhile, 360’s SIP trunking solution would provide a much more flexible and resilient inbound phone service.

With Semafone’s payment security software in place, customers are able to input their payment card details directly into their telephone keypad. These numbers are obscured from the call centre using dual tone multi frequency (DTMF) masking. So, while it’s impossible for agents to hear or see a customer’s card details, they are still able to remain in full voice communication with callers to help out with any issues that may arise during the payment process.

Semafone’s patented payment method sends payment card numbers straight to the payment service provider (PSP), completely bypassing AO’s internal contact centre IT infrastructure. Fully scalable, the solution can easily cope with demand peaks to ensure every payment is taken securely.

To ensure customers can always get through and speak to an agent, no matter how many callers are trying to reach the contact centre, 360 Solutions would boost capacity by supplementing AO’s existing channels with 390 additional SIP channels.

Giving AO the capacity to cope with 600 concurrent calls at peak periods by delivering telephone lines over IP using SIP protocols, this meant AO would gain the bandwidth needed to cope with seasonal demand. What’s more, the solution would also give AO the ability to divert calls to back-up locations or mobile phones instantly, and from anywhere, to achieve truly dynamic call loading capabilities during peak periods.

The Implementation
It was imperative the contact centre stayed up and running at all times. So any implementation and testing had to be undertaken out of hours after 10pm.

Throughout the process key stakeholders from Semafone, 360 Solutions and AO worked together seamlessly to oversee the two primary work streams: the ‘voice capture’ project team would undertake the SIP implementation and phone line number migration, while the ‘payment’ team was responsible for building and integrating the new secure payment process into AO’s payment capture screen.

Following the successful go-live, training workshops for AO’s in-house trainers were led by Semafone.

The Benefits
The new secure payment and voice capture systems have delivered multiple benefits:

- PCI DSS compliance for all payments taken over the phone has been achieved – a key business requirement for AO
- Migrating from ISDN to SIP has provided significant benefits including flexibility and scalability
- AO now has the scalability needed to cope with peak times and seasonal demands – ensuring customer service commitments can be maintained at all times
- The flexibility of the combined solution means AO can quickly handle expansion into new markets – agent seats can be added or removed as needed

As Adam Warne, IT Director at AO, concludes: “AO’s contact centres handle thousands of customer interactions daily and these numbers jump dramatically during peak retail periods like Black Friday, Christmas and other seasonal holidays. With the new EU GDPR data protection legislation due to come into effect in May 2018, AO is determined to take every step possible to ensure that customer payments taken over the phone are secure.

“During implementation, Semafone went beyond the call of duty to ensure we were able to maintain continuity of service for customers. Our agents have found Cardprotect really easy to use and feedback from customers has been very positive. Not only are they happier about being able to remain in contact with agents throughout the entire call – they also truly appreciate the additional level of payment security we’ve put in place.” ●

> **“AO’s contact centres handle thousands of customer interactions daily and these numbers jump dramatically during peak retail periods like Black Friday, Christmas and other seasonal holidays. With the new EU GDPR data protection legislation due to come into effect in May 2018, AO is determined to take every step possible to ensure that customer payments taken over the phone are secure.”**
>
> *Adam Warne, IT Director, AO*

Silver Lining: Solving a core business issue

When a highly-regulated FI runs call centre processes that impede business efficiency and cannot meet regulatory requirements, a new solution is required. This was the situation faced by Silver Lining.

Silver Lining have had the pleasure of working with one of the UK's leading insurance brokers. Founded in 1997, the company initially specialised in providing private car insurance policies, but has since expanded its portfolio to cover home, bike and van insurance as well as numerous other products and services.

The business has over two million customers, and takes tens of thousands of calls every year. Thus, it was of vital importance to them that any card payments made during these calls were completely secure and compliant with industry regulations.

> **The solution we offered them was a simple one: a piece of secure hardware, installed on their premises, that would enable customers to enter their card details via their telephone key-pad rather than speaking them aloud.**

A critical process problem

We initially engaged the business to provide them with ISDN lines and a suite of contact centre applications including call routing and reporting. When we broached the subject of PCI DSS compliance, we found their setup to be far from adequate. The company traditionally used pause-and-resume call recording in order to protect sensitive customer card data from being captured and put at risk.

This method of data protection comes with numerous caveats. The company was required to put draconian measures in place to prevent call centre agents from noting down card details. Staff were asked to adhere to a "clear-desk policy", storing items like smartphones, paper and pens, and anything else that could be used to capture card data, in secure lockers. Understandably, this had a marked impact on staff morale, and added unnecessary hassle to proceedings within their call centres.

In addition to this, the Financial Conduct Authority (FCA) requires all calls including transactions to be logged in full, something which pause/resume recording by its very nature is unable to accomplish. As a major insurance provider, the business could not afford to run afoul of the FCA.

The solution we offered them was a simple one: a piece of secure hardware, installed on their premises, that would enable customers to enter their card details via their telephone keypad rather than speaking them aloud. This appliance would then intercept these details so that no sensitive information would be exposed to the call recorder, call centre agent, or the company's internal network.

The initial solution

This innovative technology uses DTMF masking to remove audible key tones from calls, then following validation passes the card data directly to the payment gateway without storing it or exposing it to any other device or capture source.

With this method the call recording need not be paused, ensuring compliance with FCA requirements, and since call centre agents have no access to sensitive card data there is no need for a clear-desk policy. The solution was implemented with minimal disruption, and presented to agents with an intuitive web-based payment portal that was simple to understand and use. As we were already providing their telephone lines, we were able to provide the PCI compliance solution as part of that same service wrap.

The business' CIO explains: "The key consideration here was to go with one supplier who could deliver the entire solution end-to-end. We really wanted one integrated platform that encompassed the whole solution. We needed a solution that reduced PCI compliance directives for credit and debit card voice transactions. Silver Lining delivered and exceeded our needs and expectations in one wrapped solution."

Silver Lining staff engaged with agents to provide training on the new system's functionality over the following days, and remained on call to deal with any potential issues or concerns for a significant period afterwards.

> **Moving forward, the business intends to migrate their remaining ISDN lines to SIP. With BT planning to decommission all ISDN lines in the UK by 2025, this move is inevitable, but it plans to make the switchover sooner rather than later to fully enjoy the benefits and future-proofing of SIP.**

This installation of the PCI appliance took place around three years ago, and since that time they've processed thousands of calls with the peace of mind that their customers' card data is totally secure.

A new challenge

However, within the past six months, the company has faced a new compliance challenge – one which we rose to meet.

The company operates over multiple sites, and it was decided that some of these sites would make the transition from the ISDN lines we originally provisioned, to future-proof SIP (session initiation protocol) trunking. SIP offers numerous benefits in cost saving and mobility, and so this was a natural choice for the business.

The challenge they faced was in hooking up these SIP trunks to their existing PCI appliance, in order to continue making secure transactions on these lines. Fortunately, we have further developed our PCI technology since it was initially provisioned, and we were able to build new infrastructure to seamlessly integrate both ISDN and SIP lines into their appliance with minimal fuss.

Moving forward, the business intends to migrate their remaining ISDN lines to SIP. With BT planning to decommission all ISDN lines in the UK by 2025, this move is inevitable, but it plans to make the switchover sooner rather than later to fully enjoy the benefits and future-proofing of SIP.

Cost-effective Cloud PCI

When their migration is complete, we will be able to further enhance their PCI DSS compliance offering with significant cost savings and ease of auditing with our latest innovation. Tentatively titled "Cloud PCI", our most recent solution is currently nearing the end of development and will be deployed soon.

Ultimately, with this new Cloud based compliance technology, we want to break down the traditionally massive cost barrier to entry, providing an alternative Opex model that businesses of all sizes can benefit from.

This solution moves the data capture and DTMF masking hardware from the customer premises to the Cloud, eliminating the need for investment in on-site hardware and effectively transitioning the cost of compliance from a significant capital outlay to an ongoing Opex pricing model. Secure calls are delivered via SIP trunks into the Cloud-based appliance.

This also further reduces the already small number of auditable controls on the customer site; as we host the physical hardware within our own secure data centres, the task of penetration testing falls not to the customer but to ourselves.

Ultimately, with this new Cloud-based compliance technology, we want to break down the traditionally massive cost barrier to entry, providing an alternative Opex model that businesses of all sizes can benefit from. With huge cost savings and greatly simplified auditing on the customer side, we feel that this technology makes becoming PCI DSS compliant easier than ever. We hope that the support of one of the UK's leading insurance brokers as an early adopter will help our solution to flourish within the marketplace.●

SureCloud: A single source of truth delivers GRC best practice to William Hill

A comprehensive solution tailored to the specific needs of the client not only enabled them to meet their PCI compliance objectives but also their wider compliance goals, by providing unrivalled visibility into regulation-critical data flows.

William Hill plc is a bookmaker based in London, England. With a betting heritage of over 80 years, and a place in the FTSE 250 Index, it is one of the most trusted brands in the betting industry. William Hill's numbers are impressive, representing around 25% of the market throughout the UK and Ireland, and processing an average of one million betting slips each day. William Hill also operates worldwide, employing approximately 16,600 people with main offices in the UK and Gibraltar. William Hill also offers betting by phone and by internet, along with its UK-wide Licensed Betting Offices.

As a result, William Hill collects, stores, processes and transmits large quantities of payment card data in multiple formats, which are subject to the Payment Card Industry Data Security Standard (PCI DSS) compliance framework. This framework must be adhered to across all the company's operations. GRC – governance, risk and compliance – are mission-critical.

The Project – William Hill's Challenge

To ensure compliance with PCI DSS, William Hill sought to replace its manual spreadsheet-based monitoring processes. They wanted to collate and report on compliance with PCI standards in real time, enabling staff to remediate any issues that arose across its operations. The programme's aims included:

- Continual maintenance of William Hill's adherence to strict PCI DSS compliance obligations
- Automated monitoring of current PCI DSS compliance status
- Simplified PCI DSS reporting and auditing processes for enhanced efficiency
- Enhanced visibility of compliance status enabling quicker remediation
- Enabling staff to spend more time addressing issues, and less time on manual reporting

To achieve this, William Hill identified that it required an automated, unified way of monitoring, recording and reporting its compliance status across the business, which would work across all relevant William Hill technology areas.

The Solution – SureCloud Platform

SureCloud PCI Compliance increases the efficiency and effectiveness of PCI DSS programmes by delivering them as business-as-usual activity. As well as reducing the cost and effort of achieving and maintaining PCI compliance, it also supports the recommendations set out in PCI DSS 3.2, resulting in faster certification, reduced audit costs, reduced risk, and remediation recommendations focused on areas of greatest risk and retained compliance status. The SureCloud Platform operates on a 'Software-as-a-Service (SaaS)' model, which inherently reduces the total cost of ownership (TCO) for our customers. It is extremely scalable and can be tailored to meet the demands of all our users.

In William Hill's case, SureCloud tailored the PCI Compliance Application following a series of on-site and interactive workshops with key stakeholders, along with documentation reviews, to create a customised version for William Hill's unique cardholder data environment (CDE).

The SureCloud Platform enables William Hill to be self-sufficient, managing technical issues including forgotten passwords, adding and removing users, and specific questions about form creation and dashboard setup.

SureCloud worked with William Hill to identify the applicable controls within their PCI compliance scope. Processes include PCI compliance auditing, exception tracking and activity management, which are now automated via user definable building blocks:

Forms: William Hill users can populate the data in forms, capturing elements of processes such as PCI control lists. These forms are extremely adaptable and provide a clear audit paperchain.

Workflows: William Hill users can closely control the flow of forms through a process, and once again produce a clear, automated paper trail.

User Definable Dashboards: William Hill users can get either a summary or granular view of process activity, depending on their precise needs at that time.

SureCloud PCI compliance comes with a set of template forms and workflows to fast track process implementation. Other features include the ability to:

i. Define and track projects and tasks to ensure they're delivered on time. For example, requesting that a person completes a specific section or adds evidence for a compliance requirement.

ii. Store documents, such as the evidence for a security control, in a central repository and link the evidence to a compliance requirement or control.

iii. Run a selection of operational and management reports providing different views of the information for different stakeholders.

The SureCloud platform enables William Hill to be self-sufficient, managing technical issues including forgotten passwords, adding and removing users, and specific questions about form creation and dashboard setup. This ensures that William Hill can keep tight control over its user base, quickly and easily accessing any information it might need at short notice.

William Hill has a pre-populated PCI DSS 3.2 Control library – essentially a set of the latest PCI 3.2 requirements. The control library contains all 12 PCI Requirements and sub-requirements, including testing procedure and guidance.

"SureCloud's ability to take a comprehensive solution and tailor it to our specific needs has not only enabled us to meet our PCI compliance objectives but also our wider compliance goals, all from its single source of truth platform. Through working with SureCloud, we have been able to streamline many of our processes, free up resources to work more strategically and have gained unrivalled visibility into the data flows that fall under our regulatory compliance frameworks."

Craig Connolly, Head of Information Security Risk & Assurance, William Hill

William Hill can internally report on compliance every financial quarter, by tracking controls relevant to a specific William Hill technology area. This means that for all internal technology areas, where these are required to evidence compliance at the frequency specified, a status is marked against each control.

As an ASV (Approved Scanning Vendor), SureCloud automates William Hill's workflow and task management to remediate against any identified vulnerabilities. We also ensure that William Hill meets requirement 11.2 of the PCI DSS, through the performing of automated quarterly scans.

Immediate visibility to the scanning report allows William Hill users to centrally track progress and manage remediation. This ensures a clean report is ready for submission each quarter, as required by the Council. The SureCloud platform has also helped William Hill to file the clean scans in one central place and store all the evidence against the remediation work carried out.

The Results

On the results gained from using the SureCloud Platform, William Hill's Head of Information Security Risk & Assurance, Craig Connolly, says: "SureCloud's ability to take a comprehensive solution and tailor it to our specific needs has not only enabled us to meet our PCI compliance objectives but also our wider compliance goals, all from its single source of truth platform. Through working with SureCloud, we have been able to streamline many of our processes, free up resources to work more strategically and have gained unrivalled visibility into the data flows that fall under our regulatory compliance frameworks."

William Hill has been able to meet its PCI compliance goals via a 'single source of truth' technology platform. SureCloud's focus on efficiency, and on providing one or more dashboards for managing all PCI compliance processes, means that William Hill has drastically sped up its compliance actions, and generated a single unified source of information. The company has also utilised the SureCloud Platform for the running and management of external vulnerability scans. SureCloud has not only ensured smooth PCI compliance management; it has also become the foundation for a robust yet flexible IT security posture. ●

TokenEx: Inflection integrates tokenisation to protect customer data

A search for the most flexible and open tokenisation platform that would work with how the client's systems operate led this customer to TokenEx. Tokenisation of PII data is a natural next step.

As e-commerce, social connections, privacy, and data security become the focal points of our online lives, B2B and B2C companies are creating commerce platforms to manage the millions of daily people-to-people connections and their associated payment transactions.

Among the companies tackling this multifaceted business problem is Silicon Valley-based Inflection. The 10-year old company's identity protection and records access websites are used by both businesses and consumers to research, protect, and maintain personally identifiable information.

PeopleSmart, for example, helps create and maintain person-to-person connections among a constantly moving population. GoodHire helps small businesses screen potential employees so they can hire the right people for the right projects. IdentitySmart and Identity.com help individuals protect their identity from theft and manage the personal information that's available through public records. Customers subscribe to Inflection services and purchase its products online using payment cards for single purchases or to set up recurring billing.

With trust at the heart of its mission, Inflection is keenly aware of its obligation to protect its customers' information. "Respect for user preferences and privacy is core to what we do," says Matt Muller, who leads Inflection's 20-person Trust team. "Our commitment to protecting our customers' identities requires that we make sure the information they entrust to us stays secure."

As the rate of attacks on even the most sophisticated organisations increases, removing all payment and personal data is a key way to ensure that a successful data breach results in the data thieves getting nothing of value. On top of that, all e-commerce sites that accept payment card data must conform to PCI compliance. Keeping IT and financial systems in PCI compliance is complex, very costly in terms of manpower, and, unfortunately, is no guarantee against a data breach.

> **"Our commitment to protecting our customers' identities requires that we make sure the information they entrust to us stays secure."**
>
> *Matt Muller, who leads Inflection's 20-person Trust team*

Tokenisation reduces PCI costs, improves security

Inflection set out to ratchet up the security of its online payment processing and reduce the scope and costs of its PCI compliance. An interdepartmental team from Finance, Trust and Engineering began the search for a tokenisation platform that could readily integrate with the company's innovative STORM platform, which provides a secure foundation for the company's identity protection and records access services.

"When we started looking at technologies to protect our customers' payment and personal information, tokenisation was at the top of the list for its ability to completely remove cardholder data from our systems," Muller explains. Once all cardholder data is tokenised and stored in secure Cloud data vaults, that data would not be exposed even if a breach of Inflection's systems occurred. It also vastly reduces the cost and effort of PCI compliance.

Jeremy Wood, VP of Finance at Inflection, explains that the company's PCI challenge was, "to find a Cloud security platform that could take over the role of integrator by working with our existing payment processing, fraud detection, and card refresh vendors while removing all cardholder data from the Inflection systems."

> **"To find a Cloud security platform that could take over the role of integrator by working with our existing payment processing, fraud detection, and card refresh vendors while removing all cardholder data from the Inflection systems."**
>
> *Jeremy Wood, VP Finance, Inflection*

Complex requirements

While payment processors and other vendors offer rudimentary tokenisation, keeping all the payment card vendors synchronised both in real-time and in batch processing modes requires a flexible tokenisation partner with the willingness and capability to adapt to an organisation's processes.

And while most payment processors only tokenise payment data related to their cards and banks, Inflection needed a tokenisation vendor that was payment-processor agnostic. The combined requirements of flexibility, open integration with service providers, and the ability to support any payment processor led the Inflection team to choose the TokenEx Cloud Security Platform.

"With every vendor other than TokenEx we had to basically hand them the keys to our ability to integrate with existing partners, restricting the way we work, and limiting our choice of payment vendors," says Nachi Sendowski, Chief Architect at Inflection. "We had to take their whole package and forfeit the way we do integration. The willingness of TokenEx to be the integrator of our vendors is unique."

Jeremy Wood adds: "The TokenEx customer references we talked to were off the charts with satisfaction on service and support. It was amazing. The other aspect that convinced us to go with TokenEx was their ability to tokenise personally identifiable information. TokenEx was the only provider we looked at that can tokenise all types of data."

Weaving a web of integration

Once the decision was made to use the TokenEx Cloud Security Platform, integration began with an Inflection team of three engineers, two quality assurance members, and a project manager.

The first step was to tokenise the existing primary account numbers (PANs) stored in Inflection systems and store them in the TokenEx Cloud Data Vaults. This one-time batch process replaced all PANs with tokens that are only useful for transactions between TokenEx and Inflection.

Next, the TokenEx Web Services API was integrated with the STORM platform. Avanti Ketkar, Lead Platform Engineer, describes the process: "We integrated TokenEx SOAP Web APIs directly into our payment streams. Using TokenEx client-side encryption, the customer PAN is encrypted immediately at the point of payment. The result is passed to TokenEx to tokenise and vault. Only TokenEx has the private key to decrypt the PAN, and the actual PAN is never stored in our systems, even in memory."

This one step reduces the scope of PCI compliance to a minimal number of controls. Since all of Inflection's websites and products are built on STORM, the integration with TokenEx was effective immediately across the platform.

Fraud detection critical

Fraud detection and prevention is a critical step in all payment processing at Inflection. TokenEx natively incorporates Inflection's existing fraud prevention vendors into its Web Services API, so for each payment Inflection is able to have the transaction analysed in real-time for signs of fraud. Once again, no PANs are transmitted or received, minimising any chance of data theft.

Inflection also integrates with third-party chargeback vendors to ensure that existing subscription payments are valid.

"With TokenEx acting as the central point of integration, we can continue to operate our business as usual, sending batch files of tokens for the cards we want to refresh, or help prevent chargebacks, and TokenEx sends the batch files of payment data to the vendors," Ketkar explains.

"We get the same responses back that we are used to, but we never touch the actual PAN data. The ability of TokenEx to be the middleman with all the vendors we need to work with is a huge plus."

Testing of the complete payment processing cycle began with the existing payment stream operating in parallel. "We turned on the TokenEx integration to test for one day," Ketkar says.

"We had one technical glitch that caused some card brands to be rejected. TokenEx fixed the issue over the weekend and pushed it to production by Monday morning. One of the great things about this implementation is that TokenEx has phenomenal tech support. Even during the evaluation process they were answering questions quickly and making changes to support the way we work."

Matt Muller concurs: "With other vendors, a fix can take a month just to push to a sandbox environment, never mind production. It's refreshing when a vendor treats your processes as critically as you do. And even though this seems like a standard implementation, it was surprising to us to see how few tokenisation vendors have the flexibility of TokenEx.

In fact, there were no other vendors who could actually be the complete integrator and readily work with all our third-party services. The customisability of TokenEx is one of their greatest strengths."

Once the initial test was completed and the technical glitch quickly resolved, the TokenEx payment stream was turned back on. With all the third-party vendor integrations finished by the end of May, the existing processing stream was switched off entirely. All payment processing now flows through TokenEx. No cardholder data is stored or transmitted by Inflection systems during transactions. Complete tokenisation was accomplished in just eight weeks.

Reaching the goal of tokenising all cardholder data in such a short timeframe is a tribute to the synergy of the Inflection and TokenEx teams, the privacy and security controls of the STORM platform, and the flexibility of the TokenEx Cloud Security Platform.

Now come the benefits through greater security of cardholder data, reduced risk of losing data through potential breaches, and savings through significantly reduced scope of PCI compliance.

Wood states, "We estimate, even at this early stage, that our PCI compliance cost will be reduced by at least 30%, which includes reduced costs for supporting PCI hardware and software upgrades."

Cardholder data secured, PII data next

Matt Muller reflects on the company mission: "Inflection takes privacy seriously because we understand the value and sensitivity of personal information. We work hard to create awareness and transparency around responsible privacy frameworks, with a holistic approach that marries technology and empathy."

Selecting TokenEx Cloud Security Platform resulted from a search for the most flexible and open tokenisation platform that would work with the way Inflection's systems operate. Tokenisation of PII data is a natural next step for Inflection as the company continues building identity management and protection applications for the STORM platform. ●

Sponsors

Armor

Contact: Steve Gooding, Director of Partners and Alliances, EMEA
Tel: +44 800 500 3167 x 2512
Email: stephen.gooding@armor.com
Website: www.armor.com
Twitter: https://twitter.com/armor

CardEasy from Syntec

Contact: Simon Beeching, Business Development Director
Tel: +44 20 7741 2013
Email: simon.beeching@syntec.co.uk
Website: www.syntec.co.uk
Twitter: @synteccontact

Eckoh

Contact: Tony Porter, Head of Global Marketing
Tel:+44 1442 458 460
Email: tellmemore@eckoh.com
Website: : www.eckoh.com
Twitter: twitter.com/Eckoh

ECSC

Contact: Graham Boler, PCI DSS Service Director
Tel: +44 1274 736 223
Email: graham.boler@ecsc.co.uk
Website: www.ecsc.co.uk
Twitter: ECSC_Group

Mastercard Payment Gateway Services

Contact: Agata Lane, Director, Product Marketing, Europe
Tel: +44 20 751 32101
Email: agata.lane@mastercard.com
Website: www.mastercard.com/gateway
Twitter: https://twitter.com/MasterCard_PGS

Pay360 by Capita

Contact: Sales
Tel: +44 3333 137160
Email: pay360digitalsales@capita.co.uk
Website: www.pay360.com
Twitter: @Pay360byCapita

Sponsors

PCI Pal

Contact: Tony Smith, Sales Director, EMEA
Tel: +44 330 131 0330
Email: info@pcipal.com
Website: www.pcipal.com
Twitter: @pcipal

SecurityMetrics

Contact: Ian Eyles, Director, European Business
Tel: +44 207 993 8030
Email: ieyles@securitymetrics.com
Website: www.securitymetrics.com
Twitter: @securitymetrics

Semafone

Contact: Niraj Hassani, Sales Development Associate
Tel: +44 845 543 0822
Email: emeasales@semafone.com
Website: www.semafone.com
Twitter: @semafone

Silver Lining

Contact: Aisha Hawkes, Marketing
Tel: +44 345 313 1111
Email: aisha.hawkes@silver-lining.com
Website: www.silver-lining.com
Twitter: @silverliningUK

SureCloud

Contact: Afrika Morris, Marketing Manager
Tel: +44 7833 459 647
Email: afrika.morris@surecloud.com
Website: https://www.surecloud.com
Twitter: @SureCloud

TokenEx

Contact: JP Nelson, Business Development
Tel: +1 877 316 4544 x113
Email: jnelson@tokenex.com
Website: tokenex.com
Twitter: @TokenEx

About AKJ Associates

For more than a decade, AKJ Associates has specialised in connecting information security stakeholders and service suppliers to help solve the security, compliance and risk management challenges facing organisations and corporations around the globe. Our current portfolio focuses on information security, data protection, regulatory compliance, fraud, electronic discovery, forensics, payments risk, and the PCI DSS.

With an international presence, we have staged events in cities that include London, Singapore, Abu Dhabi, Amsterdam, Cairo, Dubai, Frankfurt, Hong Kong, Istanbul, Madrid, Milan, Moscow, Mumbai and Paris.

Content and speaking opportunities

Simon Brady, Editor
Tel: +44 (0) 20 7430 0630
Email: simon.brady@akjassociates.com

Sponsorship and exhibit enquiries

UK, Europe and the Middle East
Robert Walker, Director
Tel: +44 (0) 20 7841 2926
Email: robert.walker@akjassociates.com

Sponsorship and exhibit enquiries

Asia Pacific
James Wilson, Head of APAC
Tel: +44 (0) 20 7269 8904
Email: james.wilson@akjassociates.com

Registration enquiries

Rachel Sier, Head of Delegate Sales
Tel: +44 (0) 20 7242 4364
Email: rachel.sier@akjassociates.com

AKJ Associates

We would like to thank our sponsors

ARMOR™

CLOUD SECURITY, UNCOMPROMISED.™

pcipal®

CardEasy™

Keypad payment by phone

From

Syntec

securityMETRICS®

Eckoh

semafone®

securing data · protecting reputations

ecsc

more secure

silver lining

communication innovation

mastercard.

Payment Gateway Services

SureCloud®

Always Be Certain

Pay360

by Capita

TOKENEX