AKJ Associates

PCI DSS: Case Studies in Excellence

Forthcoming events

3rd & 4th March 2020
London

10th March 2020
Dubai

1st April 2020
Paris

5th May 2020
Munich

8th July 2020
London

16th September 2020
Abu Dhabi

22nd September 2020
London

23rd September 2020
Stockholm

15th October 2020
London

15th October 2020
London

4th November 2020
Edinburgh

November 2020
Kuwait

17th November 2020
Madrid

1st December 2020
Amsterdam

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

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.

You only have to look at the frequency with which high-profile credit card data losses make the national press, and the sheer volume of card data available on the Dark Web, to see the scale of the problem. Card data is highly monetizable, and so remains one of the most attractive targets for cyber criminals.

Despite this, as with other compliance efforts, PCI DSS suffers from a lack of glamour, and 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, technology and other digital operational risks.

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 marketplace and selects those vendors it believes are making an outstanding contribution to better compliance with the evolving demands of 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. ●

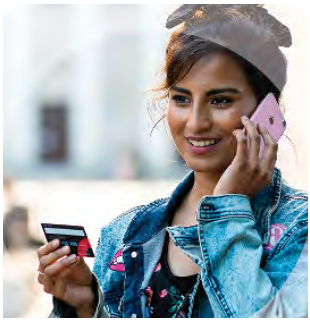
Editor
Simon Brady
e: simon.brady@akjassociates.com

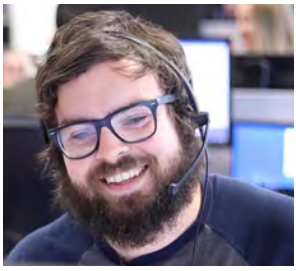
Production editor
Norma Kelly
e: normaewart@me.com

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





Advantio: Tackling fraud in the hotel industry

A complex environment including large numbers of card-present transactions poses complex fraud challenges for hotels and satisfying PCI DSS requirement 9.9 is critical. One of the largest hotel chains in the world partnered with Advantio to reduce the level of risk to their customers and business.

Achieving and maintaining PCI DSS Requirement 9.9 compliance across all their hotels is a major objective of one of the largest hotel chains in the world. In partnership with Advantio, this chain is reaching its vision across 1700+ hotels worldwide, 5500+ users and 6000+ devices.

Most hotels today accept credit and debit cards as a form of payment from their customers. Whether at the bar, the reception, the parking facilities or to secure a dinner reservation payment cards are commonplace. Managing these assets and ensuring their security is an enormous task for hotel chains like our client.

PCI DSS requirements 9.9
The level of face-to-face interactions between cashiers and customers taking place in a hotel means that PCI DSS Requirement 9.9 is prevalent here. In fact, any business accepting card-present type transactions must comply with requirement 9.9.

A complex environment poses fraud challenges
These card-present type transactions utilize PoS (Point-of-Sale) as well as PED (PIN Entry Device). While these offer convenience to customers, they can pose a substantial risk of fraud to organizations like our hotel chain client using them. Criminals target PoS devices aiming to tamper with them, steal or replace them with manipulated terminals. Card skimming with the goal of collecting cardholder data while transactions occur is a common fraud method. Vigilance is key to avoid existing and any newly developing fraud methods.

One of the largest hotel chains in the world partnered with Advantio to reduce the level of risk to their customers and business.

Reducing risk at every level
Advantio understands that risk must be reduced at every level of the organization. This means collaborating with staff from global managers to hotel employees working with PoS devices on a day to day basis. The latter is crucial for solving fraud challenges and becoming PCI DSS Requirement 9.9 compliant. The risk is the greatest at the terminal level. Advantio ensures that our intuitive solution is easy to use by all employees, regardless of their security experience.

Advantio's cloud-based ZeroRisk PINpoint is the right solution for this global hotel chain.

The user-role based training and ongoing support combined with the intuitive

software mean that hotel staff can comfortably act as security auditors on the front line. Security managers and global security leaders in the chain benefit from the ability to simply add and edit terminals when needed. They also benefit from real-time data and status updates, as well as the on-time notification of PoS devices expiring, thus ensuring an accurate asset inventory at the same time.

Advantio's ZeroRisk PINpoint recognizes security management at every level of the business: individual hotel, city, country, region and worldwide. This ensures that risk is minimized on an organizational level and fraud tackled from frontline staff to the boardroom.

Audits at the core of 9.9
Audits sit at the core of PCI DSS Requirement 9.9. A complete inspection has to take place at least once per year for organizations like this hotel chain. ZeroRisk PINpoint allows them to manage, track and audit virtually any kind of payment card reader (including ATMs) with ease.

When our client felt that more regular audits were needed to sufficiently fight fraud, the simplicity offered by PINpoint provided the solution. Through the PINpoint Quick Audit feature, they perform reviews at every shift change (3 times per day). Quick Audit features include:

- Simple user interface utilizing images and photos
- Time-saving tools to report issues
- e-Mail reminders to complete inspections

During the audit, the physical and logical security of devices is investigated. Photos of each device (up to 6 per terminal) are recorded which are used for comparisons in Quick Audits. Security managers are guided through the annual audit with a simple survey. The final result confirms the security of the devices and consequently compliance.

Effective management of 6000+ assets
To ensure compliance, organizations must be able to monitor the status of each device individually while also being able to view wider perspectives (e.g. regional level) in real-time. For a global leader such as this hotel chain, it means managing 6000+ assets across 1700+ locations.

ZeroRisk PINpoint eases the organization and population of device inventories. Assets can be added manually through mobile devices or via batch-imports of existing records. Automated synchronization of established databases is also possible when ZeroRisk PINpoint is interconnected via APIs. The solution's inventory features further provide filtering functionalities and detailed views to give the hotel's security managers a high degree of control over the card reader fleet.

A strategic business partnership
A security partnership goes beyond providing software and tools. It includes bespoke training and ongoing support. Advantio facilitates customized training online (live) and on-demand as well as multilingual customer support for users at all levels of the organization.

The senior management is kept up-to-date through regular meetings, calls, and webinars in which procedures, industry insights, and policies are discussed. In addition, customized dashboards allow them to monitor and report on activities at a global, regional, country, city or hotel level. They are informed about potential challenges and the need to replace devices through automated e-mails, ensuring the prevention of issues. Advantio gives support at every step of the compliance journey. This means implementation and daily security tasks are simplified for the entire organization.

The future holds further features such as a native mobile application for auditors in multiple languages, in-app e-learning modules and terminal geolocalization (via GPS coordinates).

Advantio is proud of this partnership and its growth.

- **Multilingual** - 83 countries. We support our clients on four continents
- **Proven success** - From a 30% starting point, 91% compliance reached globally
- **Exceeding expectations** - Preventing fraud through 3X daily audits

Simple solutions to complex business needs

"For organizations of any size compliance is a complex challenge. No business should be faced with additional risk, regardless of whether security experts or frontline staff are involved in the PCI DSS compliance process. This is why simplicity is at the heart of ZeroRisk PINpoint,"
Marco Borza CEO of Advantio explains.

ZeroRisk PINpoint solutions for your business include:

- **Wizard-driven card terminal auditing** Using a simple, wizard-driven smartphone app (Android and iOS), non-technical merchants can be guided through the process of auditing the physical security of their payment card terminals
- **Pre-configured wizard settings** Users can customize the auditing experience and tailor it to their physical device fleet.
- **Centralized data capture and reporting** With the ability to see and report on each payment terminal across every outlet, businesses have everything they need to demonstrate PCI DSS compliance and to plan future improvements.
- **On-demand Quick Audits** Merchants can conduct a reduced physical security check much more frequently to avoid fraud.
- **Device lifecycle management** Merchants can monitor every device from cradle to grave, from being held in stock, deployed to the shop floor, or expired – and all stages in between.
- **Remote trigger audit requests and security check** The ZeroRisk PINpoint management console tracks movements of terminals automatically, alerting the Merchant Portfolio Authority (MPA) to suspicious or unexpected activity ready for further investigation.
- **ZeroRisk Suite integration and API provisions** ZeroRisk PINpoint and the entire ZeroRisk Suite offer complete RESTful APIs to extend the platform to meet your specific auditing and compliance needs.
- **Comprehensive payment terminal support** From PoS to ATM, any device that can read a payment card can also have its physical risks assessed through ZeroRisk PINpoint.

If you are searching for a reliable business partner to achieve PCI DSS Requirement 9.9 compliance, speak to Advantio. ●
advantio.com
contact@advantio.com

www.cyberviser.com

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.

CardEasy from Syntec: Protecting phone payments

CardEasy 'keypad payment by phone' is Syntec's patented DTMF masking solution for card payment security 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.

Hiscox chooses CardEasy
Hiscox is a specialist insurer, underwriting a range of commercial and personal risks. It has grown from a single underwriter based at Lloyd's into a FTSE 100 company, with offices in 14 countries and customers around the world.

Improving phone payment security for customers
In August 2017, Hiscox worked with an external auditing company to review its phone payment security and PCI DSS compliance. It reviewed ways of improving the customer experience as well as reducing the internal workload required to maintain compliance.

Following the review, approval was granted for Hiscox to change the payments processes used within the business for 'over the phone' credit/debit card payments.

A formal RFP process was initiated to source the supply of a DTMF masking solution, to capture cardholder data without asking customers to read their card numbers out over the phone, which Syntec research shows that 80% of consumers prefer not to do.

Why did Hiscox choose CardEasy?
The CardEasy 'keypad payment by phone' DTMF masking system offered Hiscox a 'one-stop shop' for phone payment security, offering an improved customer experience whilst de-scoping its contact centre environments from PCI DSS controls (including agents, network, call & screen recordings). It also avoids piecemeal methods such as 'pause and resume' for call recordings. This suited both commercial and regulatory requirements, as the FCA require full length call recordings (which CardEasy allows for), as the DTMF tones of the card capture are flattened and so cannot be discerned from call recordings.

CardEasy future-proofs phone payment security too, as it is a managed, multi-tenanted service provided by Syntec, a leading PCI DSS level-1 international service provider.

What was involved in the deployment?
CardEasy integrated seamlessly with Hiscox's COLT SIP telephony and Cisco Call Manager, using premise-based ('CPE') equipment in London and Paris to facilitate the CardEasy managed service.

Results

Hiscox employees found the change from taking card payments from customers orally, to customers keying in their own card numbers, to be an easy transition, and a method customers generally prefer, intuitively appreciating the data security benefits. Agents also prefer the new system, finding it less prone to error, fast and efficient. ●

"Overall we're very happy with CardEasy. We need systems that support our high quality customer service ethos and meet our commercial requirements and in our case, CardEasy matches those needs and does exactly what it promised."

Sean Carney, Head of Operations, Direct UK

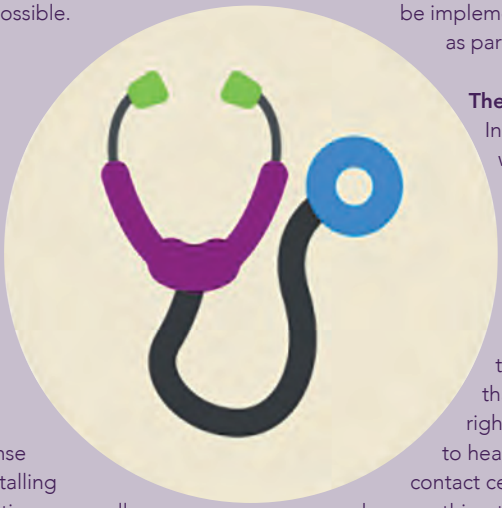
Major healthcare benefits management firm — USA

The client in this case is a major healthcare benefits management firm based in the USA. The organisation generates a minority of its revenue from credit card payments taken over the phone, so it did not want to make a large investment in PCI compliance but rather to descope from PCI altogether. It was also important to be able to demonstrate to callers that credit card payments were being taken in the most secure way possible.

Why CardEasy?

There were a number of factors that drove the organisation's decision to implement the CardEasy solution.

- CardEasy offered a hosted solution: The organisation has four locations that take calls so did not want the expense associated with installing an on premise solution across all four locations.
- Speed of implementation: Other providers were quoting installation times of six to nine months whereas CardEasy was able to offer a hosted solution to be up and running in all the organisation's call centres within four weeks.
- Customised to deal with specific requirements: During the implementation process the organisation came across a number of feature enhancements that were needed. The flexibility of the CardEasy system meant that these could be implemented straight away as part of the process.



The results

In a description that will resonate with many security specialists, the CISO explains the benefits thus: "The biggest benefit has been that it's working and that's what you want, right? We don't want to hear anything from our contact centres. If we don't hear anything then that means it's working as expected, they don't have any complaints. I always check in and they say, 'No problems, it's working like it's supposed to.' That's what's important." ●

Why global cosmetics firm Avon chose CardEasy

Avon is the world's second-largest direct selling company, specialising in beauty, household and personal care products with a global network of representatives selling door to door and through brochures.

The challenge

Avon 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.

Why CardEasy?

The decision to implement CardEasy was driven by the need for a DTMF masking system that would work with its 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. Avon 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.

"Our aim was to try and make the yearly process a lot easier and to reduce the questions on the form we have to complete. To do this we decided to eradicate card details from our infrastructure completely," explains Jason Earnshaw, SSC Technology and Projects Manager, Avon

"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 experience of the caller would be consistent and not disjointed. The last thing we wanted was for a caller to be rerouted halfway through the call to a different IVR that had been set up just to process payments," says Earnshaw.

CardEasy was selected because it worked seamlessly with Avon's existing on-premise IVR system as well as with its other suppliers' systems. As Earnshaw emphasizes: "It was very important to us that we selected a solution that would seamlessly integrate with our existing systems. We have vendors that create and manage our IVR. We have different vendors for our telephone systems. CardEasy was able to integrate effectively with multiple vendors' systems."

AVON
the company for women

"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, Avon

The results

From a caller's perspective, the only real difference is that the card number is no longer played back to them as Avon used to do before. Previously, the caller entered their card number, and it would be confirmed back to them. In the new world, they are simply asked to enter their card number and then move on, speeding 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. ●

Comforte AG: Using tokenization to tailor security to the business

Encryption is an effective and secure tool for protecting data, but its usefulness in high-volume, real-time payment environments is compromised by the demands it makes on IT infrastructure. This high-profile fashion retailer used Comforte to implement a tokenization solution to provide both speed and security.

The customer

In most retail stores, whenever a customer uses a payment card, the transaction details are stored in a central computer system to facilitate the exchange of money for the items sold. Unless the retailer outsources their payment processing to a service provider, storing transaction details is a normal business operation.

The largest fashion retailer in the US is no exception. With close to 900 stores in North America, accepting payment cards has long been a staple as part of their customers' experience: the firm has accepted payments from all major card labels (Visa, MasterCard, Amex, and Discover) for more than 30 years.

Explanation of the problem

Stored transaction details contain payment card data, which is a huge target for bad-actors or hackers looking to steal valuable data. On the dark web and underground websites, stolen credit and debit card details are sold for large sums of money, used to purchase illegal items, and exploited for other criminal purposes.

This is exactly what happened to this highly-recognized and trusted retailer. A few years ago, they experienced a data breach of an undisclosed amount of customer records. The data breach incident exploited gaps in their data security program, which prompted decision-makers at the board level to invest in a more robust data security solution.

As part of their existing data security program, the retailer already used encryption to protect the payment card numbers, as well as an internal reference number associated with every payment card. However, personal information (names, addresses, birthdates, etc.) of their valued customers remained unprotected. The high possibility of suffering another data breach due to unprotected data was not something the company wanted to risk.

Activating encryption for customer data across their complex landscape would overburden their hybrid infrastructure. Encryption is excellent for protecting data, however, to use the actual data for standard business purposes (like back-office processing, disputes and reconciliation, settlement, and customer loyalty programs), decryption needed to occur. Encryption and decryption processes take up computing power

and may impact transaction speed and performance. During peak times when customers visit their stores, the transaction volumes may reach over 100 transactions per second collectively from all the registers in the stores as well as online transactions. The last thing this retailer wanted to do was slow down authorizations happening at their registers. This would harm their world-renowned customer service.

Encryption and decryption also increase IT operations, specifically the management of encryption keys. As a common practice in encryption processing, encryption key management responsibilities require refreshing and replacing encryption keys every-so-often (also called rotating keys), as to reduce the possibility of data exposure should the encryption keys be lost or stolen. The retailer expects its volumes to grow year over year; therefore it was natural for them to expect their operations and key management functionality to grow as well. To put this effort into perspective, based on the annual volume from this retailer, rotating encryption keys on one billion payment cards every year was not a task they wanted to continue.

This company was also working on ways to minimize risk, not increasing it. So, the concept of adding more sensitive data to a huge encryption program was unattractive: the more sensitive data under encryption, the higher the risk of encryption key exposure the retailer faced. Security professionals know that hackers typically do not attempt to break the encryption algorithms; they attempt to steal encryption keys. Therefore, counter-intuitively, more sensitive data protected with encryption could be seen as increasing their risk, rather than minimizing it.

Why tokenization?

Tokenization was the data protection method the retailer chose to secure its sensitive data throughout its enterprise. Tokenization of sensitive data uses cryptography to generate a surrogate value (also called a token) of the original data. Tokenization differs from classic encryption because tokenization does not use an encryption key as part of the cryptography process. Tokenization is a data protection method with less risk of sensitive data exposure (since no encryption keys exist) and less operational impact since no encryption key management activity needs to be planned and resourced.

However, there was one more major requirement the retailer mandated before finalizing their decision. The retailer wanted to be sure that when sensitive data was tokenized, the retailer could then use the tokenized data throughout their enterprise and still receive the same results. This requirement is called 'maintaining referential integrity.' In simple terms, if card number "4444 4444" is tokenized into value "9876 5432," then the same card is used one year later, the tokenization process will still tokenize the original card value as "9876 5432". Referential integrity allows the retailer to

maintain data usability throughout the lifecycle of each customer, throughout their applications and services, and provide the data security and privacy necessary to stave off data exposure incidents or data breaches.

No other approach provided data protection, privacy, and referential integrity while maintaining the lowest level of risk tolerance provided by tokenization. Therefore, the retailer was completely convinced and committed to securing its enterprise with tokenization.

The benefits
The retailer was already in compliance with PCI DSS requirements. The switch to tokenization had no impact on their PCI DSS compliance stance, as tokenization is recognized by the PCI Security Standards Council as a strong approach to payment cardholder data protection.

Two added benefits resulted from the switch to tokenization as the data protection method. First, the retailer can potentially reduce the scope of the security audits they are subjected to each year. Typically, the security audits for PCI DSS compliance require the scope of audit to include all systems which contain the original payment cardholder data. Since the tokenization process replaces the original data with a surrogate (token) value, some systems can be taken out of the scope of the security audit, since the original data no longer exists. A complete study has not yet been completed, but it is anticipated that the retailer may save more than 60% in time and resources as a result of Audit Scope Reduction due to tokenization.

Secondly, tokenization positions the retailer to be ready to respond to other data privacy laws surrounding the processing of personally identifiable information (PII). In the US, each state has come out with – or will be coming out with – data privacy laws that protect customer data. Based on how the retailer uses personal data from its customers, it may be subject to some of these data privacy laws. Tokenization fulfills the act of replacing sensitive data with surrogate values, which puts the retailer in a strong position when looking to meet compliance with data privacy laws.

The process (from proving it, to using it)
The retailer did require a small, focused Proof of Concept (POC) project, which our solution was able to meet on-time and with all requirements met. Due to the sensitive nature and the specificity of their requirements, the details for the POC are not in the public domain.

Where the customer stands today, what about tomorrow?
As one may expect of an organization with 30 years' history of accepting payment cards, and over one billion payment cardholder records, the project to improve its data security has the full attention of each department involved. The retailer is in full project mode and has already completed the first milestone towards getting fully implemented with tokenization.

In summary, the keys to success were convincingly met:

- Minimize the existing risk of cardholder and customer data
- Present negligible transactional impact on retail stores or online services;
- Maintain referential integrity thus allowing tokenized data to operate as if it were the original data;
- Extend data protection beyond payment card numbers to include personal info from customers ●

Eckoh: De-scoping the contact centre

Financial services firms are particular targets for cyber-criminals so PCI DSS compliance, GDPR compliance and data security in general are critical. Eckoh's solution takes the contact centre out of scope, maintaining data integrity and business efficiency.

The customer
The company was founded in 1976 and is headquartered in London focusing its businesses on international payments, bureau de change and issuing prepaid credit cards for use by travellers. It is the world's largest foreign exchange bureau.

Today they have 1,500 outlets based in tourist locations and in over 100 airports across 26 countries. They provide customers with over-the-counter currency exchange as well as prepaid cards which travellers receive before they travel. They have developed a growing network of over 1,100 ATMs at both on-airport and off-airport locations around the world and their mobile foreign exchange platform handled 1.4 million mobile and online transactions in 2016.

Their UK contact centre operation has roughly 100 agents handling customer queries and processing payments over the telephone for foreign currency.

The challenge
Working with the exchange of currency, this business is a target for fraudsters. In response to this they have built some robust processes, involving many layers, to help prevent a breach or any fraudulent activity occurring in the contact centre. These processes include extra training for agents that requires them to listen out for rustling of papers when the customer is asked for their card details. This is because it could signify that customer is not holding an actual card but is searching acquired paperwork for a card number which would indicate that this customer is not the legal cardholder.

This very real threat to both the business and reputation, as well as the end-customers' card security, meant that further measures were needed to protect all stakeholders.

At present they use a NICE call recording platform and, at the point where a payment needs to be taken, their agents pause the call recording so that sensitive details are not recorded or stored. While this had provided a degree of protection and contributed to their PCI DSS compliance, the number of payments that their agents take continues to rise, resulting in the need for a more stringent and secure solution.

In conjunction with their drive to find a simpler and more reliable way to achieve PCI DSS compliance, the business has a top priority to have Disaster Recovery (DR) practices in place. They also have a secondary contact centre site that can be used

in the event of a failure at their primary contact centre. However, one of the toughest challenges is that the trigger for switching between sites was not simple to put into action. In order to ensure Business Continuity, they sought a more reliable and effective solution to this element of their service.

Client objectives

- Protect the business and customer data from the risk of fraud and the impact of a data breach
- Prevent agents from seeing, hearing, recording or storing sensitive card data
- Maintain full call recording, without trapping sensitive data
- Ensure that the agent can stay in contact with the customer throughout
- Scale up, and down, to match business needs and customer demand
- Simplify PCI DSS compliance and maintain compliance - every minute of every day
- Ensure robust Disaster Recovery practices are in place.

Why they chose Eckoh

Until recently the business had been using manual solutions for PCI DSS compliance. They felt these were right for the business at the time. However, as the business grew, and they started taking considerably more phone payments for foreign currency, they were unable to scale up their operation to cope effectively. They also wanted to simplify the burden of compliance.

The business aim is to make money easy to spend and send. This brings some challenges and risks, so they turned to Eckoh whose secure payment solution is proven to be quick and simple to implement. It takes the customer's contact centre completely out of scope of the PCI DSS audit which is a massive simplification for them and means they can reduce the risks significantly. That brings major benefits to the business and their customers.

What Eckoh deliver

- **For PCI DSS compliance and securing payments:** Eckoh's patented CallGuard solution was implemented, using the company's existing payment pages. This was a critical requirement as they had already undergone some deep-level integration to their multiple CRM systems which they wished to maintain. The simplicity of Eckoh's CallGuard means that very limited work needs to be done to implement the solution and will not affect the current integrations that are in place.
- **For Disaster Recovery and Business Continuity:** EckohROUTE – a natural language call routing solution - allows the business to take control of where calls are delivered via a simple-to-use

online interface. Eckoh will help the business build a pre-configured routing so that, in the click of a button, they can instantly route all the incoming calls to the contact centre into their DR site.

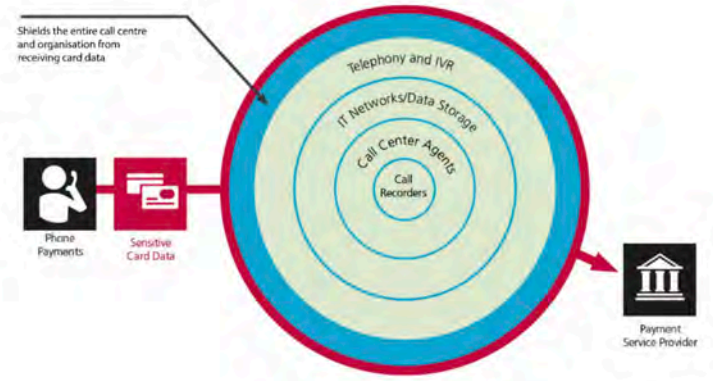
Agent assisted payments in a PCI DSS compliant manner: CallGuard Hosted
The business chose the CallGuard Hosted solution because it removes the entire contact centre (agents, call recordings, telephony, networks and systems) from the scope of PCI DSS. The service enables their contact centre agents to remain on the phone with the caller and guide them verbally through the payment process.

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

How does CallGuard work?
CallGuard completely de-scopes a contact centre. All incoming calls to the customer contact centre come through Eckoh's secure platform. When the agent needs to take a payment the agent's phone and web sessions are linked to a CallGuard ID. This ID is displayed on the agent's CallGuard web panel and the agent then enters the ID into their phone keypad. Alternatively, the ID can be played down the phone as audio and then the agent types the ID into the CallGuard web panel. CallGuard allows the caller to remain on the phone with the customer's contact centre agent, who will guide them through the payment process, assist in the event of any difficulty and complete any final tasks.

When a payment is required, the agent asks the caller to enter the details using

The CallGuard process



their telephone keypad, which will generate DTMF tones. CallGuard recognises these tones as sensitive information and replaces them with flat tones. Call recording continues as normal. The agent receives visual process indicators on their web panel and remains on the line with the caller, guiding throughout the entire process, and correcting any errors if necessary.

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

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

How does the business benefit?
Securing payments: Eckoh's CallGuard solution ensures that all payments are completely secure and comply with PCI DSS. It also means that customers can make payments over the phone with an agent.

PCI DSS compliance: The robustness of the solutions, and the simple fact that no data is permitted to enter the business's environment, means that the contact centre and agents are de-scoped from PCI DSS audit. This simplifies the compliance process and makes it easier to maintain compliance – ensuring customers and the business are protected every minute of every day.

Exceptional customer service: Being able to offer customers the ability to make payments in a channel, at a time or on a device that suits them is a major customer service differentiator.

Maintain agent-customer contact: Because the solution prevents any sensitive data coming into the system the agent can stay in contact with the customer throughout the interaction. This is a reassurance to the customer who previously may have worried about what was happening during the payment process, as well as making the agent's life easier without having to remember to stop/start a recording.

For this business it was really important that they found a solution that was easy to use for their agents. They need to have confidence that, when they're speaking to a customer, they can rely on the technology and they can reassure the customer that the payment that they're taking is secure and will be processed without any issues. The solution really does work and it works well for the agents using it, and for the customer.

GDPR compliance: While PCI DSS compliance does not constitute complete GDPR compliance it certainly contributes because often, the systems used to protect cardholder data can be used to protect personal data too. That's because it is often collected at the same point in the interaction. Because Eckoh's solutions prevent any sensitive data entering the contact centre systems, there is nothing there to be at risk and so it can contribute to compliance with GDPR as well.

The business has benefitted in the following ways:

- Agents no longer hear the cardholder data being read out. The customer enters their card details into their telephone handset keypad.
- The agent no longer sees the cardholder data. They only see asterisks or hashes (*/#) in place of the card data on their screen
- The card data is not stored anywhere in the company's contact centre environment nor in call recordings
- The entire contact centre is removed from PCI DSS audit scope – simplifying their compliance process.
- The business can be sure that they are, and remain, fully PCI DSS compliant every minute of every day
- The risk of fraud is significantly reduced – as there is no data available to steal
- Easy switching between contact centres means that they can demonstrate their DR, business continuity and sustainability credentials.

PCI DSS and GDPR

Eckoh's solution has once again solved more than just the customer's immediate PCI DSS compliance requirements by also contributing to GDPR compliance. It delivers well beyond the scope of the contract providing security, peace of mind and reassurance to the paying customer. What's more, Eckoh's continuous innovation and broad breadth of solutions mean that payments and customer engagement tools can be added whenever changing needs demand.

Simplest solution

The important distinction for Eckoh and this business is the ease with which Eckoh's solution has been implemented because it requires minimal integration and so does not disrupt existing systems and processes. This has not been possible with other solutions on the market due to their complex design and implementation.

If there's no data, there's nothing to steal

Making things appear to vanish has been a magician's trick for centuries. Now Eckoh have made it happen with sensitive card data — instantly removing a compliance challenge and a risk that otherwise threatens to unseat today's contact centres. With data prevented from entering the customer's environment, there's nothing for thieves to steal, providing unrivalled security that protects sensitive data.

Compliance every day

The nature of CallGuard means that the customer has achieved, and can maintain, PCI DSS compliance every minute of every day. With the problem solved, the business can focus on its core services to businesses and customers across the globe while securing its customers' payments, providing new levels of confidence, disaster recovery, business continuity practices and peace of mind for everyone. ●

www.cyberviser.com

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.

ECSC: PCI DSS and the importance of getting it right

Are your suppliers putting you, your customers, and your PCI DSS compliance status at risk? A real-life 'not it!' story, how it led to a breach, and how ECSC helped their client recover.

Background

Until recent years, it could be argued that for many organisations cyber security has been a bit of an afterthought. It is therefore reassuring to see the increased emphasis organisations are placing on prioritising their cyber security, with many now making it a board issue.

Having said that, cyber security continues to present many challenges to management, mainly as a result of it being a relatively new, fast-changing area of organisational risk, with few people that understand it. This is something we're witnessing in many well established organisations that have experienced rapid growth, where the day-to-day running of the business remains unchanged.

Like many traditional retailers, this client saw the potential to expand their offering into online sales, and as they rightly recognised that their expertise lay within traditional sales the IT elements were outsourced.

That was certainly the case for this client. Like many traditional retailers, this client saw the potential to expand their offering into online sales, and as they rightly recognised that their expertise lay within traditional sales the IT elements were outsourced.

The Challenge

The client selected an 'e-commerce specialist', to build, run and modify their e-commerce platform, with their in-house digital team focusing on the look and feel of the site, with some control over content in terms of uploading various marketing campaigns. From a PCI point of view, the client considers this all to be outsourced and therefore the responsibility of the third-party specialist. The third-party specialist believes that the responsibility remains with the client as it wasn't agreed as part of their brief; and failing that with the data centre in which the data sits.

At no point are either the client or the third-party specialist putting any focus on security.

The client was later contacted by a customer who informed them they were seeing an anti-virus alert when trying to access their website. This instigated a chain of investigation, which unfortunately confirmed the website had been maliciously tampered with, and having gained access to an admin account, malware was installed; in this case a card skimmer.

As part of our forensic investigation, we found that the exploit was a zero-day vulnerability, meaning when we found it there was no other evidence that this was a previously known vulnerability. Further investigation confirmed that searches

looking for sites that would be vulnerable to this type of exploit had begun 12 months previously. In the 6 months that followed, a second phase began where the attacker created a new admin account. Finally, a few days before the exploit became known, the attacker logged in and introduced the card skimmer, gaining access to several million users' personal data.

Solution

As we approach our twentieth year, of all the breaches we have been involved with or of those reported in the press and to the Information Commissioner's Office (ICO) we are yet to come across one that couldn't have been prevented, as was the case here. For this client adopting the PCI Data Security Standard would have provided sensible steps to adhere to security best practices. In particular allowing for:

- Secure configuration
- Use of security controls
- Logging and monitoring – the SQL injection attack would have been picked up and the new admin account created
- Penetration testing – as a zero day vulnerability it wouldn't have been picked up by scanning but it may have been found via a pen test.

Following our forensic investigation to identify the root cause and contain the breach, we then focused on recovery, assisting the client in working with the major card brands and the ICO.

As part of remediation we provided QSA support and the client can now demonstrate PCI compliance as a Level 1 Visa merchant. Additionally, the successful completion of their Report on Compliance (RoC) continues to demonstrate to their customers their ongoing commitment to security and compliance.

Final Thoughts

You must take responsibility for your own cyber security, even if you believe yourself to be exempt from PCI DSS because you have outsourced to the 'experts'. The example above is one of many we come across where neither party takes ownership and ultimately ends in a breach.

Don't expect those you outsource to, to take responsibility for PCI DSS unless you specifically ask them to and it is written into the Terms and Conditions of the service agreement. Ultimately, you need to understand the cyber security expectations on you and not assume that outsourced service providers are taking care of it. If in doubt, seek advice from independent specialists.

About ECSC

Established in 2000, ECSC Group plc 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 you achieve rapid compliance with the PCI DSS standard. Our PCI specialists are all Payment Card Industry Qualified Security Assessors (PCI QSA).

In addition ECSC is the UK's longest running full-service cyber security provider, specialising in 24/7/365 security breach detection and Artificial Intelligence (AI). A cyber security partner that can help you in all aspects of your information and cyber security requirements, we have helped clients in over 20 countries recover from incidents, enhance their cyber security, and gain a range of information and cyber security certifications such as PCI DSS.

Contact
Clare Macdonald
clare.macdonald@ecsc.co.uk
01274 736 223
www.ecsc.co.uk

GALA TECHNOLOGY
integrated technology solutions

SOTpay
SECURE . COMPLY. PROTECT.

DO YOU WANT TO KNOW WHY WE KEEP WINNING AWARDS?

THEN CONTACT OUR TEAM TODAY

01709 911 661
www.galatechnology.com
info@sotpay.co.uk

Gala Technology are the development team behind the multi award winning secure payment solution SOTpay.

We believe that every business should have access to affordable technology that allows them to take secure and PCI DSS compliant payments, across a host of channels, including telephony, e-commerce and web-chat, whilst negating the risk of fraud related chargeback and reducing processing costs.

Our cloud based SOTpay platform gives you the flexibility to take secure payments via email, SMS, Electronic Invoice or even on Social Media channels, remaining in constant contact with the cardholder or simply receiving agent notifications when payments are completed.

With no additional hardware or amends to your telephony or network environment required. SOTpay is the most cost effective solution on the market to remove your organisation from the scope of complex PCI DSS requirements.

ELIMINATE FRAUD RELATED CHARGEBACKS

REDUCE PROCESSING COSTS

PCI DSS COMPLIANCE

CLOUD BASED SOLUTION

OMNI-CHANNEL PAYMENTS

PROTECT YOUR REPUTATION

CALL OUR TEAM TODAY

01709 911 661

www.galatechnology.com

Unit 54, Century Business Centre, Century Park, Manvers, Rotherham S63 5DA

PCI Pal: Better security, better business

Cloud-based payment systems allow businesses to take sensitive customer data out of scope for PCI DSS. This insurer used PCI Pal to secure its Card-holder Not Present payments and saw a sharp fall in customer drop outs.

Payment card data is the ultimate reward for hackers, so businesses need to address all areas of vulnerability. PCI Pal's Agent Assist supports global contact centres in safeguarding telephone-based card payments. Its globally-accessible cloud platform empowers organisations to take Cardholder Not Present payments securely without bringing their environments into scope of the PCI DSS.

The client

The Verex Group is an innovative provider to the UK motor insurance and vehicle manufacturer accident aftercare sectors. Its specialist insurance services business works in the interests of car buyers who want their vehicle repaired to vehicle manufacturer approved standards, vehicle manufacturers, their franchise dealers and approved body-shop networks and provides comprehensive vehicle manufacturer-branded motor insurance and accident aftercare services.

"We needed to identify an assisted mid-call solution that would overcome this problem, while also ensuring we remain PCI DSS Compliant in the way our customers' payment details are handled."

Jack Davis, Salesforce & Omnichannel Development Manager for Verex Group

Verex's team of 70+ contact centre agents located across two sites in Rickmansworth and Bristol in the UK, along with several remote home-based workers, handles on average more than 300 telephone-based payment transactions every day.

A mid-call Interactive Voice Response (IVR) system was previously deployed that allowed agents to re-route callers to an IVR system to complete the final payment stage for their insurance policy, renewal, or adjustment.

The challenge

There were however several issues arising from this method that needed to be addressed, as Jack Davis, Salesforce & Omnichannel Development Manager for Verex Group explains:

"We were finding that every day, a high percentage of callers would drop-out of the payment process; anywhere between 20% and 30% of payments by phone would fail at the first attempt. A key issue was that if a customer had a query or inputted their card details incorrectly, there was no way of them communicating with us at the time, so they would drop-off the call and, hopefully, try again.

"Not only did this mean we were seeing high failure rates, but it also meant that if the customer called back, there was no guarantee that they would speak with the same agent. As our agents are rewarded for successful customer outcomes upon completion of each transaction they personally handle, this was a major frustration for our team.

"We needed to identify an assisted mid-call solution that would overcome this problem, while also ensuring we remain PCI DSS compliant in the way our customers' payment details are handled."

To add to this, NewVoiceMedia, a Vonage Company, which handles the contact centre telephony solutions for Verex, had advised the team that the existing mid-call IVR solution was being discontinued and an alternative would need to be arranged. Following discussions with NewVoiceMedia it was agreed that Verex would migrate away from a mid-call IVR to a more user friendly, assisted option.

In summary:
Between 20%-30% of callers dropping-out of the payment process at the first attempt.

If a customer had a query or inputted their card details incorrectly, there was no way of them communicating this at the time so they would drop-off the call and – hopefully – try again.

If the customer called back, there was no guarantee they would speak with the same agent; as they receive commission upon completion of each transaction they personally handle, this was a major frustration for the team.

They needed to identify an assisted mid-call solution that would overcome this problem, while ensuring the company remains PCI DSS Compliant.

The Solution would therefore need to enable them to continue recording calls to make sure they comply with the insurance industry regulations.

The Solution
Following NewVoiceMedia's recommendation, Verex selected PCI Pal's Agent Assist solution, which is a true cloud secure payments solution that is fully integrated with NewVoiceMedia.

Originally the team assessed three solutions; an alternative mid-call solution, PCI Pal's Agent Assist and a 'pause and resume' option. Confirms Jack, "The assisted option really struck us as being the best as it would enable us to provide a more personalised approach on every customer interaction. With Pause and Resume, it requires agents to be switched on to this; there's a huge reliance on

staff to get this right as if they forget to pause, we're in breach. Also, if they forget to un-pause and we haven't recorded the terms and conditions being read for example, and there's a claim, we don't want to be hit with a £1M claim as this wasn't recorded! We operate in a highly regulated industry and so it's vital that we're on top of our game here; we felt PCI Pal's solution removes this issue for us completely."

Instead, Agent Assist appealed to Verex as it would allow them to take card payments securely while the agent and customer remained in conversation. With no call transfers required, the customer is able to input their card details using their telephone keypad. If any assistance is needed, the agent remains on the line and is there to assist, meaning fewer dropped calls, faster transaction times and greater service continuity for the customer.

"We operate in a highly regulated industry and so it's vital that we're on top of our game here; we felt PCI Pal's solution removes this issue for us completely."

Jack Davis, Salesforce & Omnichannel Development Manager for Verex Group

It also means that no card details are orally provided, so the threat of potential insider frauds is not present and removes the burden of handling any sensitive card details from its staff.

Once the customer has provided their details, the agent simply presses the 'process card' payment button on the CRM screen and it instructs the PCI Pal solution to send the transaction to the payment provider for processing. No card details are seen or heard by the agent, and no data enters Verex's infrastructure, reducing the scope of PCI DSS compliance.

Successful Integration

Tom Bowen, a Senior Database Architect (Insurance) for Verex worked closely with NewVoiceMedia and PCI Pal to integrate the solution into Verex's existing CRM's iFrame dashboard, as he confirms:

"The whole process of integrating PCI Pal's Agent Assist was as smooth and as slick as any recent project implementation I have been involved in with Verex; from the initial conversations to completion it took no longer than two and a half months. We were initially supplied with a comprehensive integration specification proof of concept, and had an assigned account manager, Matt Davis, who was completely on the ball and with whom we held weekly project calls. Matt coordinated everything between NewVoiceMedia, a Vonage company, our payment gateway providers and our internal developers, and made sure everything was in place

in terms of the development, testing and implementation of the PCI Pal solution.

"There were a few technical hurdles to overcome on the way, such as imbedding the PCI Pal iframe interface into our broker software, but we had a lot of knowledgeable people involved in the project, including our senior insurance CRM developers. This meant we all knew who was doing what, and it resulted in a seamless transition to the new PCI Pal solution, which was delivered on schedule."

Objectives Successfully Achieved

With data security high on the agenda for Verex, payment card security is assured thanks to Agent Assist. When reflecting on the results since Agent Assist went live, both Jack and Tom are quick to praise the way the solution has supported Verex:

Confirms Jack, "PCI Pal's Agent Assist is a far better solution; since launching we have seen call drop-out rates fall from up to 30% to just one or two per cent. Now, agents can interact directly with customers and so the points of failure are far less. They are there to handhold customers through the experience, whereas before if a customer mistyped their details or were unsure about something they had to start again, which was frustrating for them and our agents. It's far more customer-friendly now."

Tom adds, "There's certainly less margin for error and since Agent Assist went live we have seen that our call rates have improved. We're faster at processing payments and so we've seen our calls reduce, on average, by at least 30 seconds, which adds up when you're working with the volumes that we do."

On average, calls to discuss and book an insurance policy were originally 15 minutes. Since using Agent Assist, average call durations are now around 13.5, which over the course of a month, across 70+ agents, calculates to quite a time saving.

Explains Jack, "All agents have said they prefer the new system; it's improved their efficiency, they haven't had to dramatically change the way they work, plus with dropped-calls all but disappearing, they are achieving successful customer outcomes on every transaction call they handle, which for them is a major advantage."

"The process of buying a policy is now easier; the process is much more refined and so customers are less likely to drop out. For our agents, our call times have improved which is a big measurement for us. Ultimately, our agents prefer it, our customers prefer it and we are seeing a big jump in efficiencies all round."

Jack Davis, Salesforce & Omnichannel Development Manager for Verex Group

From a technical and management perspective, PCI Pal's solution provides metrics and developer tools that the team can use to track performance and debug any issues with payment processing on individual transactional cases. Adds Tom, "This level of functionality and transparency was not as refined under the older, mid-call IVR solution, so PCI Pal's Agent Assist provides us with another clear advantage."

Concludes Jack, "The process of buying a policy is now easier; the process is much more refined and so customers are less likely to drop out. For our agents,

our call times have improved which is a big measurement for us. Ultimately, our agents prefer it, our customers prefer it and we are seeing a big jump in efficiencies all round."

At-A-Glance Summary – Successful Delivery of Client Objectives:

- With PCI Pal's Agent Assist, The Verex Group has reduced call drop-out rates from up to 30% to just 2%
- Call duration has shortened from an average of 15 minutes to 13.5 minutes each, enabling contact centre staff to handle more calls each day
- Payments are handled faster, with less margin for error
- The contact centre agent remains in constant contact with the customer to provide assistance, where needed, and ensure the payment is securely handled
- Call recording remains in place as no payment information is verbally provided
- Improved metrics enable the management to see which agents are handling which payments, with far greater transparency than ever before
- Agents prefer working with Agent Assist – it makes their lives easier and with less call drop-outs they are receiving commission on all payments they process
- Agent Assist was integrated extremely quickly – on time
- The Verex Group is fully PCI compliant.

PCI Pal's Agent Assist supports global contact centres in safeguarding Card-holder Not Present payments by ensuring sensitive card data is NEVER disclosed to the contact centre agent or enters an organisation's network.

Instead, using DTMF masking technology, Agent Assist captures payment details securely whilst enabling agents and customers to remain in full conversation. It is a scalable cloud-based solution, which integrates with many of the major payment providers, while being carrier, phone system and CRM agnostic.

Once customers have entered payment details using the telephone keypad, Agent Assist transmits the data directly to the Payment Service Provider (PSP) for authorisation; no cardholder data ever enters the company's environment, meaning the scope of PCI DSS is vastly reduced. As no card data is spoken, call recording can run seamlessly ensuring that organisations retain a complete audio file for compliance and security.

The customer and agent experience is seamless and reductions in average call handling time are regularly achieved. Payment conversion is often improved too, particularly when the system is used in place of automated payment systems.

Contact Centre Payment Security Assured for The Verex Group ●

Prism Infosec: Driving PCI Compliance Through Innovative Security Testing

Using an innovative advanced red teaming approach to identify risks associated with a retail client's PCI Cardholder Data Environment (CDE).

Prism Infosec, a Payment Card Industry (PCI) Qualified Security Assessor (QSA) and European CREST member company, used an innovative advanced red teaming approach to identify risks associated with a retail client's PCI Cardholder Data Environment (CDE). The delivery of an extensive red team engagement meant that the retailer could comply with multiple requirements of the Data Security Standard (DSS), whilst raising the level of information security associated with the protection of cardholder data and personal information. The combination of Prism Infosec's technical expertise, along with significant experience with PCI compliance, delivered a truly unique client engagement.

Client Requirement for Innovation

Prism Infosec's client, a major UK retailer wished to comply with the PCI DSS for the protection of its cardholder data, but also wanted more than just a "tick box exercise". The client was very clear that simply meeting the bare minimum of PCI DSS penetration testing through segmentation and web application testing would fall short of their requirements - they wanted their partner to add greater value and identify gaps in the control framework across the organisation and identify whether their critical data assets (cardholder data and personal information) were adequately protected from advanced threats.

Prism Infosec delivered a red teaming exercise to establish whether the organisation's security controls could be circumvented, thereby allowing unauthorised access to customer details and cardholder data. The Prism Infosec team adopted the mindset of a tenacious attack team who would use multiple exploit and compromise routes, including phishing and spear-phishing attempts, social engineering and physical break-ins.

The Prism Infosec team adopted the mindset of a tenacious attack team who would use multiple exploit and compromise routes, including phishing and spear-phishing attempts, social engineering and physical break-ins.

Defining the Engagement

Prism Infosec engaged with the client's Chief Information Security Officer (CISO) and the Security Manager to define the project's objectives. It was important to define these early in the engagement to ensure key stakeholders had a clear

expectation of the required goals and outcomes. Furthermore, Prism Infosec learned more about how the organisation wanted to test the effectiveness of an outsourced Security Operations Centre (SOC) and Security Information and Event Management (SIEM) service.

During this initial pre-engagement phase of the project, Prism Infosec worked with the client to agree a clear and unambiguous statement of work that detailed the essential success elements, these were:

- **Objectives** – the key objectives of the planned exercise, which included whether it would be possible to exfiltrate sample records of PCI and/or personal data stored internally, either within the Cardholder Data Environment or otherwise;
- **Agreed Attack Types** – including internal and external (to the organisation) network- based attacks, application layer attacks, social engineering (including phishing and spear-phishing) and physical break-ins. Additionally, other innovative break-in methods were agreed, such as leaving potentially malware laden USB sticks in the vicinity of the reception area to determine whether a member of staff placed them in their laptops;
- **Scope and Initial Information** – to satisfy the client's expectation but without constraining the team's creativity, a minimal scope and set of boundaries were agreed. This included restricting the test to the client's UK operations and excluding certain subsidiaries;
- **Out of Scope Attacks** – given the organisation and its payment handling were in a productive state, purposeful Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on perimeter, internal systems and networks needed to be out of scope. To minimise disruption, test to the limit of the organisation's appetite for risk and best focus resources, both parties agreed and documented out of scope test types;
- **Communication Channels** – given the client wanted to test the effectiveness of the monitoring and response teams in identifying attack methods, Prism Infosec established clear communication channels and escalation routes. These were documented and agreed in the statement of work such that any communication (including emergency escalations, general test progress updates and incident response handling) points within both the client and Prism Infosec were established;
- **Time, Coverage and Budget** – the length of the project and consultant's time assigned to it, this had to strike an effective balance between ensuring enough time to cover the proposed testing, as well as the client's budget. Prism Infosec produced a clear timetable of events and associated costs for each phase based on extensive experience of bringing greatest value to the client. The timetable helped the client determine the types of attacks that would occur

and when, and helped the CISO and Security Manager understand whether the attacks during the project window were malicious or simulated exercises by the authorised attack team;
- **Agreed Output** – specifying and agreeing the format of the report, the client appreciated the format of our sample report but also wanted the ability to quickly include risks in their risk register. Prism Infosec agreed the fields that should be included and understood the organisational risk scoring methodology to ensure the statement of work made it clear what information was to be captured.

Clear definition of the approach, communication channels, timescales and budget boundaries meant that the client was assured the project was properly planned and would be executed in a formal and structured way.

Knowledge is the Key to Success
The test began by conducting a significant period of surveillance on the organisation, both electronically and physically.

This included:
- Assimilating information about the target company, its structure and key locations from its own corporate website as well as online resources. Prism Infosec identified locations for the head office and contact centre;
- Identifying people and email addresses within the organisation using common popular social networking sites such as LinkedIn, Facebook, Twitter and other online forums;
- Finding networks and key systems associated with the target based upon Internet registration records;
- Looking for case studies that could assist with identifying key technologies and security controls that might be in place;
- Searching darknet forums and cracked password/hash dumps for information and organisational email addresses that have been previously compromised;
- Finding key resources such as network, system and security administrators and personnel from freely available Internet resources;
- Using mapping and satellite views to observe the layout and geography of locations and searching for floorplans;
- Visiting sites to survey ingress points such as reception areas, loading bays, fire escapes and secondary entrances. Additionally, busy periods (such as morning arrival, lunchtimes and staff departure times) or shift change patterns were identified as these can often be the opportunities that attackers can exploit. Furthermore, it was possible to identify physical security controls, such as barriers, CCTV, access pass layouts and associated lanyard colours and logos.

The Prism Infosec team managed to gain unauthorised access into the contact centre by tailgating members of staff into the building during the busy lunch period and showing a fake pass to the security personnel.

Attack Scenarios
Following the period of surveillance, a number of attack scenarios were established which could lead to success:
- **Contact Centre** – this was located in a shared business campus and used by people who were not associated

with the organisation making it easier for the team to be less conspicuous. The transient nature of staff within the contact centre and their casual dress presented an informal environment which could potentially be exploited. It was also possible to identify lanyard colours and photo badge formats used by the organisation. The contact centre access facility also seemed to be weak, with a clear entry route into the rest of the building past the reception area;

- **Head Office** – security seemed tight in the head office location with airport style barriers in reception restricting unauthorised access to the rest of the building. However, it was theorised that leaving USB sticks branded with the organisation's logo on the tables in the waiting area may be successful;
- **Spear Phishing** – a significant online recruitment strategy was identified and known to be in operation. Using this knowledge, a plan was formed to compromise security through a CV that included a macro, that if run by a less security aware worker in the Human Resources team, could introduce a malicious payload.

Standard Internet-based penetration test attempts were ruled out, as online searches showed they had engaged the services of other approved security vendors and were conducting Approved Scanning Vendor (ASV) scans on a quarterly basis. It was felt that this route could use too much time, and that the chance of success was low and could trigger intrusion detection.

Attack Execution

The attacks were executed and success was achieved via two of the planned scenarios. The Prism Infosec team managed to gain unauthorised access into the contact centre by tailgating members of staff into the building during the busy lunch period and showing a fake pass to the security personnel. This allowed access through the RFID access control, as well-intending staff held the door open allowing the team to follow them into the main office. Once in the building it was possible to connect a micro custom-made backdoor device to an unused network port under a desk and establish a bridge to the corporate network over both Wi-Fi and 4G.

Once the team back at the Prism Infosec offices had observed that the connection was successfully established, it was possible for the red team to exit the organisation without any further confrontation and the attack continued remotely with a reduced risk of physical challenge. This also gave the team time to conduct "under the radar" network enumeration and location of potential weaknesses. Furthermore, as the device was located within the contact centre network, it was thought that there would be an increased opportunity for success to compromise either desktops or services processing payments or personal details.

Manual low volume probing of the networks over a further three weeks identified that a single server was missing a critical Microsoft patch, that had a public exploit that been successfully tested by Prism Infosec.

Exploitation of the server allowed the team to gain a high level of privileges and using attack chaining techniques, it was quickly possible to escalate from a local user on the system to an administrative account with access to many other systems in the client's internal domain.

Prism Infosec managed to establish

an ongoing remote graphical user interface into the client environment and gain access to many other servers within a short space of time. Through investigation of the local and remote network maps, it was possible to locate servers that were accessible from the contact centre environment that had hostnames associated with PCI systems as well as SQL databases. This allowed the team to quickly home in on target servers associated with the target data. Connections to the databases and manual analysis of the contents using SQL statements allowed the team to quickly identify and locate the target objectives.

Given that Prism Infosec had established a covert channel into the environment, it was straightforward to exfiltrate sample records, which were anonymised to ensure the client's customer data was not fully exposed, yet would demonstrate to the client that the targets had been achieved. It would have been possible to transmit this in a relatively straightforward manner using the client's own Internet connection.

The spear phishing attack was also successful, for which Prism Infosec's technical team crafted an email and a macro-enabled Word document purporting to be a CV. The macro within the email was crafted to avoid the AV technology that had been identified from the open source surveillance and establish a command and control (C2) connection to our servers. After an initial enquiry to ask whether a specific role we had found on the Internet was still open to applications (essentially to identify active monitoring of the mailbox and "warm" the recipient), the document was transmitted to the HR team.

Within minutes the control channel was

established and Prism Infosec's team had control of the desktop within the client environment. This was on a different network to the contact centre, but within a short amount of time access to the same servers within the PCI and database environments was possible.

Prism Infosec had identified and successfully demonstrated two separate attack vectors that would achieve the same goals.

Results and Benefits

Following the exercise Prism Infosec produced the report and risk register entries for the client and formally presented them to the organisation's CISO. The report described in detail how the attacks were planned and executed, including those attacks that were unsuccessful. The output from the exercise clearly identified flaws in people, process, policy and technology (P3T) and provided clear, actionable and pragmatic recommendations on how to address individual issues

as well as root causes. The report also satisfied a number of the PCI DSS requirements for conducting penetration tests and segmentation assessments bringing real value to the client.

The client was delighted with the results as it had demonstrated a simulated cyber-attack on the organisation and identified real methods that could be used to compromise payment and customer data. It was thought that previous assessments that had been conducted had been too narrowly scoped and whilst they had satisfied PCI requirements for conducting annual segmentation testing, they would not identify a number of critical risks associated with the environment.

Furthermore, the testing had been delivered on schedule, within budget and had highlighted gaps in the monitoring and incident handling that were supposedly in place to identify ongoing attacks against the client. Essentially, the client had not received any reports of our activity (or identified the physical backdoor placed within the network) during the entire attack simulation. It was then possible to use the Prism Infosec report output to conduct a period of risk management and a programme of improvements.

The client was not only able to satisfy PCI DSS and Information Commissioner's Office (ICO) requirements but also take away some key core issues that could drive security improvements moving forward:

- **Think about the physical** – how small weaknesses in location, access controls, could be exploited by an attacker;
- **Implementing a polite but firm challenge culture** – how if something does not look quite right it should be challenged, otherwise an attacker will exploit familiarity and trust;
- **Protecting against the "plug-in"** – how the organisation can "buy" valuable time when an attacker is trying to locate an area to host command and control boxes;
- **Network Segmentation** – Defence-in-depth and supporting the organisation with a strong network architecture and segregating key data;
- **[Active] Monitoring** – Ensuring that anomalous activity was identified and responded to;
- **Licensing and Patching** – how all systems are important and to minimise attacker lateral movement;
- **Password Security** –Local admin passwords and privilege escalation;
- **Data Management –** domain access privileges, bulk data access, database encryption; and
- **Internet Communications and Egress Filtering** – the dangers of allowing Internet access on server desktops and ease of exfiltration of data and facilitating C2 connections. ●

TalkTalk Connects to a Secure and PCI DSS Compliant Future with **Semafone**

Cardprotect Voice+ is Semafone's trusted solution for protecting customers' credit card or debit card data during telephone payment transactions. TalkTalk needed a guaranteed way to keep its customer data safe and take its contact centre completely 'out of scope' of PCI DSS and realised it could do this by using Semafone's Cardprotect Voice+ solution.

Background
TalkTalk is a young company with a long history. Established in 2003, today it's the UK's leading value for money consumer and B2B telecoms provider.

The Challenge
TalkTalk handles a significant number of payment transactions each day. With a wide variety of payment methods and channels to choose from, a growing number of customers opt to make online or telephone payments using their credit card.

To keep its customers' personal data safe at all times, TalkTalk uses a form of tokenisation for all card data, irrespective of the channel used to collect it. The data for online channels is secured using a secure iframe with its acquiring bank. With so many customers choosing to pay via the telephone, it was essential that this channel complied with the Payment Card Industry Data Security Standard (PCI DSS).

The PCI DSS has strict rules relating to the way sensitive authentication data, such as the three-digit security code on the back of a payment card is handled to ensure it is kept safe. In the early days, TalkTalk had to ask customers to read their card details out loud so that agents could manually input their payment details onto the system. All calls were recorded and a 'pause-and-resume' method was used to avoid sensitive card data being stored on call recordings. TalkTalk then worked directly with its Payment Service Provider (PSP) who validated and processed the payment.

As TalkTalk experienced rapid market growth, the company realised that it needed a completely new approach to descope the hundreds of checks and controls required by PCI DSS guidelines to keep data safe. That meant finding a robust compliance solution that would enable its contact centre to record the entire telephone call, but not store payment card data.

The Solution
In 2011 TalkTalk was introduced to Semafone and it became clear that the only guaranteed way of taking its contact centre 'out of scope' of PCI DSS was to remove all payment card data completely,

Jashan Sidhu – Director of Bill, Pay & Collect at TalkTalk

and it could do this by using Semafone's Cardprotect Voice+ solution.

Cardprotect Voice+ uses Semafone's patented payment method and dual-tone multi-frequency masking technology (DTMF) to enable TalkTalk's customers to enter their credit card details into their telephone keypad; the incoming card numbers are then intercepted, and the call centre agent is presented with masked (flat tone) digits. Once the system has verified that the information entered is correct, it then seamlessly passes the payment transaction data through to the payment service provider (PSP) for processing, by-passing the contact centre and the desktop environment completely. The solution dramatically reduces the complexity and number of controls required for PCI DSS and allows the agent and customer to remain in full voice communication throughout the entire process.

"Cardprotect Voice+ did everything it promised and the team at Semafone were a joy to work with, supporting us at every step."

Jashan Sidhu, Director of Bill, Pay & Collect at TalkTalk

Jashan Sidhu, Director of Bill, Pay & Collect at TalkTalk, commented: "The Semafone solution appealed, as we could see that it would allow us to handle customer data even more securely and it would be a great enabler to become PCI DSS compliant. Our agents were able to stay in contact with customers at all times during the payment process and the customers felt far more comfortable tapping numbers into their phone than saying them out loud."

The Move to a CPE Solution Within TalkTalk's Data Centre

TalkTalk initially deployed Cardprotect Voice+ 'on premises' in its UK contact centres, later expanding the solution to serve TalkTalk's overseas contact centres.

In its quest to protect customer data, TalkTalk continually tests and challenges its entire network to ensure that payment card data stays 'out of scope' of PCI DSS and remains secure. Previously, card data was transmitted to its PSP, and was potentially still at risk when it touched its systems' network. TalkTalk worked closely with Semafone to create a solution that primarily protected its customers by handling their card data in the best way possible, which in turn allowed the company to gain and maintain its PCI DSS accreditation.

Jashan Sidhu explained: "Cardprotect Voice+ did everything it promised and the team at Semafone were a joy to work with, supporting us at every step. This gave us the confidence to take advantage of Semafone's platform services, which would provide further levels of security by removing the data from our systems completely. We set the wheels in motion to roll out a far more integrated programme that involved moving our call routing through Semafone."

The Implementation

TalkTalk worked closely with its Qualified Security Assessor (QSA), Semafone and its PSP to fully integrate Cardprotect Voice+. A joint project team worked

tirelessly to embed the solution across all systems and ensure payment card data was not stored on TalkTalk's systems by routing it through Semafone's platform.

Like most large scale projects, the delivery, implementation and integration were very complex and required great expertise from both the internal teams at TalkTalk and external partners. The Semafone changes impacted various channels and teams across the business, however, the way in which Cardprotect Voice+ integrates via iframes and embeds payment pages and fragments ensured TalkTalk's customers could continue their journey seamlessly without disruption and TalkTalk is able to ensure its payment journeys are simple, secure and seamless for its customers.

The Benefits

Jashan Sidhu commented: "PCI DSS compliancy was a massive project for TalkTalk and Semafone enabled us to reduce a huge number of applications across our voice recordings and IVR payment capabilities – it simply took away the need to read out card numbers, therefore the information was no longer stored in our voice/IVR application."

The success of this project was a major achievement for TalkTalk, who became one of the first UK Carriers to become fully PCI DSS compliant.

Jashan Sidhu continued: "We worked as a tight unit and Semafone delivered on time, achieving exactly the right solution for TalkTalk. Over 18,000 customers now pay via the telephone each week and they are happy and secure in the knowledge that their data is safe. Indeed, there has been an increase in credit card payments across the board and as a Tier 1 service provider, who is subject to regular external

audits, we are confident that our systems are robust and fully compliant with the PCI DSS guidelines."

Today, the company processes thousands of credit card transactions securely each day via a variety of payment channels. Its team of over 1,200 contact centre agents can now easily and securely handle millions of transactions per year.

> **"We worked as a tight unit and Semafone delivered on time, achieving exactly the right solution for TalkTalk."**
>
> *Jashan Sidhu, Director of Bill, Pay & Collect at TalkTalk*

Jashan Sidhu concluded: "Sadly, the world has changed, criminals are far more sophisticated – we have to continually train our staff to be vigilant and lock the doors behind us at all times, but the good news is that criminals cannot steal data that is not there." ●

CASE STUDY

SILVERFORT

GLOBAL ONLINE PAYMENTS COMPANY BLUESNAP IMPLEMENTS SILVERFORT TO ACHIEVE COMPLIANCE WITH PCI DSS

BlueSnap® As a payment processor, BlueSnap needed to comply with the Payment Card Industry Data Security Standard (PCI DSS) information security standard. PCI DSS v3.2 Req 8.3 requires firms to incorporate multi-factor authentication (MFA) for all non-console access to the cardholder data environment (CDE) for personnel with administrative access, as well as any remote network access originating from outside the entity's network. This includes both users and administrators, as well as third-party access for support or maintenance.

Complying with these requirements is a challenge for organizations, due to the difficulty of implementing MFA for various systems that are part of the CDE.
With regular MFA solutions, this typically requires deployment of software agents on relevant servers, performing local configurations and segmenting the network. For some types of servers and components, implementing MFA is not possible, because deploying 3rd party software agents on them is not technically feasible or not allowed.

Silverfort provides BlueSnap with an easy-to-install, easy-to-use, centrally managed platform that delivers MFA for all user access to all sensitive systems and resources, without the need to modify those production-critical systems in any way.

QUICK FACTS

ORGANIZATION

A global payments company headquartered in the USA, with offices in United Kingdom and Israel. The company provides an All-in-One Payment Platform designed to increase sales and reduce costs for B2B and B2C businesses.

CHALLENGE

- Comply with PCI DSS requirements to enforce MFA for remote and privileged user access to the cardholder data environment
- Find an MFA solution that could support BlueSnap's VPN and VMware systems as well as various Windows and Linux servers without undue complexity and without deploying software agents
- Meet PCI DSS user access audit

SOLUTION

- Silverfort MFA was incorporated to protect non-console access to all CDE systems
- The solution was extended to secure remote VPN access of all users
- A consolidated audit trail was provided for monitoring user access to all systems and resources

RESULTS

- PCI DSS requirements for secure access and a comprehensive audit trail easily addressed
- MFA incorporated for all sensitive use cases within hours, including VPN, VMware systems and sensitive Windows and Linux servers,
- A consolidated audit trail helps track and monitor user access to all systems and resources, including granular detail and realtime risk assessment
- Visibility into shared service accounts allowed the organization to bring those accounts back into compliance with security best practices
- No changes were made to existing systems, no software agents were required

PROTECTING PRIVILEGED USER ACCESS TO THE CDE

To address PCI DSS requirement 8.3, BlueSnap looked into incorporating MFA for privileged users accessing the Cardholder Data Environment. These users included administrators, DevOps engineers, support personnel and BI developers, who access internal production systems. BlueSnap's production systems run on a variety of platforms including VMWare, Windows-based servers and Linux based servers. Privileged users often use non-console access, including SSH and RDP, to connect and work on those systems.

The first system to be addressed was the VMware vCenter Server. The VMware vCenter Server is the centralized management utility for VMware, and is used to manage virtual machines, multiple ESXi hosts and all dependent components from a single centralized location.

Since most MFA solutions do not support an integration with VMWare, BlueSnap was struggling to protect this sensitive system. However, since Silverfort's MFA solution does not require any integration or software installation, it was easily applied to secure privileged access to vCenter.

The implementation was quick and easy. A proof of concept was set up in just a couple of hours, and within a month BlueSnap extended the solution to secure privileged access in all offices across the globe.

Additional policies were quickly added to secure privileged access to other servers, including hypervisors, Windows and Linux servers. Silverfort's MFA was applied on all privileged user access including non-console RDP and SSH access, ensuring all access to these systems was properly secured and PCI DSS requirements were met across the globe.

> ***"Silverfort enabled us to address PCI DSS requirements and easily incorporate MFA to secure privileged access to systems we couldn't previously protect"***
>
> *Michael Rubenchuk, VP of IT Operations and Infrastructure at BlueSnap*

SECURING REMOTE VPN ACCESS

With the MFA system in place to secure privileged access to the CDE, BlueSnap wanted to incorporate Silverfort's MFA solution to secure remote VPN access of all employees. BlueSnap had recently replaced its VPN but the new product was not supported by the existing MFA solution. Incorporating a new MFA solution is not only expensive, but is also painful to implement, as most MFA solutions require custom integrations and configurations.

BlueSnap was looking for a cost effective MFA solution that could support the VPN as well as its sensitive internal systems from a single platform.

Silverfort's agentless technology allowed the company to incorporate MFA for secure VPN access using the same Silverfort platform that was deployed to secure privileged access to the CDE. Silverfort's unique architecture enabled holistic protection without the need to make any change to the VPN or undertake any custom integrations or additional software installations.

User enrollment to the Silverfort mobile MFA app, that receives the push notifications for required authentication, was completed within a few days, and provided a frictionless user experience.

TRACKING AND MONITORING ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA

To comply with PCI DSS, BlueSnap not only required MFA, it also needed to address requirement 10 to track and monitor all access to network resources and cardholder data. Before implementing Silverfort, the company used several tools to audit user access to systems – each tool providing limited coverage and generating a standalone audit trail in its own format.

With Silverfort's Authentication Platform, BlueSnap has a consolidated audit trail for all user access across the entire organization, including on-premise and cloud systems. Since Silverfort monitors and analyzes all authentication activity, it provides unparalleled visibility into user activities across the different systems and resources in a single audit trail. This enables BlueSnap to easily track and trace back suspicious activity to a specific user. Silverfort's unparalleled networkwide visibility is also leveraged by its Risk-Engine to analyze the user's behavior and calculate a risk score. The user's risk score combined with the organization's overall risk level is utilized by Silverfort to apply risk-based adaptive authentication policies.

DETECTING USAGE OF SHARED ACCOUNTS

As a byproduct of this visibility, BlueSnap was able to detect the use of privileged shared accounts from various endpoints for accessing different resources. Shared accounts are considered a bad practice because they create insufficient audit trail, don't allow accountability of a specific person/system in the case of unauthorized or malicious use, and often lead to bad password management habits.

Once detected, these accounts were replaced with more suitable personal accounts.

"Other solutions were difficult to implement. Silverfort saved us a lot of resources and time by avoiding any modifications to our systems."

Michael Rubenchuk,
VP of IT Operations and Infrastructure at BlueSnap

CONCLUSION

With Silverfort, BlueSnap can now comply with the PCI DSS standard by securing remote and privileged access with MFA and auditing all user access across the organization.

Silverfort's Authentication Platform enabled BlueSnap to meet PCI DSS requirements for all its systems, including systems it couldn't previously protect, without installing software agents, without complex architecture changes, and without custom and expensive integrations.

BlueSnap was able to easily extend MFA for all the organization's users and to any system or resource and gain unparalleled visibility with a consolidated audit trail.

CONTACT US
US: (+1) 646.893.7857
43 Westland Avenue, Boston, Massachusetts

Israel: (+972) 54.660.0161
30 Ha'arbaa St, Floor 26, Tel Aviv, Israel
info@silverfort.com

Silver Lining – Every CLOUD has one!

A fixed-price, one-stop solution allowed this client to achieve payment security for their customers as well as improving end-user experience.

The customer
With over 45 years' experience in providing 'non-standard' insurance cover, one of the UK's largest independent insurance brokers engaged Silver Lining Convergence to improve their IT and telecommunications estate.

The challenge
Their existing systems provided minimal ROI against the substantial monthly costs it incurred, allowed too great a margin for error, and consumed inefficient agent/man-hours. With the heightened PCI regulation, compliance was also an increasing priority. Silver Lining worked with them to identify that the issues they were encountering were largely due to the use of outdated and inefficient technologies.

The solution
Silver Lining delivers a vast array of IT and telecommunication solutions utilising our privately owned and operated 4th generation cloud infrastructure. Complete ownership to this level enables us to guarantee security and uptime for our customers providing a 99.999% up-time guarantee. We are also able to tailor bespoke solutions to resolve our customers issues.

Following a comprehensive review of existing systems, we were able to provide a detailed roadmap proposing our PCI-SIP product to the customer. It was agreed to deploy a variety of new available technologies which would support the planned business growth, whilst improving customer experience and retention, achieving PCI DSS compliance, and importantly delivering significant cost savings to the business. This product integrates with their existing back-office systems to enable smooth business processes and allows us to automate processing functions, reducing errors and ultimately agent handling times, optimising the end-user experience.

The benefits
Having Silver Lining as a single supplier for all services ensured a cost effective, smooth transition from legacy systems to new. It also provided payment security for their 90,000 policy holders, lifting their business out of scope utilising our cloud-based PCI solution.

As a Level 1 PCI-DSS certified provider we were able to evidence the benefits of moving their existing payment handling process to a cloud-based operation, offering significant efficiencies in an OPEX model. This presented a 'per-channel' based pricing model and streamlined the onboarding process for new sites and reducing the requirement of costly

hardware and reducing maintenance and management of on-premise solutions.

The outcome

"We chose to deploy the Silver Lining PCI solution due to the ease of implementation, but most importantly because it will provide our customers with a simple and secure process for making payments whilst ensuring they can continue to receive the best possible service from our team of insurance experts.

The team at Silver Lining were able to share their expert knowledge of PCI and worked with us to understand our business model and requirements to ensure the solution aligned with our strategic goals." Associate Director of IT.

Why Silver Lining?

"Working with this client, a leading name in the insurance industry, to design a solution that aligned with their requirements was a simple process, they had a clear understanding of what they wanted in order to continue to provide an excellent level of service to their customers. They were looking for a fixed-cost solution which would allow them to achieve PCI compliance, and help to improve their company's excellent brand within their specialist sector.

Our expert knowledge of all things Telephony, Contact Centre and PCI, allowed for a solution design which is not only aimed at delivering a great secure customer experience, but also aimed at improving the performance and efficiency of the contact centre, helping to deliver a return on the investment for the client." Allan Packer, Managing Director. Silver Lining Convergence Ltd. ●

"Our expert knowledge of all things Telephony, Contact Centre and PCI, allowed for a solution design which is not only aimed at delivering a great secure customer experience, but also aimed at improving the performance and efficiency of the contact centre"

Allan Packer, Managing Director. Silver Lining Convergence Ltd

Sponsors

Advantio
Phone: +353 (0)15065556
Email: contact@advantio.com
Website: www.advantio.com
Twitter: @advantioglobal
LinkedIn: Advantio

CardEasy by Syntec
Contact: Simon Beeching
Tel: 020 7741 2013
Email: simon.beeching@syntec.co.uk
Website: www.syntec.co.uk
twitter @synteccontact

Comforte
Contact: Thomas Stoesser
Tel: +49 (0)611 931 9900
Email: t.stoesser@comforte.com
Website: www.comforte.com
twitter: @comforteAG

Eckoh
Contact: Claire Lynam
Email: Claire.lynam@eckoh.com
Tel: 01442 458419
Website: www.eckoh.com
twitter: https://twitter.com/Eckoh
LinkedIn: https://www.linkedin.com/company/eckoh-plc

ECSC
Contact: Graham Boler
t: 01274 736 223
Email: info@ecsc.co.uk
Website: https://www.ecsc.co.uk

Sponsors

Gala Technology
Contact : Steven Jones
Email: sjones@galatechnology.com
Website: https://www.galatechnology.co.uk/
twitter: @SOTpay

PCI Pal
Contact: Lorna Bradford
Tel: +44 (0)330 131 0342
Email:lorna.bradford@pcipal.com
Website: https://www.pcipal.com
twitter: @PCIPAL

Prism Infosec
Contact: Jas Kaur
Tel:+44 (0)1242 652100
Email: jas.kaur@prisminfosec.com
Website: https://prisminfosec.com

Semafone
Tel: +44 (0)845 543 0822
Email: info@semafone.com
Wesite: https://www.semafone.com
twitter: @semafone

Silverfort
Contact: Dries Robberechts
Tel: +32 474 53 03 02 / +1 202 688 3098
Email: info@silverfort.com
Website: https://www.Silverfort.com
twitter: @Silverfort

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