AKJ Associates

# PCI DSS: Case Studies in Excellence


Awards for Excellence 2019

# Working together to solve PCI DSS compliance

**Digital transformation, e-Commerce innovation and the spread of new payment technologies and channels are making life more and more difficult for PCI DSS professionals. One answer is better third-party compliance solutions.**

Achieving and maintaining compliance with PCI DSS has always been a tough ask. Not only is the standard itself rigorous and regularly updated, but card data is at the centre of almost every company's e-Commerce or digital transfomation strategy.

In addition, as with other compliance efforts, its lack of glamour, its complexity and technicality, and its upfront and ongoing costs, make it a hard sell to Boards already struggling with a global tsunami of regulation across data privacy, financial crime and technology risk.

These challenges may partly explain the latest findings from Verizon. After documenting improvements in the overall level of PCI DSS compliance for several years in a row, Verizon's 2018 Payment Security Report revealed a decline in organizations' level of full PCI DSS compliance for the first time. In the 2018 report, 52.5 percent of organizations were compliant with PCI-DSS, declining from the 55.4 percent reported in 2017.

Given how hard even the largest firms find PCI DSS compliance, and given the need for solutions that suit all affected businesses, the PCI DSS vendor community is an ever more key part of helping companies protect critical customer data.

Every year, AKJ reviews the PCI DSS solutions markeplace and selects those vendors it believes are making an outstanding contribution to better compliance with the PCI DSS.

This book is a selection of those solutions, illustrated by client case studies. These vendors, by their innovative work for a range of customers, have proved that they are up to the challenge of this new era of PCI DSS compliance. ●

**Editor**
Simon Brady
e: simon.brady@akjassociates.com

**Production editor**
Norma Kelly
e: normaewart@me.com

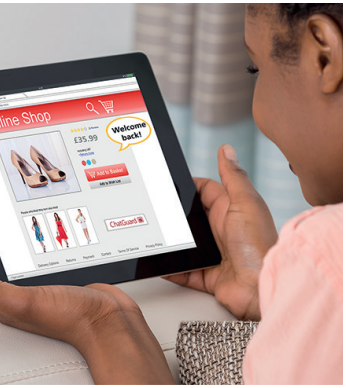
**Forum organiser:**
**AKJ Associates Ltd**
27 John Street
London
WC1N 2BX
t: +44 (0) 20 7242 4364
f: +44 (0) 20 7831 2175

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

# Contents







# Contents




# **Blackfoot:** The challenge of managing cyber risk and compliance

**Cyber Risk and Compliance are now enshrined in law. Understanding your exposures is the first step to mitigating them. Outsourcing is one solution.**

Previously, PCI DSS has been a contractual obligation rather than a legal requirement. Organisations have to ensure that their systems and processes now comply with law or face ever increasing penalties, not just contractually, but now also from both the ICO as well as potential group actions from affected customers or staff.

Managing cyber risk and compliance obligations is an increasingly complex and expensive endeavor, and getting it wrong can lead to substantial financial and reputational damage.

**The challenge**

Our client is a private members' club that holds large amounts of personal information and takes lots of card payments via multiple acceptance channels across locations all around the world.

They had a challenge in assuring investors and members that they were 'doing the right thing' and were compliant with the new Data Protection Act and as part of that also achieving PCI Compliance, across all acceptance channels spanning their entire global operations.

In achieving this they faced three main challenges:

- Understanding what Data Protection/ GDPR means and how and where it applies
- Understanding their cyber risk profile and how much security was appropriate
- Understanding what PCI DSS Compliance means and how and where it applies

**What risks do we face?**

It is difficult for most organisations to evaluate exactly where their cyber risks lie, and what those risks mean from a financial point of view. It is even harder to ensure that these are explained to senior management in clear, simple, actionable terms.

- How do we manage this day by day?
- How compliant should we be?

- Where does GDPR apply?
- What does PCI DSS mean for us?

**From objective to solution**
The objective was to create a plan and implement a programme of work to enable the board to give assurance that, a) they were doing the right thing, and b) were managing cyber risk and compliance to Data Protection/GDPR as well as PCI DSS.

Blackfoot's Cyber Assure managed service is designed to take the problem away from the client, leaving them safe in the knowledge that, as partners, we will ensure that cyber risks are minimized and systems and processes are de-risked making compliance quicker and easier.

Working with the client in a partnership, with intimate knowledge of the organisation's structures, Blackfoot will work to identify and minimize cyber risks, giving clients the comfort they need that experts are taking care of it.

After initial conversations with the client, so that we gained an understanding of what was and wasn't important to them, we conducted an organisation-wide cyber risk assessment.

This gave the organisation a starting point and a clear, simple, and consistent picture of different cyber risks and the potential impacts they could have on the business.

These included risks to confidentiality of personal and financial information, the integrity of information held by the business, the availability of critical systems, and the authority to process personal data.

Once we had agreed a Cyber Risk treatment programme, we split the work into logical steps.


We started with raising the maturity of cyber governance by holding executive briefings and then implemented regular governance and progress meetings with senior stakeholders: this enabled buy-in across the business, ensuring quick adoption of the programme.

The programme of work was then ordered according to risk, ensuring the quickest reduction in risk over time. It covered a number of areas including:

**GDPR**
We conducted an organisation-wide GDPR assessment. This revealed all the gaps in compliance and after conducting Privacy Impact Assessments we were able to risk-base the order of treatment, ensuring the risks were reduced as quickly as they could be.

We helped reduce the scope of GDPR through altering processes which resulted in the client processing less Personal Data, leading to a halving of systems processing personal data, significantly reducing both the time and costs of compliance.

As the final part of the GDPR assessment process we looked at the required cyber security controls and appropriate levels of maturity to ensure sufficient accountability measures, again based on the earlier work we had carried out we had calculated their appropriate levels, based on the risks they posed.

**Payment Acceptance Risk**
With payments, we started with simplifying the global acquiring contracts and looking at better card processing processes to minimize the PCI DSS scope per acceptance channel.

Once we had agreed with the client the changes to certain processes and the altering of current practices, we had an agreed scope per acceptance channel.

We also helped advise on tokenization and digital wallets for member card payments, reducing the amount of payments taken by 70% and therefore the potential impact of a card data breach.

**Cyber Work Programme**
Taking a holistic approach we merged all Data Protection, Cyber Risk and PCI DSS requirements and implemented the following activities:

- Implemented Information Security Policies and Procedures, which were mapped for all risk and compliance requirements. This ensured that staff only had to deal with a single change in the way they worked.
- To ensure staff understood why we were asking them to change their daily processes and adding more documentation to certain daily tasks we implemented our award-winning SAT across all 4,500 staff, giving staff the understanding of why the organisation was asking for everyone to pull together and keep staff and member data safe and protected. As part of this we conduct regular phishing tests to highlight staff who needed ongoing training.
- We trained their incident response team and have regular 'dry runs' scheduled to keep them up to date and well versed should a major cyber incident occur, reducing the potential impact of any cyber attack.
- We have designed a gradually increasing testing schedule, allowing relevant staff and partners to improve patching of systems and secure coding of applications. The first year we have conducted internal vulnerability scanning and external penetration testing, setting a baseline for year


2 and 3 BAU testing of systems and applications on a regular basis.

- As a dynamic organisation there are lots of new initiatives, most reliant upon digital and technology. To that effect we have assisted project management in implementing privacy and security by design for all new systems and applications.
- As supply chain risks are growing we have focused on assessing their supply chain for cyber risks and compliance issues. We helped risk rate the entire supply chain and then implemented a cyber supply assurance programme dealing with the most risky suppliers.

**Impressive Results**

By investing in the Blackfoot managed service, the client has achieved the following in under a year.

- Cyber governance function in place with measurable KRIs and KPIs
- GDPR framework implemented with building Accountability Measures Payment risk and PCI
  - Streamlined acquiring from multiple to a single acquiring contract
  - Reduced time to PCI compliance from three years to 14 months
  - Saved client over £2 million in capex and £300k in annual op ex.
  - Reduced the volume of card payments by over 70% through the introduction of tokenization and digital wallets for members
  - Reduced and implemented acceptance channel controls as follows:
    - eCommerce from SAQ D to SAQ A
    - Face to Face from SAQ D to SAQ
    - P2PECNP from SAQ CVT to SAQ P2PE

With the board now receiving regular updates on progress they now have the confidence to go back to both members and investors and give them the assurance that they are doing the right thing. That they are minimizing Cyber Risk in the organization by both complying with GDPR globally – as the highest international standard for protecting member and staff data – as well as now being PCI compliant and reducing the risk of card processing breaches as we've recently seen. ●

# CardEasy from Syntec:
# Protecting 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 award-winning, patented CardEasy 'keypad payment by phone' DTMF masking system enables merchants to de-scope their call centre environment and call recordings from PCI DSS. This reduces the risk and cost associated with managing card payment transactions in contact centres, including outsourcers and homeworkers.

CardEasy increases customer trust and improves the customer/agent experience, reducing 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 as an independent UK network operator and 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 reading their payment card numbers out aloud 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). There is also a customer self-service Autopay alternative, which works with 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 Provider (PSP) 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.

## Why a direct-sell cosmetics organisation with global network chose CardEasy

**The challenge**

The organisation takes a significant number of payments by phone each year, either via its IVR or via call centre agents. This meant that its contact centre operation was in scope for PCI DSS.

The costs of adhering to PCI requirements were significant. Each year the company had to upgrade its infrastructure and retrain its agents in the new requirements. Consequently, it planned to use DTMF masking to descope entirely from PCI DSS and reduce the administrative and financial burden of the annual audit and to reduce the questions on the form they have to complete. To do this they decided to eradicate card details from their infrastructure completely.

**Why CardEasy?**

The decision to implement CardEasy was driven by the need for a DTMF masking system that would work with their existing systems, enable payments to be taken by both IVR and by agents, work with the in house contact centre and with outsourcers, and provide a seamless experience for callers.

The organisation had a good and robust IVR system that had been in place since 2004 and had a lot of functionality that it was important not to lose.

"It was very important for us to find a solution that would work with our existing IVR. We didn't want to have to change our IVR system in order to get the benefits of DTMF masking. We also wanted to make sure that the callers' experience would not be disjointed. The last thing we wanted was for a caller to be rerouted half way through the call to a different IVR that had been set up just to process payments," says the SSC Technology and Projects Manager.

CardEasy was selected because it worked seamlessly with the organisation's existing on-premise IVR system as well as with its other suppliers' systems.

It was very important to the company that it selected a solution that would seamlessly integrate with existing systems. It has vendors that create and manage our IVR and different vendors for its telephone systems. CardEasy was able to integrate effectively with multiple vendors' systems.

**The results**

From a caller's perspective, the only real difference is that their card number is no longer played back to them as happened before. Previously, the caller entered their card number, and then it would be confirmed back to them. In the new process, they are asked to enter their card number and then move on which actually speeds up the process slightly. The BIN checking is still being done so the caller can't get all the way to the end of the process only to find that they've entered their card number incorrectly. ●

**"One of the good things about CardEasy is that it is payment processor or acquirer agnostic so you have one solution that fits all of your customers. Generally, the amount of effort that Syntec has had to put in from an integration perspective has been very little, which has been really good. Confidence levels are high. Everything is good."**

*SSC Technology and Projects Manager*

# Locus H2O Wireless removes PCI risk from omni-channel contact centre in the USA

## A four-week integration with Syntec's CardEasy keypad payment by phone and TokenEx cloud tokenisation.

The contact centre is becoming the nexus of omni-channel commerce. Incorporating interactive voice recognition (IVR) systems, live agents, chat bots and web portals, what was once a problem-solving support centre is now the focal point of payments that flow from customers through telephony lines. But with that shift comes the responsibility of securing the payment and personal information that is collected, stored and processed by agents and automated devices.

Contact centres with human agents that accept payment card information must conform to the highest levels of the PCI Data Security Standard (DSS) — an expensive, time-consuming and ongoing process. However, by removing all payment card information from the conversation between customers and live or automated agents, re-routing the sensitive data out of internal business systems, and storing only tokenised data, the need for PCI compliance can be greatly reduced and the call centre secured from data attacks.

### The challenge facing H2O Wireless

H2O Wireless provides its customers with pre-paid cellular services, both through direct and indirect sales. Customers choose a plan that meets their data, text and voice needs and pay a set monthly fee, with no contract or hidden fees. Tech-savvy customers can use the web portal or IVR, or new customers can get personal help from an agent. In all these channels customer payment and personal information is captured by human or software systems, stored and reused as needed. The organisation processes over 350,000 transactions a month, 3.6 million transactions every year, and this number is increasing.

> ***"Even though we were using very strong encryption models to protect the payment and personal information, it was still passing through and being managed by our systems. Critically, our human agents in the contact centre were being exposed to payment account numbers over the phone, creating a tricky PCI compliance problem. We needed to get rid of that step as well."***
>
> Carlos Moreno, Payment and Fraud Analyst, Locus Telecommunications

Locus has bespoke CRM and back-office financial systems tailored to meet its business needs. These specialised systems process all payment and customer account data for multiple business units including H2O. Since human agents were exposed to the incoming sensitive data, keeping these on-premise systems and the contact centre in compliance with PCI DSS was a massive effort. New Euro-zone data privacy regulations such as GDPR require even more security over personal information for international organisations.

H2O's key objective was to keep the sensitive data from entering its systems, but without having to alter the existing IT applications.

### Searching for an open and flexible security platform

The first step of reducing the scope of PCI compliance entailed choosing a security platform that could not only provide the necessary tokenisation of payment data before it entered H2O Wireless systems, but vault it off-premise. The most critical requirement however, was to find a tokenisation vendor that could integrate with the existing H2O Wireless systems and business processes and require very minimal changes to them. The TokenEx Cloud Security Platform fitted the bill.

The TokenEx Cloud Security Platform is a flexible and open solution which intercepts payment data, turns sensitive data into tokens

***"We chose Syntec because they had the solution that we needed to de-scope our live contact centre agent and IVR environment. Syntec was the only vendor that provided the flexibility to integrate with our home-grown systems because their system can be cloud-based, with no requirement to change any of our existing IT. The same flexibility offered by TokenEx was offered by Syntec."***

*Carlos Moreno, Payment and Fraud Analyst, Locus Telecommunications*

(the tokenisation process), and stores the real data, personal or payment, in secure cloud data vaults. Tokens are returned to the client's systems to be used for payment processing and account management. This means that sensitive data is never accepted, stored, or transmitted by the client's internal business systems. In this way, business processes continue functioning as usual using tokens and, should a breach occur, no sensitive data is exposed. As a result, the scope of PCI compliance is greatly reduced to a few PCI DSS self-assessment questionnaire points, at a much lower cost and overhead.

## Diverting incoming payment card data to the cloud with Syntec CardEasy

However, to reduce PCI compliance requirements to the absolute minimum, there still remained the initial receipt of PANs through the contact centre via a live agent or the IVR system. The existing system let customers enter their payment information through DTMF (dual tone multiple frequency or touch-tone signalling) keypads on landline or mobile phones, but the human agent was still on the line and could conceivably intercept the PAN. Likewise, with the IVR the PAN was still being received and decoded from the DTMF signals and recorded in the contact centre system. This process keeps the contact centre in scope for PCI compliance and is difficult to monitor.

TokenEx could not intercept the incoming DTMF signals and tokenise them directly – they had to be digitised first using Syntec's patented CardEasy keypad payment by phone DTMF system. CardEasy can be deployed as a cloud service, integrating with the TokenEx cloud platform, to ensure that payment card numbers never enter the contact centre environment.

Syntec's CardEasy system was also quick to implement. CardEasy interfaces with any telephone call centre solution and back-office system out of the box. It intercepts the DTMF tones representing the customer-entered PANs, decodes them and, in the H2O Wireless implementation, sends the PANs directly to TokenEx to be tokenised and stored. Agents and the IVR system never hear, see or receive the digits or tones for the complete PANs, so they are not available for capture in call centre systems or call recordings, thereby keeping the contact centre out of scope for PCI compliance.

## Achieving a PCI compliant contact centre in four weeks

**Carlos Moreno summarises the success of the project with two quantifiable and significant savings.**

***"One of the biggest savings is something that we were able to quantify from the very beginning — that we could keep our homegrown systems as they are. We didn't have to spend any effort or funding to integrate something new or change our payment strategy. We're talking about potential savings of nearly half a million dollars if we had to purchase just a new CRM system—not even counting the manpower and time it would take. Looking at savings for PCI compliance, if we had to create our own PCI Island with separate servers and databases to isolate the contact centre, the hardware costs alone would be onerous. Being able to work with TokenEx and Syntec to become PCI compliant with no changes to our operations and IT infrastructure is a huge benefit. Doing so in four weeks is really a great way to measure success."*** ●

## CardEasy works just as effectively for callers in the USA, Germany and Australia as in the UK


***"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*

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.

(*Continued from p8)*

**Deployment Flexibility**

The CardEasy system can either be hosted in Syntec's network or deployed as a telephony-agnostic, hybrid premise-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 premise- based equipment. All versions use the CardEasy cloud for their PSP connections and the hybrid and 'pure cloud' options work with the merchant's 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 (e.g. 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 premise-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.

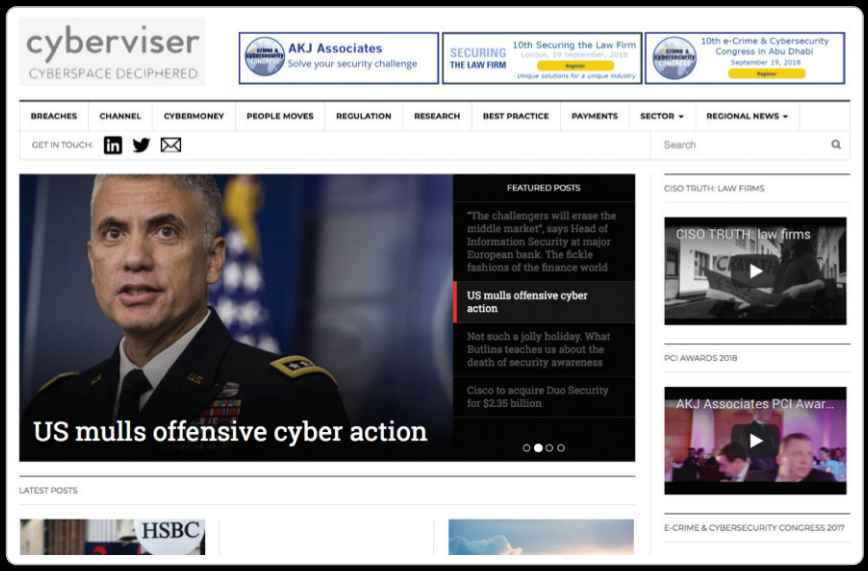
CardEasy is available globally. ●

# www.cyberviser.com – launching now!

You know AKJ Associates for its 20-year record of market-leading conferences and events in cybersecurity and compliance. Under the e-Crime Congress, Securing the Law Firm and PCI London brands, we have consistently tried to get ahead of the trends shaping your market and careers, instead of rehashing the same old ideas.

We were first to bring CFOs and institutional investors to you, to reveal what business and stakeholders really think about cyber. We were at the forefront of understanding the collision of cybersecurity, operational risk and compliance. And we have not been afraid to confront cybersecurity's many inconvenient truths.

To expand the resources we provide to you, we are launching a website to continue our mission of delivering independent thought leadership, news and views.




## www.cyberviser.com will bring you:

- ✓ **Research and data:** AKJ Associates' proprietary data and conclusions gathered from security professionals around the globe. Our first project, 'Who Secures the UAE' is now live.
- ✓ **News and comment:** the most significant news stories with interpretation and comment from AKJ editors and the market.
- ✓ **Best practice:** what works and what doesn't, direct from leading end-users and security practitioners.
- ✓ **Regulation:** the latest global news on regulation and compliance, cross-sector, cross-region.
- ✓ **People:** who is firing, who is hiring and what are they paying? CISO profiles and interviews.
- ✓ **Vendors:** start-ups, funding, M&A, new solutions and new technologies.

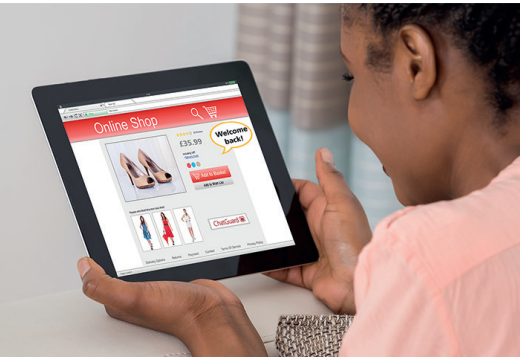
# **Eckoh:** Introducing the World's First Secure Payment via Chat

**While Chat is a great way to increase customer engagement and prevent cart abandonment, without secure payment it can create more problems. Eckoh's innovation provides the solution.**

### How Eckoh have addressed the challenges

**Sales abandonment:** Contact centres have embraced Chat as an engagement tool. It has proven to be successful in preventing cart abandonment as customers are able to get real-time answers to their queries. 79% of customers say that they prefer Chat because of the immediacy of it. [eConsultancy]

**Providing seamless customer journeys:** Before secure payment in Chat was available, contact centre agents would have to direct customers away from Chat to either call a contact centre or to a different website in order to make a payment. This breaks the journey and frustrates the customer who then has to repeat all the information about their order. Given that 77% of customers won't make a purchase if there's no Chat support why would a business want to send their customer away right at the point of purchase? [Business2Community]




**Fraud prevention & enhanced security:** In some cases, contact centre agents are actually asking the customer to type their payment card details into an unsecure Chat window. Naturally this is insecure and exposes the customers' sensitive data to an insecure connection as well as the contact centre agent. It is obviously not PCI DSS compliant.

**Payment preferences:** Consumers want to choose how they pay, regardless of channel. However, until Eckoh launched its ChatGuard solution there was no secure way to do this while in a Chat session. Given how popular Chat is with customers today this posed a challenge for contact centres when it came to preventing sales abandonment.

**Multi-Channel delivery:** While Chat has become a leading customer engagement channel it did not originally cater for taking an actual payment. By

introducing its secure payment solution, Eckoh has made it possible to extend the customer experience and robust security into a new payment method to satisfy both agents and customers.

**Reducing friction in payments:** Removing the need for the agent, or customer, to change screens in order to make a payment, has ensured that the payment process is smoother and seamless.

### Innovation

As the leader in Secure Payment and Contact Centre solutions, Eckoh is committed to bringing the latest and best solutions to the market without ignoring traditional engagement channels. Creating a solution for making a secure payment while in a Chat session was a truly ground-breaking innovation and Eckoh were the world's first to do so. This clearly demonstrates Eckoh's ability to see the future direction of payments as well as customer preferences and technology capabilities.

### How it works…

A customer can browse at leisure through a company's website and use the Chat function to ask questions, check price, delivery options and even availability so they are well informed when they make their buying decision.

Once products are chosen, payment options appear within the Chat window itself. The payment is secure and PCI DSS compliant, so a customer's data is protected.

The Chat agent remains on-hand throughout the process to advise or guide the customer. Importantly the agent never sees cardholder or personal data thanks to Eckoh's tokenisation technology. The agent only sees meaningless, tokenised numbers and receives a confirmation and payment reference once the customer has completed the purchase.

### Why it's ground breaking...

- Eckoh were the first PCI DSS Level One Service Provider to carry out a secure payment through Chat
- It takes an existing secure payment technology into a new channel
- Contact centres can offer payments in a customer's channel of choice
- It reduces the risk of fraud, utilising Eckoh's tokenisation technology
- It demonstrates forward thinking innovation
- It helps keep contact centres at the forefront of secure payments
- It's delivered tangible financial results for a major UK online retailer.

### Benefits

**Convenience: For customers:** At the point of making a payment they don't have to switch screens or systems, so it is ultra-convenient to make the payment within the Chat session. **For agents:** Having started an engagement the agent doesn't risk losing the sale because they can stay in contact with the customer throughout the payment process and don't have to switch screens or systems.

**Enhanced security:** Because it uses Eckoh's renowned secure payment process it offers the same levels of security to customer data as Eckoh's other secure payment solutions. The Chat element is also secure as the conversations are held over a secure connection, so it is not publicly available to any outsider. This means agents can ask the customer to type their card details into a specific secure payment Chat window to reduce the risk of losing a sale.

Tony Porter, Head of Global Marketing at Eckoh, says: "The solution is quick and easy to implement and can take businesses ahead of their competitors, delighting your customers at the same time by offering them the payment channel of their choice and differentiating their customer experience."

**Reduce cart abandonment:** Agents can avoid losing customers at the point of payment by being able to take the secure payment there and then, rather than asking a customer to go to another website or call a contact centre in order to make a payment.

**Enhanced customer experience:** Being able to respond to a customer's queries about a purchase, agents can then provide a seamless journey through to payment without having to leave the Chat session. This means customers don't have to repeat all their queries when being re-directed to another place to make a payment.

**Shared Payment Module:** It utilises an Eckoh platform that services a number of other PCI DSS compliant payment channels such as IVR, mobile app, web, SMS or agent assisted. Meaning access to a wide range of payment methods through a single integration and supplier.

**Payment evolution:** Merchants can now offer a new, flexible and scalable way to take secure, hassle-free, PCI DSS compliant online payments.

**Universal value:** It's just as valuable in enhancing customer experience for any online business regardless of sector and has corresponding benefits to the end customer.

**A world first**

Truly ground-breaking: Eckoh were the world's first PCI DSS Level One Service Provider to offer secure payment via Chat.

**Tangible results:** One of Eckoh's strategic clients in the retail sector has seen an increase in sales of £48,000 through using Chat. That same retail business and its sister company, now have 79% of their customers using Chat to make a purchase.

**World-class innovation:** It appears nonsensical that a customer, choosing to engage via Chat, would then have to exit that tool and go somewhere else to make a payment. Far better for the customer and agent to be able to complete the purchase while still in the Chat session. Eckoh's invention has created a real, secure payment solution which harnesses its already established tokenisation technology to secure personal and payment card details.

**Evolves payment methods:** This solution helps keep contact centre payment methods at the forefront of customer engagement by offering customers the payment channel of choice.

**Wider application:** It's a win-win solution for any contact centre and their customers because it is applicable to any sector or business, providing great experiences that will keep their consumers coming back.

As Tony Porter, Head of Global Marketing at Eckoh, concludes: "We're always looking for opportunities to create new, flexible and scalable ways to take friction–free payments. The addition of secure ChatGuard is a great example of innovation that will truly enhance the customer experience." ●


“ I did find this event extremely well organised and all speakers and presentations were smooth and seamless. It was a pleasure to be there! I found it very thoughtful to have short seminars in between too. ”

Risk and Compliance Manager,
Wirex Ltd

“ Another great PCI event with excellent speakers from various backgrounds and industries. Thought the panel discussions were particularly thought provoking and came away with lots of food for thought. ”

Lead IT Auditor,
Camelot Group

“ Another worthwhile PCI London with plenty of insights on best practice to maintain compliance with PCI DSS as well as a look ahead to the future of payments, and emerging compliance and security benefits from AI technology. Well done. ”

Head of Information Security,
Travis Perkins

“ As a project manager new to both PCI and GDPR, I found the PCI London seminar extremely useful. The speakers were informative and educational whilst the seminars provided an insight to real-life case studies from security professionals. A thoroughly interesting day. ”

Project Manager,
The Travel Corporation

**PCI 2018 sponsors included:**

Strategic Sponsors

Pay360 by Capita · gemalto security to be free · SRM Smart Security. Smart Compliance.

Education Seminar Sponsors

ARMOR · barclaycard · datadivider · CardEasy Keypad payment by phone from Syntec · CRYPTOMATHIC · PCIpal · TOKENEX

Networking Sponsors

Aeriandi Voice Matters · blackfoot · IT governance · f5 · Infradata · RMINGTON INFORMATION SECURITY · semafone securing data - protecting reputations · silver lining communication innovation

For more information, please call Robert Walker on +44 (0) 20 7404 4597
or email robert.walker@akjassociates.com

# **ECSC:** Managed security and artificial intelligence

**One of the difficulties with many SIEM solutions is the amount of resource required to make sense of the raw data they produce, even with AI in place. A 24/7 managed SIEM solution is much more efficient for many clients, allowing expert consultants to make sense of the data and identify where action is required.**

**Background**

As a lifestyle business, whose customer base is predominantly high net worth clients, success relies hugely on their reputation. As such, the security of their clients' data is an ongoing high priority. This is evidenced by the regular penetration testing they already carry out with ECSC, in addition to becoming ISO 27001 certified with our support.

**"PCI DSS compliance is not simple; it is a complex standard, and achieving full compliance can be very costly for an organisation, in terms of both investment and time. For this client, we had already established time was an issue."**

*Graham Boler, PCI DSS Service Director, ECSC*

Their service is a global offering, operating across all time zones and via multiple languages with systems distributed across five continents. A significant part of what they do is take card payments via their call centre, meaning they had a requirement to demonstrate their PCI compliance, and as a Level 1 Visa merchant, processing in excess of six million Visa transactions a year they had an added responsibility of completing a Report on Compliance (ROC).

As an existing client, they approached ECSC to help them gain PCI compliance and a ROC. Despite having a global headcount of almost 1000, the resource they had available to own the project in-house was limited, in addition to a number of changes within personnel. The client had previously relied on software to alert them to suspicious activity against their stored carddata.

**Solution**

The client required a solution that would essentially require as little of their time as possible, whilst allowing them to demonstrate how serious they were about security and not taking any short cuts.

PCI DSS compliance is not simple; it is a complex standard, and achieving full compliance can be very costly for an organisation, in terms of both investment and time. For this client, we had already established time was an issue.

Due to the global operation of this client, their in-scope systems were substantial, equating to approximately 1,000 call centre desktop PCs, 200 Windows servers and a variety of Amazon Web Services cloud components.

The software used by the client was a 'Security Information and Event

Management (SIEM) solution' purchased with the objective of making sense of their cybersecurity information, events and alerts in a bid to prove continuous monitoring as part of their compliance. Unfortunately for the client this is only half the story.

A common element of an effective SIEM is that they create work, whether in-house or outsourced. It is not enough to simply collect the logs, they must be reviewed regularly and most critically, to take action to understand what they are telling you and to act on any potential issues.

After a review of what vendor alternatives were available, the client opted to deploy an ECSC Managed Security ARIEL SIEM solution, which now monitors events from both their traditional on-premise devices and cloud infrastructure, providing intelligence not just on external threats but also internal activities which break policy, for example the installation of software, unusual user behaviour and so on.

As part of our SIEM solution we incorporate KEPLER Artificial Intelligence (AI) which enables us to handle large volumes of events and alerts to satisfy PCI DSS requirements.

AI is not used as a standalone feature but instead feeds structured intelligence to our highly trained ECSC Security Operations Centre (SOC) engineers, who make sense of complex data from a wide range of sources, and then provide the client with meaningful information to take necessary action; giving context to often highly technical information.

We currently analyse over five billion events per month. ECSC operates 24/7/365 from our two Security Operation


Centres, located in the UK and Australia. By outsourcing your security, clear delineation of focus and roles can be established.

**Outcome**

Our client now has complete peace of mind that they have effective processes and systems in place to maintain PCI compliance at all times. By deploying the ARIEL SIEM solution, they are no longer required to perform any configuration management or monitoring themselves – freeing up their time to concentrate on their general day-to-day business.

The successful completion of their ROC continues to demonstrate to their clients their ongoing commitment to security and compliance, and that they're not looking to simply 'tick a box'.

**About ECSC**

ECSC was the first UK organisation to achieve PCI DSS Level-1 Service Provider Certification for a wide range of IT security managed services. We can also provide flexible solutions to help achieve rapid compliance to the PCI DSS standard. Our PCI specialists are all Payment Card Industry Qualified Security Assessors (PCI QSA). ●

# **Gala Technology:** A new approach to scope reduction for remote (CNP) transactions

**The challenges associated with handling remote/MOTO transactions are significant. How can merchants cost effectively avoid chargebacks from compromised card data or stolen payment cards?**

In the UK, in 2017, £731.8 million was processed in fraudulent transactions with 77% (£566 million) coming from compromised card data.

More than 191 million incidents of financial fraud occurred in 2017 according to official figures released from UK Finance, representing a 3% increase compared to 2016.

In addition, a leading payment service provider's fraud prevention guide states that authorisation does not guarantee against merchant chargebacks.

"Because the card and cardholder are not present, you are unable to physically check the card or the identity of the cardholder. You (the merchant) therefore need to be particularly careful about CNP (card not present) transactions, because it is much easier for the fraudster to disguise their true identity. You (the merchant) are responsible for ensuring that CNP transactions are not fraudulent. If a transaction is fraudulent, you will be liable for the loss. You need to ensure that you have procedures in place to protect your business against fraud."

In Security Metrics' analysis of merchant scans in 2017 they found 114 million unencrypted card numbers and identified that 69% of the UK businesses scanned were storing unencrypted card data. This means hundreds of thousands of businesses are at risk of a breach and the associated penalties. This is how we helped one merchant address the challenges of handling Remote/MOTO (mail order/telephone order) transactions.

The problem: ABC Limited is the UK's leading tyre distributor and has been supplying the trade industry for over 45 years. Trading from three distribution centres, last year they supplied in excess of 2.5 million tyres, generating over £142 million in revenue. As a company, ABC Limited was facing some significant challenges, especially around PCI DSS compliance and the associated risk from handling Sensitive Authentication Data.

The majority of ABC's transactions are processed as CNP or MOTO transactions. A significant number of card payments are handled in their central contact centre and, like many companies that handle MOTO transactions, they

struggled to evidence PCI compliance to their Acquirer and to complete PCI DSS certification with their compliance partners, Security Metrics.

Struggling to evidence and certify PCI compliance, ABC Limited was:

- Concerned they might suffer a data breach
- Concerned with the spiralling costs associated with processing CNP MOTO transactions. Because MOTO transactions are regarded as 'non-secure' by acquirers, i.e. higher risk, ABC Limited was faced with incremental 'non-secure' transaction charges of 0.5% of the transaction value, on top of their normal acquiring rates/merchant service charge. This equated to in excess of £40,000 per annum.
- Also faced with additional 'non-compliance' fees from their acquirer, @ £600 per annum.
- In addition, because the MOTO transaction is "non-secure", i.e. cannot be authenticated, Acquirers advise merchants to only deliver products to the registered cardholders' address.
- Then as part of the authorisation process, Issuers carry out an Address Verification Service [AVS check] on the post code registered to the cardholder's account.
- They also check the CV2 printed on the signature strip on the back of the card and associated with the Card number on the front of the card. Unfortunately, however, even if the security code is correct and the AVS check is positive, and regardless of whether or not delivery is signed for, if the cardholder challenges the charge on his/her statement, the transaction may be charged back to the merchant.

It is only if the merchant can successfully challenge the chargeback, that the merchant will get the amount re-credited to the merchant bank account. Having

suffered a number of such chargebacks, ABC Limited decided to ONLY ship tyres to the card holder's address. This obviously led to frequent customer service issues.

**So they decided to tackle the problem...**
In an effort to address the difficulty associated with making the telephone payment PCI compliant, ABC Limited challenged their acquirer to suggest a positive, cost effective solution. The acquirer suggested solutions developed to address PCI compliance e.g. IVR and DTMF suppression, to support the journey to PCI DSS compliance.

The timescales for deployment and the difficulty in making a business case for the CAPEX expenditure were not received positively by the Board, especially as neither solution addressed their concerns with regard to the number of chargebacks and the incremental 'non-secure' fees, for CNP/MOTO transactions.

The requirements and key objectives in looking for a solution to help with their journey towards PCI DSS compliance, reduction/elimination of a risk of a breach of cardholder data and to address chargebacks and increasing cost of processing CNP payments, ABC Limited had very specific requirements and objectives:

- Reduction/Elimination of a risk of a breach of cardholder data


- Reduction of scope of PCI DSS compliance
- Introduction of tokenisation to help manage recurring payments for regular customers
- Elimination of PCI DSS monthly non-compliance fee
- Protection from fraud related chargebacks
- Ability to deliver products to alternative addresses
- Cost effective solution, not encumbered with a costly capital expenditure
- Ability to take multi/OMNI channel payments

So, ABC Limited's Acquirer reached out to Gala Technology, in part, because their payment solution, SOTpay [Secure Order Transfer Payment] had already won the 'Security Innovation of the Year' at the national IT awards, to try and solve this complex problem and meet ABC Limited's requirements and key objectives.

**About SOTpay**
SOTpay eliminates the risk of fraud related charge-backs for businesses, by authenticating MOTO and Omni-channel CNP transactions and also processes the payment in a PCI compliant manner. The cloud-based technology does not require any additional hardware or amendments to existing telephony or network configuration and is Acquirer and PSP agnostic. Totally eliminating the need for capital expenditure, SOTpay can support businesses of all shapes and sizes from a small corner shop taking occasional MOTO transactions to large multi seat contact centres. The attractive 'pay-as-you-go' contracts ensure the solution is affordable for level 1 to level 4 merchants alike. SOTpay enables the cardholder to securely input their card details without

disclosing the card number and sensitive card information to the merchant/ merchant agent, thus providing a cost-effective scope reduction approach to PCI DSS. Eliminating cardholder data in its entirety from the merchant environment makes achieving and maintaining PCI DSS compliance easier and more manageable for the merchant.

The flexibility of the SOTpay technology enables the merchant to accept secure and compliant transactions across numerous channels, boosting business by allowing cardholders to complete transactions in their desired channel of engagement. For example, if someone is engaging with the business on Facebook, SOTpay allows the business to take payment within the Facebook Messenger environment. Likewise with web chat applications. The merchant/ merchant agent remains in constant contact with the cardholder, whether via telephony or digital channels such as web chat, and is also able to record the calls whether for business, customer service or compliance requirements, without the need to use pause and resume technologies etc. The agent also has constant visibility of where the cardholder is on the payment journey without seeing /touching the card number and sensitive authentication data.

This allows the agent to guide the customer through each step of the transaction without ever losing contact, which results in a higher transaction acceptance rate and less call abandonment. Where it is not convenient for the customer to complete the transaction immediately, SOTpay offers a delayed, non-attended transaction process, allowing the cardholder to complete the transaction at their leisure. SOTpay will then notify the merchant when the transaction has been completed. SOTpay will also notify the merchant of any payments that have not yet been completed, allowing the merchant to re-engage with the customer and chase payments accordingly.

As SOTpay uses additional authentication methods during the payment process, it essentially converts a 'non-secure' payment into a fully authenticated 'secure' payment, which is processed as such by the Acquirer. This alone eliminates the incremental 'non-secure' charge now imposed by Acquirers for MOTO payments, i.e. the uplift of 0.5% of the transaction value, on top of the normal merchant service charge referred to above. The process of fully authenticating the cardholder also ensures that liability for fraud related chargebacks is "shifted" from the merchant to the issuer.

**"Gala Technology's SOTpay product is the first solution I have seen that makes achieving and maintaining PCI DSS compliance much easier for merchants"**

*Connie G Penn, Card Payments and PCI DSS subject matter expert, Kilrush Consultancy Ltd*

With liability for fraud related chargebacks eliminated, the merchant can also deliver to an alternative delivery address, instead of just to the registered cardholder's address, as previously required by the Acquirer. It is estimated that a billion pounds of genuine business is turned away annually by businesses who do not feel able to take the risk of delivering to third party addresses. SOTpay removes the risk.

**The Project Process**
Following the introduction from the Acquirer, Gala Technology visited ABC Limited at their premises to understand their challenges and key objectives. Armed with this information a collaborative strategy was designed.

**Key Objective 1: Reduction/elimination of risk of a breach on cardholder data**
SOTpay eliminates all cardholder data from the merchant's environment.

**Key Objective 2: Reduce the scope of PCI DSS compliance**
As SOTpay prevents sensitive payment cardholder information from entering the merchant's environment, PCI DSS scope is significantly reduced, enabling compliance to be more easily achieved and maintained.

**Key Objective 3: Introduction of tokenisation to help manage recurring payments for regular customers**
This was something that our platform did not offer. However, as a large percentage of ABC Limited's transactions were from loyal customers. Gala Technology deemed it was critical to facilitate tokenisation for repeat transactions to enable ABC Limited to conduct simple 'one click' payments, facilitating a positive customer experience.

Gala Technology did not charge anything for this enhancement to SOTpay, as we appreciated that it provided a valuable service for other merchants and cardholders going forward.

**Key Objective 4: Elimination of PCI DSS monthly non-compliance fee and reduce acquiring costs**
As SOTpay facilitates an easier journey towards PCI Compliance, ABC Limited achieved PCI Compliance almost immediately after implementing SOTpay. In addition, because SOTpay converts a 'non-secure' CNP transaction into a 'secure' transaction, the incremental charges that ABC Limited had for "non secure" payments were immediately nullified. This gave ABC Limited a saving of over £40,000 per annum. This essentially ensured that after deploying and paying for the SOTpay service, the merchant was financially better off.

**Key Objective 5: Protection from fraud related chargebacks**
By authenticating the cardholder, SOTpay eliminates fraud related chargebacks, because the authentication of the cardholder shifts liability for fraud from the merchant back to the issuer.

**Key Objective 6: Ability to deliver products to alternative addresses**
This key objective was also achieved. Because the card is authenticated, goods can be delivered to other addresses, rather than to just the cardholder's registered address.

**Key Objective 7: Cost effective solution, not encumbered with a costly capital expenditure**
The SOTpay digital cloud-based solution does not require additional hardware and consequently is an OPEX, 'pay-as-you-go' solution. This meant that ABC Limited did not have any up-front cost. Gala Technology simply charges a fixed (pence) per transaction fee, enabling the merchant to fully understand how much deployment will cost.

**Key Objective 8: Ability to take multi/ OMNI channel payments**
As customers embrace digital transformation further, businesses are under more pressure to take a multichannel approach. This means

engaging with clients on various platforms such as Facebook, Web Chat, Twitter, Skype, etc. SOTpay enabled the business to accept secure and compliant payments across all digital channels, helping support ABC Limited's future growth plan and requirements for secure cardholder authentication as part of the Second Payment Service Directive (PSD2) set to take effect in September 2019.

**According to ABC Limited's Finance Manager:**
"SOTpay simply benefits everyone. Our customers benefit from greater security, no longer providing their card details to our organisation, and we benefit from PCI DSS compliance, better security for card payments, reduced risk of fraud, elimination of the monthly non-compliance fee and a reduction in Merchant Service Charges. The dashboard is simple to use, requires very little training, and the team at Gala Technology were excellent throughout the implementation and support process."

**Connie G. Penn, Managing Director Kilrush Consultancy Ltd:**
"Gala Technology's SOTpay product is the first solution I have seen that makes achieving and maintaining PCI DSS compliance much easier for merchants and also more cost effective in maintaining compliance. My experience so far with SOTpay is a significant reduction in the time, effort and cost of achieving and maintaining PCI DSS compliance.

In addition, from a cards perspective, completely separate from PCI DSS, SOTpay provides significant benefits to the other stakeholders in the card payment ecosystem:


• The Issuer benefits from a significant reduction in fraud, because for the first time the card is authenticated in a MOTO payment.

• The Acquirer benefits from a significant reduction in fraud in its merchant portfolio, because for the first time the card used in the MOTO payment can be authenticated.

• The merchant benefits from significantly reduced processing and compliance costs and total elimination of fraud related chargebacks.

• The cardholder benefits, in that because the card payment is "secured" the goods and or services can be delivered to third party addresses."

Gala Technology is committed to ensuring that all merchants, regardless of whether they are an SME or multi seat contact centre, can use the SOTpay solution to reduce card processing costs, combat fraud/cyber risk and help support compliance with the Payment Card Industry Data Security Standard, cost effectively. ●

# **Enterprise Recon from Ground Labs:** Taking the pain out of finding sensitive data

**Hackers can't steal personal data if you do not store it. However, discovering exactly what you have and where it is, is no easy task. This solution allows firms to prove their capabilities pre-purchase and then help with PCI DSS and GDPR compliance.**

**Enterprise Recon from Ground Labs helped this major UK retailer:**

- Recognise the challenge of finding sensitive data and dealing with the new GDPR legislation
- Accurately test the effectiveness of Enterprise Recon
- Save money by making an informed decision

**Background**

The client was one of the UK's top retailers with over 1,400 stores nationwide and more than 180,000 employees.


**The Challenge**

To stay one step ahead of the new GDPR legislation, the retailer's information security team determined that the organisation needed to augment their current security mechanisms to find sensitive data and deal with the challenge of GDPR. After an extensive review process, they decided it would be necessary to implement a new security strategy in line with article 25 of GDPR, Data Protection by Design and by Default.

They knew they could not make a solution purchase decision without being able to technically evaluate the product and prove a return on investment to the business.

Based on their years of experience of testing new technologies they needed to evaluate the technology pre-purchase as well as post-deployment. This meant scoping out their own requirements during the proof of concept (POC).

"Testing the product is the only process that allows us to verify the potential impact of the scale of sensitive data


hidden within our network," explains the Information Security Manager (ISM).

The POC allowed them to see how effective the software would be in helping them to handle parts of the GDPR legislation such as a Subject Access Request, (SAR) that previously caused significant challenges.

The team had conducted manual SARs in the past but were unsure their manual process captured all the data they required.

"It was an arduous and painstaking process to manually evaluate our entire network and systems. It was time consuming and not practical to scale. We needed a piece of software that would automate and speed up the process," explains the ISM.

One of the requirements of the solution was to track and trend the data over time. This would give the business a detailed view of how much sensitive data was at risk and how much it had been reduced through regular scanning and remediation.

**The Solution**

To solve their problem the retailer turned to Ground Labs and its flagship product, Enterprise Recon, the first comprehensive, sensitive data discovery product that allows companies to discover, monitor and remediate sensitive data across their systems and network.

The product enabled the customer to replace the inconsistent manual searching methods they had used previously with a professional, state-of-the-art, automated data discovery solution.

**Enterprise Recon helped the UK retailer to:**

- Evaluate and test the effectiveness of their capability to discover and remediate financial data across their systems.
- Create specific user permissions for each department head giving them control over their area. It allowed them to manage their data and start to track the areas of the business that needed attention and resources.
- Save hundreds of thousands of pounds by helping the firm make business decisions that reduce risk and aid them with privacy law compliance.

**"We now have effective software that allows us to validate to the business the importance of an effective tool to find sensitive data where it resides."**

*Information Security Manager*

**The Result**

By having the ability to regularly search its entire network and systems for sensitive data, the company now has a tested tool for its PCI compliance and also will satisfy the commission that it has taken adequate steps to comply with GDPR, at the same time freeing up departmental time and money for other projects. ●

# **Pay360:** Giving control back to the fraud team

**The problem with many third-party fraud solutions is the lack of control they give users. Pay360's Optimize solved this client's problems.**

**The challenge**

Go-Ahead is a transport company with 38 years' experience working in the bus and rail industry. From overseeing franchises including London & Southeastern Railway and Govia Thameslink Railway, to managing companies overseas, Go-Ahead wishes to ensure it addresses security- and fraud-related challenges using the most effective solutions to ensure protection, with customer experience paramount.

With an ever-increasing fraud activity within e-commerce, Go-Ahead was observing various symptoms of fraudulent activity on their account. This was consuming significant time and resource for Debs Mayne, Group Retail Fraud Prevention Manager, and her team. They were incurring costs as well as seeing a reduction in conversion rates, impacting revenues as a result.

**"In one month we saw a 54% increase in stopped fraudulent activity using the Optimize tool and we've continued to see a consistent amount of declined fraud every month since."**

*Debs Mayne, Group Retail Fraud Prevention Manager, Go-Ahead*

Previously Go-Ahead was using a fraud tool which was more limited in its capability. Whilst successful in identifying fraudulent transactions, the tool didn't give Debs the control she needed to manage the rules herself to adapt to their risk appetite. Any changes had to be requested via a third party, which caused delays to the implementation of those requirements.

Debs manages all aspects of retail fraud at Go-Ahead and explains the problems they were facing: "We had to alert the external team that we'd spotted some suspicious activity, and then they had to apply a new rule to resolve this on our behalf."

**Optimize – a unique fraud and risk platform in the cloud**

Pay360 by Capita provides flexible, secure payments and revenue optimisation solutions to a wide range of global private and public sector markets. From payments collections which use artificial intelligence, to cutting-edge fraud and risk management, Pay360's solutions are designed to increase conversions and revenue whilst improving customer experience.

Optimize is a comprehensive identity and fraud management suite, split into modules so companies such as Go-Ahead can tailor the cloud solution to meet their evolving requirements as their business grows.

After trialling Pay360's Optimize fraud and

risk software, Debs could see instantly what the rules were doing, and the impact they would have once implemented. Go-Ahead was impressed with Optimize and decided the solution would resolve the challenges they'd had in the past and increase revenues.

Debs had confidence in Optimize because she could see immediately how it would help the company reduce fraud and chargebacks. She explains: "I knew it was effective and that it would work as I could see how the rules applied to live data. It was clear that chargebacks would reduce over time and I was confident it would be successful."

**Implementing the solution**

In January 2018, Go-Ahead deployed Pay360 Optimize Rules Management System into their live environment to reduce chargebacks and increase the frequency of detecting fraudulent orders.

The Optimize integration, originally part of a pilot scheme, had required next to no API coding changes: the Optimize Rules Management interface was available on Go-Ahead's management information portal, and rules were able to be generated and activated seamlessly within the Optimize interface. Pay360 also provided training seminars to ensure the Go-Ahead team felt absolutely confident navigating the solution.

**Ensuring bespoke rules which met Go-Ahead's specific needs**

Optimize features a particularly powerful fraud rules engine, enabling customers to build payment acceptance rules to suit specific scenarios, from simple checklists to complex strategies.

Account manager Bart Leonard of Pay360 explains why this makes such a difference

to Go-Ahead: "By empowering Debs to build acceptance rules herself, she has the control to create and change rules to suit the evolving needs of Go-Ahead, ensuring that the rules meet their risk appetite at any particular time."

Introducing a set of fraud rules which dictated acceptance of transactions was quite unprecedented for Go-Ahead's day to day processing, so the activation of any rules needed to be carried out carefully and meticulously. The intuitive user interface of Optimize, combined with the ability to set production rules into a live test mode, offered Go-Ahead the greater level of control they were looking for:

Bart adds: "Being able to make use of the test mode, where Debs and her team could allow Optimize analytics to run on Go-Ahead's live transactions volume, without actually having a bearing on the transaction authorisation, made a huge difference, both in practical terms and in helping the Go-Ahead fraud team build up confidence in their rule parameters. The system was also user-friendly which ensured a streamlined, seamless process."

Throughout the pilot phase, a dedicated Pay360 fraud consultant liaised with Debs and her colleagues regarding the initial setup of a few low complexity velocity control rules which were centred around 24

hour consumer spend restrictions against the same email address, weekly transaction count restrictions against the same email address and so on.

Pay360 then extended the scope of the Optimize rules engine to govern acceptance of 3D Secured transactions which didn't grant chargeback liability shift for Go-Ahead to mitigate any non-genuine transactions. Go-Ahead configured the rule to reject any transaction which did not qualify for liability shift and obtained an aggregated score of more than 7.5.

Go-Ahead then applied this rule to their busy Gatwick Express account, minimising the possibility of fraudulent orders slipping through the net unnoticed, which had been the case historically. Those rules were so effective, they're still in place to this day.

**"Our chargeback levels have reduced significantly since using Optimize - between £3-4k per month on average below the previous threshold."**

*Debs Mayne, Group Retail Fraud Prevention Manager, Go-Ahead*

**More informed fraud decisions**

Debs is able to look at the data and see real-time fraudulent activity based on the patterns identified. Not only does Optimize allow her to run rules in test mode before taking them live, but she can also create targeted rules designed to decline more fraudulent activity.

Debs explains: "Optimize enables us to be more proactive than ever before. We can make more informed decisions when managing rules, and even trial them before implementing on live data. Now Go-Ahead can tailor custom rules for transactions to determine whether to accept or reject them according to our risk appetite."

**The impact: fewer chargebacks and over 50% reduction in fraudulent activity**

The flexible, powerful rules engine of Optimize makes fraud detection easier for Debs, but it has also led to a significant drop in chargeback levels, where the issuing bank withdraws funds previously paid to Go-Ahead following an unauthorised transaction. The reduction in chargebacks is hugely positive for the company, as chargebacks are costly and expensive to defend.

The subsequent saving for Go-Ahead has been significant: "Our chargeback levels have reduced significantly since using Optimize - between £3-4k per month on average below the previous threshold," says Debs.

And this wasn't the only change that Go-Ahead saw after implementing Optimize, as they experienced a remarkable decline in fraudulent activity:

"Once Optimize went live, we knew we'd see an increase in declined fraud. In one month we saw a 54% increase in stopped fraudulent activity since using the Optimize tool. I thought the reduction in chargebacks would take time, but we saw this reduction almost immediately, and we've continued to see a consistent amount of declined fraud every month since," says Debs.

**A two week snapshot of the impact**

During a two week period from 23 March to 8 April, Optimize Rules stopped £76,790 in fraudulent GTR transactions which represented a 34% increase in fraudulent transactions which were stopped as

compared to the service previously used by Go-Ahead. During the same 2-week period, Optimize Rules stopped £75,640 of fraudulent transactions, representing a 60% increase in stopped fraudulent transactions compared to the previous service.

Overall for that two-week period, the Optimize Rules module prevented an additional £152,431 of fraudulent transactions from being processed which represents a 44% increase in successful stopped transactions compared to the previous service. Extrapolating these numbers over a year would result in an additional c.£1.8 million of fraudulent transactions being prevented or approximately £6 million in total value.

**Market-leading tools for enhanced decision-making**

The Optimize pilot delivered to the agreed objectives of reducing the levels of fraud happening across their online payment channels, reducing the amount of chargebacks received and increasing conversion. This was all in the timeframes agreed with Go-Ahead.

Go-Ahead has been so impressed by the clear, evidenced impact of Optimize that, following the pilot, they've contracted with Pay360 to utilize Optimize for the remainder of their contract periods with the train operating companies they service.

For Go-Ahead, the Optimize fraud and risk management tools complement the payment options they offer to their customers, including the online payment system provided by Pay360 which enables them to process online transactions securely.

Debs is also looking forward to making use of some of the wider Optimize suite, including Data Studio and new analysis tools to be able to analyse data more quickly and make even more of an impact in the fight against fraud.

Stephen Ferry, Managing Director, Pay360 talks about the new tools: "We're very excited about having developed new tools to really transform decision-making, using dashboards and a unique form of analytics. Visually-appealing dashboards quickly make sense of huge amounts of customer information whilst our market-leading risk mining tool highlights hidden relationships and customers' behavioural footprint by visualising data as a 360° view. This tool is the first of its kind, using interactive, real-time data visualisations to allow analysts to uncover fraudulent behaviour instantly."

Optimize encompasses multiple data sources to select from when creating bespoke rules. Thousands of unique data points are available for global intelligence gathering, social media analysis, know your customer (KYC), anti-money laundering (AML) and enhanced identity verification (ID&V) to expose suspicious behaviour as early as possible. The Optimize suite also features an automated workflow management system which makes it easier for teams to work within service level agreements for time-sensitive, business critical work by enabling the prioritisation of deferred tasks, even across global teams. This helps teams become more efficient, high value tasks can be resolved more quickly and operational costs are reduced.

**In summary**

Optimize is a powerful tool for Go-Ahead to equip their fraud and risk team with what they need to easily uncover and reject suspicious activity, ensuring better, faster business decisions which have resulted in quantifiable reduced chargebacks and increased revenue. ●

# **PCI Pal:** Transforming telephone transactions

**Regulation and the threat of financial penalties focused iFLY's attention on its call-based card transactions. The company chose PCI Pal to ensure compliance without impacting the customer journey.**

**Who is iFLY?**
iFLY is the leisure company that created modern indoor skydiving. The company started trading in 2005, having created a stable wall-to-wall cushion of air in a flight chamber, which offers a realistic and safe indoor skydiving experience. Today, iFLY has helped over 50,428 people experience the thrill of skydiving from one of its 69 locations around the world. This includes three sites in the UK – Basingstoke, Milton Keynes and Manchester – in addition to centres in the US, Canada, Europe and Asia, with more sites to follow as demand continues to grow.

**The compliance challenge**
iFLY takes its customer service seriously, in order to provide a consistent quality of service to every customer. The team of eight customer services agents handle upward of 30,000 inbound calls every year, and this number is increasing.

With every call being recorded for training and monitoring purposes, the management team was aware that it needed to change the way payment card transactions were being manually handled over the phone to comply with the Payment Card Industry Data Security Standard (PCI DSS).

Explains Alyson Williams, Finance Manager – Group for iFLY: "One of our challenges was to ensure we became PCI DSS compliant. At the time, we were manually capturing and inputting card details to our system, without pausing the call recording, and we knew this had to change."

"Regulation got us focused: failure to comply would create financial penalties across the entire business, which would be significant."

"We needed to identify a solution that would enable us to maintain our call recording process yet provide a safe and anonymous way for customers to provide their payment information – and importantly, without impacting the overall customer experience."

**How PCI Pal solved iFLY's PCI issue**
iFLY took the decision to identify a partner to manage its call centre payment card security and was recommended to contact the team at PCI Pal for help.

Matthew Lippert, Assistant Manager of iFLY said: "We needed to find a way of continuing to record our calls without the fear that we'd captured sensitive card data. I would complete online certificates to show compliance for our online business, and began to realise that we were no longer compliant because of the call centre. Help was needed and we were recommended by a consultant to contact PCI Pal."

The PCI Pal Agent Assist solution enables call centre agents to securely capture payment card data using DTMF (Dual Tone Multi Frequency), while the agent maintains full conversation with the customer.

Agent Assist integrates with the call flow and, at the point of payment, intercepts the telephone keypad tones as they are entered by the customer. This means the call handler doesn't hear or see the card data, yet the customer and agent can still have a conversation throughout the process but the sensitive card data is prevented from reaching the agent or iFLY's environment.

Continues Alyson: "For us, PCI Pal's Agent Assist was a sensible solution. Not only would it mean we were compliant, but it also integrates with our existing call centre systems and payment providers meaning we didn't have to make dramatic changes to our existing working processes."

"There was no re-engineering of our call handling or system upgrades. Instead, we've been able to integrate Agent Assist and deliver a seamless call flow for both our customers and our call handlers."

**The results**

When asked to consider the results achieved by implementing PCI Pal's Agent Assist, Alyson is quick to respond: "When completing the annual PCI Self-Assessment Questionnaire, we've gone from being Certificate D, to the highest Certificate A for our PCI compliance. This gives us peace of mind that we are compliant and not living in fear of financial fine implications."

She continues "The Agent Assist platform is easy to implement, easy to use and creates less work for the team. Taking


payment card details over the phone has become more efficient and we haven't had to make changes to the way our team operates or make any major adaptations to any of our systems."

Feedback from customers has also been positive, as Matthew adds: "Anecdotally, customers are commenting on inputting their card details on their keypad as a positive step. It's something people are becoming used to doing and with financial security being a priority for consumers, they are happy that we can demonstrate just how secure our systems are." ●

**"The Agent Assist platform is easy to implement, easy to use and creates less work for the team. Taking payment card details over the phone has become more efficient and we haven't had to make changes to the way our team operates or make any major adaptations to any of our systems."**

*Alyson Williams, Finance Manager – Group for iFLY*

# **Semafone:** The Caravan and Motorhome Club cruises to compliance

**The Caravan and Motorhome club needed a call centre PCI DSS Solution that delivered compliance while maintaining a seamless customer journey. Semafone delivered.**

**Background**
The Caravan and Motorhome Club, formerly known as The Caravan Club, describes itself as the largest touring community in Europe. The membership organisation was founded in 1907 and offers everything from campsites, yurts and holiday cottages to events, training, insurance and worldwide holidays. Members are able to pay for their subscriptions and these additional products and services using a variety of methods including direct debit, online payments, face-to-face transactions, or over the phone.

**"We liked the functionality of Semafone's solution and the company had an impressive roster of customers who already had the system and were able to testify how easy it was to implement and use."**

*Jon Laws, Financial Controller of the Caravan and Motorhome Club*

**The Challenge**
The Caravan and Motorhome Club has a centralised UK contact centre in East Grinstead, West Sussex, that employs around 110 agents to handle customer queries and take payments for products and services. The organisation handles thousands of calls every day, but the exact number is subject to seasonal variations in demand. Surges frequently occur in January, when members begin to think about booking their overseas holidays, and in March and October when many call to renew their insurance policies. When members phone in to make an enquiry, it is important to the Club that they are able to make a payment on the same call, without the need to be re-directed to another individual or an automated process.

In regular contact with its membership, the Caravan and Motorhome Club has to ensure that all of its communications are compliant with the European General Data Protection Regulation (GDPR) and that the privacy of its members is respected. With so many payment transactions taking place through the contact centre, the Club also has to comply with the Payment Card Industry Data Security Standard (PCI DSS). This applies to all payment methods made by card but is particularly challenging when it comes to telephone payments as the Caravan and Motorhome Club records all its phone calls. PCI DSS specifically

prohibits the capture of any sensitive card data on call recordings and requires strict security controls on sensitive payment data that passes through the contact centre. The Club had implemented tokenisation, which helped to achieve compliance through other channels, but telephone payments were still in PCI DSS scope.

**The Solution**

The Caravan and Motorhome Club looked at a number of options to resolve the compliance challenges for telephone payments, including Pause and Resume solutions that stop the call recording while the card numbers were read out by the customer. However, this method was discounted as there was a danger of pausing the recording at the wrong moment. Moreover, the final recording would not constitute a complete record of the call, making it inadmissible as evidence in the case of a dispute.

After a thorough review process, the Club chose Cardprotect from Semafone

to secure their telephone payments. Using this solution, members input their payment card details directly into their telephone keypad. The numbers are obscured from the contact centre using dual tone multi frequency (DTMF) masking. So, while it's impossible for agents to hear or see a member'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. Cardprotect sends payment card numbers straight to the payment service provider (PSP), completely bypassing the Club's internal contact centre IT infrastructure. Fully scalable, the solution can easily cope with the Club's demand peaks to ensure every payment is taken securely.

"We liked the functionality of Semafone's solution and the company had an impressive roster of customers who already had the system and were able to testify how easy it was to implement and use," said Jon Laws, Financial Controller of the Caravan and Motorhome Club. "Our one million membership base is comprised of people from all ages and technology awareness and abilities, so we chose a system that wouldn't pose a barrier and put them off paying over the phone."

**The Implementation**

Cardprotect was installed onto a Gamma platform, integrating with Avaya IPI telephony system. Semafone, Gamma and the Club worked collaboratively to ensure that it all came together smoothly. "It was sometimes tricky to co-ordinate, and as always, testing highlighted a few issues, but nothing that wasn't resolved easily," said Jon. "Semafone's team was on hand to help and the implementation was relatively incident-free. Training the agents to use the system was


straightforward because of its simplicity, and we made sure that everyone received the right support as it went live. With both our agents and members happy using Cardprotect, Semafone got a big thumbs up from our contact centre manager."

**Benefits**

The Caravan and Motorhome Club's top priority is its members, so one of its biggest concerns was that the new system would be accepted by people making payments. "We were delighted by how fast our members took to it," said Jon. "We've had very few complaints, and I think they are aware the new system is helping to keep their payment data safe. For us, the whole implementation was as much about looking after members' data responsibly as it was about PCI DSS compliance. And while no system is a panacea for the EU GDPR, Semafone has certainly taken care of the problem of storing card data."

**"We made sure that everyone received the right support as it went live. With both our agents and members happy using Cardprotect, Semafone got a big thumbs up from our contact centre manager."**

*Jon Laws, Financial Controller of the Caravan and Motorhome Club*

Agent productivity is enhanced by the Semafone system as it allows them to carry out additional tasks, such as filling in notes and updating records while the member is inputting their details. It has also meant that calls are often shorter because the numbers no longer need to be read out loud before being entered. The fact that the system is cloud-based, using Gamma's SIP infrastructure, not only ensures that no card data ever enters the contact centre, but means that it's easy to add more agents if needed, to accommodate increased demand.

**Future plans**

The Club is looking into further possible applications for Semafone and considering what other personal information the system may be able to protect. Top of the list are bank account details, and the organisation is already in discussions with Semafone about finding ways of securing these in the coming months. ●

# Forthcoming events

| | | | |
|---|---|---|---|
| e-crime & cybersecurity CONGRESS<br>5th & 6th March 2019<br>London | e-crime & cybersecurity CONGRESS<br>19th March 2019<br>Dubai | e-crime & cybersecurity FRANCE<br>April 2019<br>Paris | e-crime & cybersecurity SCOTLAND<br>1st May 2019<br>Edinburgh |
| e-crime & cybersecurity GERMANY<br>18th June 2019<br>Munich | PCI LONDON<br>3rd July 2019<br>London | e-crime & cybersecurity CONGRESS<br>17th September 2019<br>Abu Dhabi | |
| SECURING THE LAW FIRM<br>18th September 2019<br>London | e-crime & cybersecurity MID-YEAR<br>17th October 2019<br>London | SECURING ONLINE GAMING<br>17th October 2019<br>London | |
| e-crime & cybersecurity SPAIN<br>21st November 2019<br>Madrid | e-crime & cybersecurity NORDICS<br>27th November 2019<br>Stockholm | e-crime & cybersecurity BENELUX<br>3rd December 2019<br>Amsterdam | |

For more information, please call Robert Walker on +44 (0)20 7404 4597
or email robert.walker@akjassociates.com

# **Silver Lining:** Compliance in the cloud

**This highly-regulated client was looking to find a solution which left them entirely removed from the management of the solution, and also allowed flexibility, scalability and ease of integration with multiple sites.**

Silver Lining Convergence have had the pleasure of working with one of the UK's largest independent vehicle insurance brokers for a number of years. Established in 1998, this broker now turns over in excess of £130 million a year. They handle over 1.2 million calls a year and maintain relationships with over 20 of the leading and most trusted insurance providers. They are multi-award winning, and remain in a near constant state of evolution, continually staying abreast of the latest developments in technology and being mindful of the ways customers shop for insurance.

As an FCA regulated insurance company, this broker is required to record all phone calls – including card transactions – taken over the phone. This posed a number of compliance and data security challenges due to the sensitive nature of the data being held, as well as being listened to by the call handler. The executives of the company were concerned that they needed an electronic payment system that would be efficient and easy to manage, as well as one that would be accepted by their staff of trained professionals. The system needed to be cost-effective, and able to integrate with their existing ICT estate with minimal disruption to their customers.

In 2016, Silver Lining worked with the broker to provide a solution which would reduce PCI-DSS auditing scope for credit and debit card payments, removing the requirement for costly security measures, whilst ensuring the company met the conditions issued by their payment provider. Our solution used software which integrates seamlessly within the payment process and masks the DTMF tones with inaudible flat tones. While speaking to an agent, customers input their credit and debit card details via their phone's keypad. The number is not visible or audible to the agent and therefore cannot be recorded or stored.

Since this solution was implemented, the business has processed millions of calls with the peace of mind that their customers' card data is entirely secure. They meet both PCI and FCA requirements, and without any disruption to their customers.

As time went on and due to further expansion through acquisition, the broker was looking to find a solution which left them entirely removed from the management of the solution, and also allowed flexibility, scalability and ease of integration with multiple sites. The business had been growing at an exceptional rate, and this left issues with integrating the PCI-DSS solution within the ever-growing Multi-Protocol Label Switching (MPLS) network.

Like many businesses, this broker had been making the move from ISDN lines

to SIP trunking, ahead of BT's decision to switch off the ISDN networking in 2025, and were looking for a new solution which could integrate with their new SIP trunks. The task at hand was not an easy one: the business had over 1,500 channels which needed readying, and it was imperative that they experience little to no disruption to usual business activities.

Silver Lining has been offering their PCI-DSS product via their 4th generation cloud platform for a number of years, and we have already seen a large number of businesses adopt this solution, either via their existing channels or supplied by ourselves. The cloud platform itself is entirely owned and operated by us – from our transit layer as an internet service provider (ISP), right through to application layer. This level of total ownership means we are able to guarantee security and uptime for all of our customers – for example, all four of our data centres are UK-based, and we give a 99.99% uptime guarantee.

When this broker entered the planning stage for the project, we proposed our PCI-SIP product to them, and created a thorough roadmap for their peace of mind. After recently gaining level 1 PCI-DSS compliance for the product, we were able to prove the merits of taking the management of their solution out of house, and over to us as a cloud-based operation. The move to cloud also offered another benefit – the move from a capital expenditure to an operational one. This presented a more economical 'per-channel' based pricing model, and streamlined the onboarding process for new sites.

Implementation is planned to commence in Q1, 2019 and will be undertaken swiftly and out of hours to ensure minimal business disruption. As the user interface remains unchanged for the agents, there will be no requirement for additional staff training and once up and running, operationally, it will be 'business as usual'.

The existing on-premise hardware will be left on site, instead now being used as local survivable gateways, should there be a carrier outage on their SIP trunks. This means maintenance and management of the on-premise solution will be negligible with regards to cost.

"The key consideration here was to go with one supplier who could deliver the entire solution end-to-end," explains the business' Head of Telecommunications. "We needed a solution that reduced PCI compliance directives, which was able to sit within our SIP trunks. We chose Silver Lining for this project, having previously worked with them, as we actively wanted to work with a long-term strategic partner who could support us on our journey. Our ethos has always been to utilise all available options for us, including technology, to deliver the best for our customers. Silver Lining echo these values, so understand how important it is to us to minimise any sort of disruption, and to streamline costs and processes wherever possible. They continue to deliver on our requirements, and, indeed, often exceed our needs." ●

**"Silver Lining understand how important it is to us to minimise any sort of disruption and they continue to deliver on our requirements and indeed, often exceed our needs"**

*Head of Telecommunications*

# **Sysnet:** Supporting Cardnet's proactive approach to PCI compliance

**Lloyds Bank Cardnet has been providing businesses with card payment services since 1997. It handles more than one billion transactions a year across approximately 70,000 card terminals.**

Cardnet has taken a proactive approach to payment card data security and compliance for small to medium sized merchants, making it easier for these businesses to achieve compliance with the Payment Card Industry Data Security Standard (PCI DSS) via self-service or managed service options.

Cardnet has worked with Sysnet Global Solutions in support of their compliance management programmes since 2010. In July 2017, Cardnet piloted a concierge service called Compliance Plus based on Sysnet's Proactive Data Security (PDS) technology to assist merchants considered at most risk of a data breach.


The scope of the pilot was extended in December 2017 following positive feedback from users and after a second positive evaluation in early 2018 the programme was extended to cover the majority of Cardnet customers.

**Helping merchants find the right solution**

Cardnet are aware of the impact a payment card data breach can have on merchants and offer a range of options to help merchants report, attain and manage their PCI DSS compliance and help ensure their payment card data environments are secure. Cardnet provide merchants with three options to report and manage their PCI DSS compliance.

Firstly, they can take responsibility for selecting the appropriate Self-Assessment Questionnaire for their needs and uploading this to the Cardnet PCI portal at no charge.

The second option is Cardnet's chargeable online service, where

profiling questions are used to determine the appropriate Self Assessment Questionnaire for the merchant and guide them through the relevant security controls they require for compliance. These merchants also have access to additional information and guidance on the Cardnet PCI portal.

The third option is Compliance Plus which is a proactive data security service that secures key areas of risk in a prioritised way.

**Limiting non-compliance — a key strategy**

Limiting non-compliance with the PCI DSS is a key objective for Cardnet. If a merchant is non-compliant with the PCI DSS and experiences a data breach they are liable to receive significant penalties from the Card Schemes, and for smaller merchants there is a risk this could put them out of business.

Compliance Plus can help Cardnet customers ensure they have effective data security measures in place to reduce the risk of losing payment card data and avoid non-compliance charges and penalties.

**"PCI non-compliance charges can be an effective short-term mechanism to drive PCI programme engagement and compliance. However, as our PCI Sentiment Survey indicated, they should not be used as a long-term solution. Cardnet are to be commended in their refusal to tolerate non-compliance and benefit from non-compliance charges."**

*Gabriel Moynagh, CEO at Sysnet*

The solution is of value not just to those aiming to achieve and, importantly, maintain PCI DSS compliance, but also to those who see the value in the additional features of the product such as anti-virus, software patches and proactive record updating and task management. ●

# **TokenEx:** Securing digital transformation

**Most payment tokenisation providers focus on tokenising PCI and cannot or will not tokenise personal data. TokenEx's flexible, open tokenisation goes further.**

Through honesty, service, and a willingness to pay it forward, Discount Tire has always strived to provide unexpected experiences that delight their customers to keep them coming back for automotive products and services. In fact, many of their customers have been buying and servicing their tires at Discount Tire retail outlets for literally generations. Valuing their customer base and working to improve the patron experience even more, Discount Tire wanted to drive a digital transformation to a paperless financial application process. The goal was to make applying for in-store credit and loans easy and fast for both customers and retail staff, while keeping both the payment card information (PCI) and customer personal data out of the point-of-sale and back office systems.

In addition to increasing customer satisfaction and sales, the initiative received C-level executive support from both a business and security standpoint. Keeping customers top of mind, and in light of recent high-profile data breaches and global privacy regulations such as the General Data Protection Regulation (GDPR), Discount Tire's founder, Bruce T. Halle, gave his executives two security directives:

- Keep Discount Tire customer data safe, and
- Keep Discount Tire out of the headlines about anything related to data breaches.

Like many organisations, Discount Tire was already securing payment data to be compliant with the Payment Card Industry Data Security Standards (PCI DSS). The process of being PCI DSS compliant can be costly and time consuming. However, by using encryption, tokenisation, and cloud data vaulting, an organisation can remove customers' PCI data from their business systems, reducing the scope and cost of their PCI compliance efforts as well as the risk of data breaches that expose customer personal data, resulting in fines, lawsuits, and lost business.

Initially, Discount Tire used encryption and tokenisation for their point-of-sale PCI data by implementing P2PE devices and data management services supplied by their Verifone Point Enterprise system. However, they realised that completing a sale often requires both a credit check and an application for obtaining Discount Tire's private label credit card – or qualifying for a low-interest loan from a third-party financial provider. To efficiently process a credit application, Discount Tire needs to collect a minimum of: name, address, phone number, social security number (SSN), income, date of birth (DOB), as well as an image of the customer's signature. To hackers this is very valuable personal data that can be used for a variety of fraudulent endeavors, providing an enticing target for data theft.

At the Discount Tire retail stores, too much time was being spent by customers filling

out paper credit applications, which were then hand-keyed by employees into the point-of-sale system, thereby exposing sensitive customer personal data to employees, as well as storing it in internal business systems.

After this process, the personal data was transmitted to Discount Tire's financial partners for approval and a credit amount, but there were many potential breach points in the data flow.

Evan Hunter, Project Manager of Payments and Finance at Discount Tire, recognised there was an opportunity to streamline, and at the same time secure, the loan approval process, making it easier for customers to apply for Discount Tire's private label credit card or other low interest loans; automate the data entry process; eliminate employee handling of sensitive personal data; and remove personal data from Discount Tire's internal systems to reduce the risk of data breaches.

**Beginning the digital transformation of credit application**

The first phase of the digital transformation involved working with Verifone to design, test, and pilot a new interface called Quick Credit App that would capture at the POS terminal some of the high-value personal data – such as SSN, income, and DOB – needed for a credit application. This would be combined with customer information from Discount Tire's systems, such as customer name, address, and phone number, to complete a loan application.

The combined data could be encrypted and transmitted to the financial partner for a credit decision and, for a new customer, a credit card number. However, the process still left considerable personal data in Discount Tire's business systems. Hunter reflects on this challenge: "Do we really need to store all the personal data we collect from customers? While we use that data to provide the best customer experience possible, to understand the life cycle of the tires we sell, and the types of products our customers need, we really should not be storing it. We are experts in retailing and customer service. We are not an IT security company. I've always followed the adage, the philosopher leaves the cut of his sleeves to his tailor. We should not be in the business of trying to securely store PCI or personal data." Since the Verifone system already tokenised PCI and vaulted it with the processor, the challenge was to also tokenise, and thus pseudonymise the personal data collected for credit approvals to reduce the risk of exposing customer data, yet still have the associated tokens for use in business processes, marketing, and analytics.

**"The open integration capabilities of the TokenEx platform are essential to making these kinds of transformations possible."**

*Evan Hunter, Project Manager of Payments and Finance, Discount Tire*

What Hunter and his team needed was a tokenisation provider that could integrate seamlessly with their existing POS system, payment processors, financial credit providers, and safely tokenise and vault the personal data.

However, almost all payment tokenisation providers focus solely on tokenising PCI and cannot or will not tokenise personal data. A flexible and open tokenisation

provider can tokenise any data type and that's the capability that Discount Tire was searching for when they launched the second phase of the loan application implementation.

**A collaborative approach to data security**

Hunter talks about the search for the right security provider for their personal data pseudonymisation project: "When Discount Tire looks for security partners, we look for proof of business continuity, indemnification of loss, the ability to be added as insured under their cyber-risk policy, and the ability to hold both the data being stored and the tokenisation platform itself in escrow.

"When you meet a potential partner that can meet those stringent criteria, we know that they are confident in their solution and their business. TokenEx met all those requirements for a data security partner. After talking with the team at TokenEx, discussing in detail our problem and possible solutions, as well as interviewing their existing reference customers, we knew they were very capable of protecting their customers' data and so by extension, our customers' data."

With TokenEx selected as the tokenisation platform for personal data, the two teams quickly defined the architecture and integration points. It was a collaborative development experience for both Discount Tire and TokenEx: bringing ideas to the whiteboard, refining integration and data flows, and agreeing upon an implementation plan. Together the teams built a cutting-edge secure system for entering, transmitting, and storing personal data that would flow from Verifone POS devices, to TokenEx, to the financial lending partners and back.

**An open platform for integration is key to smooth digital transformation**

One key step that required a special integration was in processing a new application for a Discount Tire branded credit card. The goal of this integration is to capture the personal data via the Verifone Quick Credit App, send it to TokenEx to be vaulted and converted to tokens for later use in Discount Tire's systems. TokenEx sends the encrypted "real" data to the financial providers, who then send the approval and credit limit through TokenEx back to Discount Tire so the sale can be completed.

However, in that returned data is also a new credit card account number for the Discount Tire branded card. Discount Tire did not want to store the PCI – something they had just worked hard to get rid of – so TokenEx also collects that number from the financial provider, sends it to the Discount Tire processor for tokenisation, and sends the token to Discount Tire for future use.

This smooth integration works with any financial provider because TokenEx is an open integration platform and is payment processor and financial institution/lending platform agnostic.

Another sign of openness in the TokenEx Cloud Security Platform is the freedom of data ownership. TokenEx clearly states that all data stored in the TokenEx Cloud Secure Data Vaults, as well as the tokens used to mask the data, belongs to the customer. TokenEx is the custodian of the sensitive data, and customers have full right to have it returned at any time. Other vendors license the tokens used in the tokenisation process and will not provide the token/data set pairs back to the customer. This is especially critical when storing personal data, as sensitive

customer information should always be detokenised and returned upon request. Hunter remarked: "The openness and flexibility of TokenEx's platform is an important part of our trust in their business ethics, along with the other requirements we had, it proves that TokenEx has their customers' best interest front and center."

TokenEx provides an open platform for data security, integration, and process improvement to create a seamless customer experience – with connectivity to multiple financial and payment providers, so that Discount Tire can service the full spectrum of consumers. Hunter thinks this is key to Discount Tire's business philosophy. "We believe that customers' driving safety is a top priority. However, a set of four tires is not a small investment for many working families, so having affordable financing options to get the right tires, at the right time, is a critical step in ensuring customer safety and satisfaction. TokenEx will enable us to work with a range of finance providers to get the best loan deals for our customers, quickly and securely."

**A quick route to improved customer experience and secure personal data**

The entire digital transformation of the customer credit experience came together in under five months – a remarkably short time for a project that other tokenisation service providers said could not be done at all. The initial contract with TokenEx occurred in April; the integrations were tested in June and certified in July. The new system went live in mid-August. "When we first started this digital transformation project, there was some doubt that it could be successful," states Hunter. "While Discount Tire has a history of implementing cutting edge technology, such as EMV and P2PE devices, this project was of a different order, involving not just technology, but intricate integrations among several systems and vendors. That we not only successfully completed the digital transformation of our credit and loan processing and secured the personal data, but did it in only five months, is testament to the collaboration between our internal team and TokenEx. It also demonstrates that the open integration capabilities of the TokenEx platform are essential to making these kinds of transformations possible."

TOKENEX
NO DATA. NO THEFT.

**TokenEx cloud security platform secures personal and all data types**

Many digital transformation projects include the need to secure sensitive data normally stored in an organisation's business systems. Whether the data is payment, personally identifiable, healthcare, or document/image-based, the risk of exposing it to data thieves can be eliminated through a combination of encryption, tokenisation, and cloud data vaulting.

The TokenEx Cloud Security Platform employs all four of these techniques to remove sensitive data from IT systems without disrupting existing business processes. The open integration capabilities of the TokenEx platform provide proven methods of securely moving sensitive data among business partners. With TokenEx acting as custodian, your data is always your data, with a no-caveat return policy should your business needs change. ●

# **Ultracomms:** Putting PCI DSS secure payments in the telephone network

**Businesses take a risk every time they ask a customer to read card details out over the phone. Can the information be overheard? Can the data be compromised?**

Despite the threat that card-not-present fraud is expected to rise to £68 million by 2021, 66% of businesses still take payments over the phone using outdated "Pause and Resume" methods, in which call recordings are stopped while card data is read out. (ContactBabel UK Contact Centre Decision Maker's Guide, 2017.) This practice is high-risk for both the business and the customer and is likely to be deemed non-compliant when the industry watchdog, the Payment Card Industry Data Security Standards Council (PCI DSS), issues its next update.

By far the most effective strategy for ensuring against card fraud is to ensure a business is never exposed to card data in the first place.

As a PCI DSS Level 1 certified service provider, Ultracomms has a range of flexible and scalable payment solutions which shield all personally identifiable card data from contact centre agents, agent desktops, VoIP and data networks and call and screen recording.

Delivered via the cloud, integrated with the telephone network, or installed locally, its PaySure solutions provide complete payment security for customers, while ensuring their experience is not compromised.

Ultracomms' PaySure on-demand voice transit platform provides network operators and service providers with a secure and flexible telephone payment processing capability.

Traditionally, this kind of technology requires a large investment with a lengthy and complex deployment cycle fraught with integration and interoperability issues. By commoditising this technology, delivering it as an on-demand trunk network service to merchants, PaySure is proving to be a truly disruptive product in this market.

**Six Degrees is a cloud-led managed service provider. It works as a collaborative technology partner to businesses making a digital transition. With a focus on compliant technology, Six Degrees provides cloud and managed hosting services, unified communications, managed IT services, security and analytics, EPOS, helpdesk and compliance support to customers across a variety of sectors including retail, legal, manufacturing, public sector and financial services.**

Six Degrees

Offering a comprehensive range of security solutions as part of its portfolio, Six Degrees has a proven track record of supporting organisations facing an increasingly complex and ever-changing security landscape. With escalating rates of cyber-attacks carried out by an ever more professional and organised cyber-crime fraternity, the business is well aware of the risks posed by cyber criminals.

Through working with a number of known brands in the retail, legal and financial services sectors with contact centre operations, Six Degrees was aware that many of them were handling payments, not just through e-commerce, but also over the telephone.

Six Degrees recognised that customers with contact centres where telephone payment processing was required needed a solution that maintained compliance, integrated seamlessly with their contact centre and call recording software, and allowed them to deliver the best possible user experience to their end customers.

Six Degrees was already working with Ultracomms to provide telephony and SIP trunking for their contact centre customers so the business was aware of Ultracomms' PCI DSS Level 1 certified cloud platform and PaySure secure telephone payment solutions.

Ultracomms was therefore a natural fit to deliver the technology behind LivePay, Six Degrees' secure payment solution.

Matthew Brouker, Group Product Director, Six Degrees, explains that "Our customers rely on us to deliver a high quality, highly resilient voice network, packaged as a single solution and built to meet their compliance requirements."

"Working with a PCI DSS Level 1 service provider like Ultracomms allowed us to quickly and seamlessly integrate with Ultracomms' cloud, with minimum up-front investment. The flexibility of the PaySure solution makes integration at the network level simple, and has given Six Degrees the opportunity to white label the secure payment solution within our own product portfolio as LivePay." ●

paysure

# Secure telephone payments, simplified

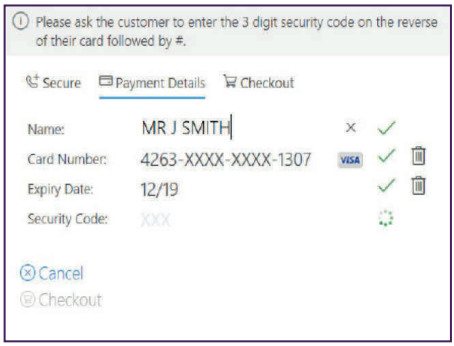
**Seamless integration**
Seamless integration is key for Six Degrees. Once deployed onto the network, the infrastructure is already in place so bringing new clients onto LivePay requires no additional investment in hardware, or costly integration work.

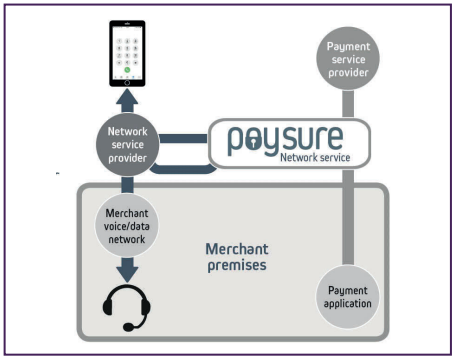
The beauty of this is that clients that are already using Six Degrees' telephony services just need to have their calls routed through the PaySure cloud in order to be able to handle their phone payments securely.

There is no need for the customer to make any changes to their existing call recording platform, and the solution is entirely platform agnostic. PCI DSS compliance will be achieved in the network, ensuring their business and their end customers remain completely secure.

**Simple and secure for customers**
The technology behind PaySure enables payments to be taken over the phone securely by masking card information. Customers are able to enter their card details using the phone keypad, avoiding the need to say them out loud to the contact centre agent and therefore removing the risk of their card information being overheard.

**The beauty of this is that clients that are already using Six Degrees' telephony services just need to have their calls routed through the PaySure cloud in order to be able to handle their phone payments securely.**




PaySure provides a secure web portal over which payments are processed, and customers enter their card details completely securely without the card information ever being seen, heard or stored in call recordings.

The agent is able to remain on the line to guide the customer through the transaction process, improving customer experience and reducing the risk of abandoned calls.

Without the need for the agent to pause or resume the call recorder, the entire call is recorded, ensuring a full audit trail is delivered, while remaining compliant with PCI DSS. ●

**Without sensitive card data ever entering the contact centre, the business is completely removed from the scope of PCI compliance. The risk of card data theft is removed, along with the potential for the financial and reputational damage that could occur as a result of a card data breach.**

The customer calls the contact centre to make a payment

The agent asks the customer to enter their card details via the telephone keypad. PaySure captures the card information removing the tones using Dual Tone Multi Frequency (DTMF) masking. The agent does not see or hear the details and flat tones are substituted so they are not recorded either.

PaySure verifies the card details with the Payment Service Provider. The agent is notified if the details are accepted or rejected. At any stage in the process the agent can cancel the transaction and start again while the customer is on the line.

**Ultracomms' PaySure on-demand voice transit platform provides network operators and service providers with a secure and flexible telephone payment processing capability. Designed for both direct and channel sales, PaySure's flexible and scalable technology enables it to be delivered as a trunk network service to its customers.**

- Enhanced value proposition for network operators and service providers
- Rapid on-demand provisioning, supporting software defined and programmable network environments for minimal time to deploy and self-service
- Clustered architecture across geographically diverse multiple points of presence, providing resilience and high levels of availability
- Ready-to-go user application and fully supported API integration options to seamlessly align with existing business applications
- High-margin overlay application to complement existing products and services
- Reduced cost of compliance and mitigated risk of a card data breach, removing the merchant operations from PCI DSS scope

- Call processing for distributed merchant operations (including homeworking and disaster recovery facilities) with a single solution
- Simple commercial model for seamless alignment with existing channel distribution models. ●

# Sponsors

**Blackfoot**
**Contact:** James Walker
**Email:** jamesw@blackfootuk.com
**Tel:** +44 845 805 2409, +44 7950 311 817
**Contact:** Matthew Tyler
**Email:** matthew.tyler@blackfootuk.com
**Tel:**+44 845 805 2409, +44 77755 07667
**Website:** www.blackfootuk.com
**Twitter:** @Blackfoot_UK

**CardEasy from Syntec**
**Contact:** Simon Beeching, Business Development Director
**Tel:**+44 7973 384496
**Email:** simon.beeching@syntec.co.uk
**Website:** www.syntec.co.uk
**Twitter:** @synteccontact

**Eckoh**
**Contact:** Tony Porter
**Tel:** +44 1442 458 460
**Email:** Tony.Porter@eckoh.com
**Website:** www.eckoh.com
**Twitter:** @Eckoh
**LinkedIn:** company/Eckoh-plc
**Facebook:** EckohPLC

**ECSC**
**Contact:** Clare MacDonald
**Tel:** +44 1274 736 223
**Email:** clare.macdonald@ecsc.co.uk
**Website:** www.ecsc.co.uk
**Twitter:** ECSC_Group

# Sponsors

**GalaTech**
**Contact:** Steven Jones
**Tel:** +44 1709 911 661
**Email:** sjones@galatechnology.com
**Website:** www.galatechnology.com
**Twitter:** @SOTpay

**Ground Labs**
**Contact:** Matt Jennings-Temple
**Tel:** +44 203 137 9898
**Email:** matt.jennings-temple@groundlabs.com
**Website:** www.groundlabs.com
**Twitter:** @Groundlabs

**Pay360 by Capita**
**Tel:** +44 333 313 7160
**Email:** Pay360digitalsales@capita.co.uk
**Website:** www.pay360.com
**LinkedIn:** company/pay360-by-capita
**Twitter:** @Pay360byCapita

**PCI Pal**
**Contact:** Jane Goodayle
**Tel:** +44 330 131 0342
**Email:** info@pcipal.com
**Website:** www.pcipal.com
**Twitter:** @pcipal

# Sponsors


**Semafone**
**Tel:** +44 (0)845 543 0822
**Email:** emeasales@semafone.com
**Website:** www.semafone.com
**Twitter:** @Semafone


**Silver Lining Convergence**
**Contact:** Sam Brown
**Tel:** +44 345 313 1111
**Email:** sam.brown@silver-lining.com
**Website:** www.silver-lining.com
**Twitter:** @silverliningUK


**Sysnet Global Solutions**
**Tel:** +353 (0)1 495 1300
**Email:** info@sysnetgs.com
**Website:** sysnetgs.com
**Twitter:** @Sysnetgs


**TokenEx**
**Contact:** John Noltensmeyer
**Tel:** +1 877 316 4544
**Email:** jnoltensmeyer@tokenex.com
**Website:** www.tokenex.com
**Twitter:** @TokenEx


**Ultracomms**
**Contact:** Liz Rawlins
**Tel:** +44 330 045 0777 or +44 7919 275070
**Email:** liz.rawlins@ultracomms.com
**Website:** https://ultracomms.com
**Twitter:** @ultracomms