ShieldQ

Delivering data compliance

PCI Compliance:
Simpler than you think

By Geoff Milton,
Director of Sales, ShieldQ

Hotels: Easy targets for cybercriminals

Many industries must protect sensitive payment card data, but no other industry is so vulnerable to payment card data theft than hotels, because they're at the receiving end of the supply chain, open to multiple points of possible breaches.

The most commonly breached point at hotels is the point of sale *(PoS)*. Even well-known hotel chains have suffered damaging breaches, with malware found in PoS systems, compromising guests' card numbers, names and security codes.

But, while PoS breaches get the headlines, there are many more high-risk payment options in the hotel industry: Bookings made via e-commerce sites, email, fax, telephone and in person at the front desk *(not to mention the back office operations involved with each booking method)* all present their own particular security challenges, many of which security assessors or hotel management have not adequately discussed or addressed. Many of these payment methods actually remain completely unprotected, leaving card data in PCI scope and hotel client's payment card details exposed.

Verizon's 2015 Data Breach Investigations report bears out these findings: over 38% of all major security breaches that occurred in 2014 were within the hotel sector. Strikingly, over 60% of serious breach incidents investigated in this study resulted in card losses, compared with just 43% in the financial services sector. Perhaps the most surprising finding: once the breach underwent forensic analysis, it was found that no organization investigated was proven to be PCI compliant. The majority of these breached hotels faced heavy fines as a consequence, plus the costs of the resulting litigation.

> **"Over 38% of all major security breaches** that occurred in 2014 were within the hotel sector."

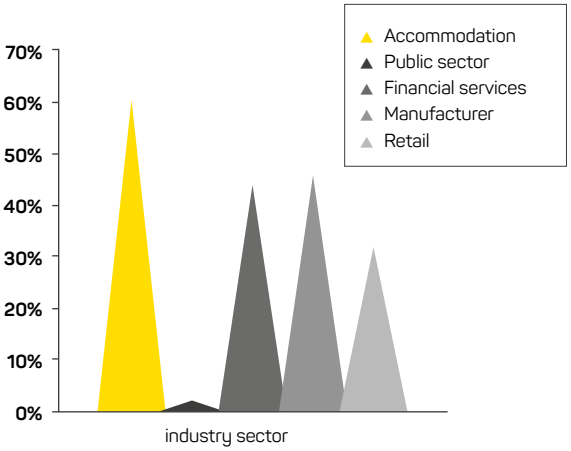
These results have remained consistent for many years, and it seems there is little sign of improvement. On the contrary: it appears the numbers are worsening, as cybercriminals' skills become ever more sophisticated, year after year.

Increased data protection penalties, decreased trust

Until recently there have been little to no consequences for non-compliant hotels suffering a data breach, with the average fine per card being just over $100; relatively

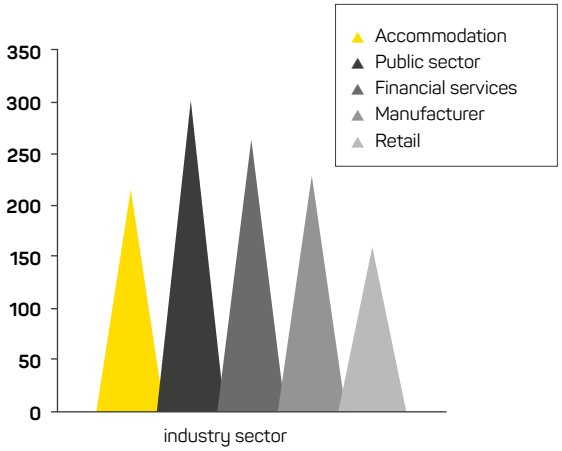
% Of Incidents With Confirmed Card Losses

Verizon Data Breach Investigations Report 2015



Confirmed Serious Incidents With Card Losses

Verizon Data Breach Investigations Report 2015



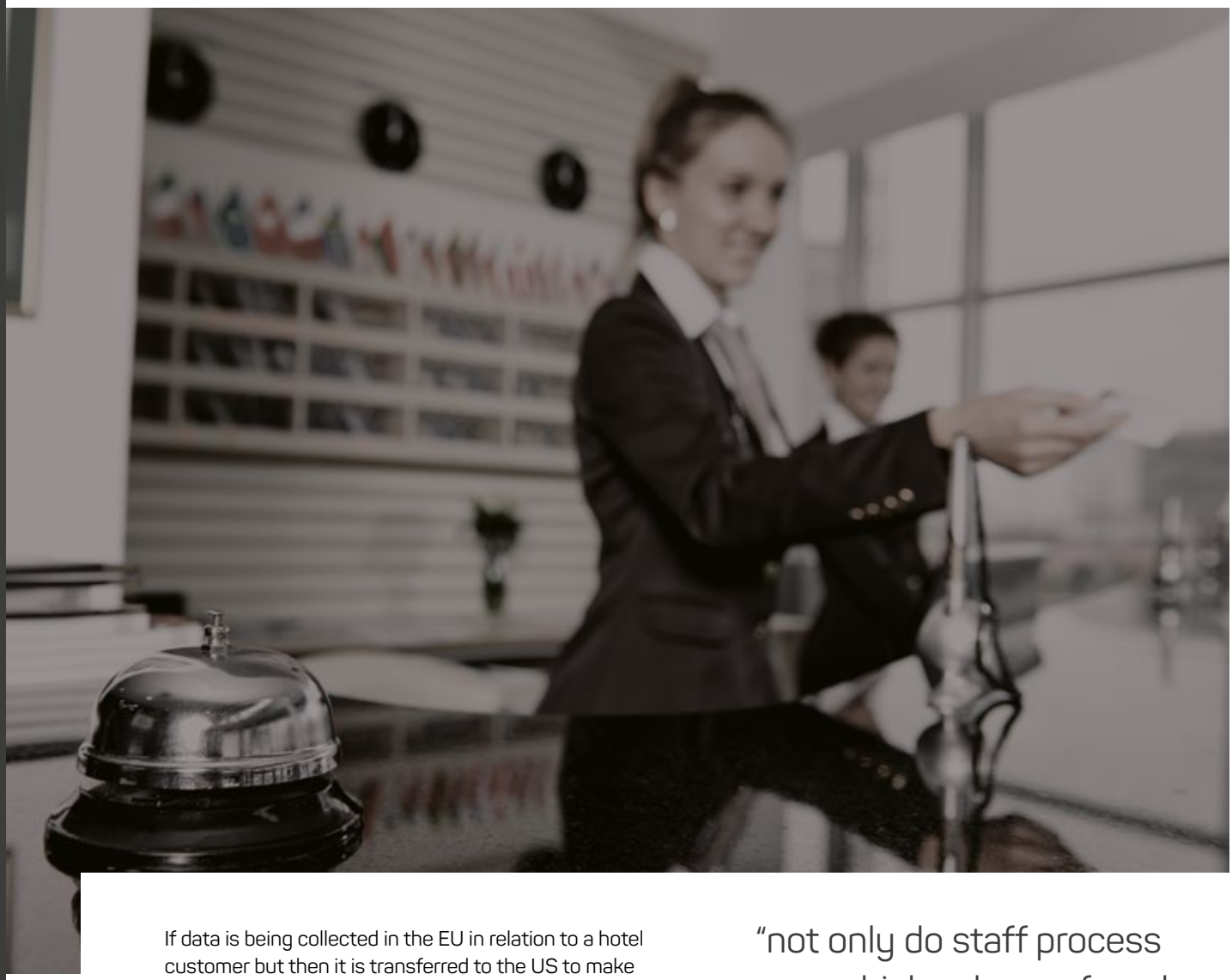
"The European Parliament's new Data Protection Law, effective as of May 24, 2018, will have a profound effect on all hoteliers globally"

insignificant. However, the European Parliament's new Data Protection Law, effective as of May 24, 2018, will have a profound effect on all hoteliers globally – not just within the European Union *(EU)*.

These new rules will apply to all hotels, no matter where they are or where an EU hotel guest may be staying. Currently, it's only hotels in the EU that must adhere to stricter standards than hotels outside the EU. Not any more. With the new regulation, however, all hotels, wherever they are based, will have to apply the same rules when they offer hotel bookings to EU citizens. Thus, for example, if a US hotel group operates in the US or in Europe and holds or processes EU citizens' bookings, then EU data protection rules will apply.

Other key highlights of the new legislation include:

- **Sanctions.** Using a tiered approach for penalties, data protection authorities propose fines of up to 4% of annual worldwide turnover. Other specified infringements can result in fines of up to 2% of annual worldwide turnover.
- **Compliance.** The regulation places huge obligations on data controllers to maintain certain documentation and conduct data protection impact assessments.
- **Breach notifications.** Such notices must be handled without undue delay, and where possible, within 72 hours.
- **Data processing responsibilities.** Those handling data now have direct obligations, including implementing technical and organizational measures, notifying data controllers of breaches and appointing a data protection officer, if required.
- **International transfers.** The rules require informed consent for where data will be stored. When "Safe Harbor rules" were abolished in 2015 hotel groups outside the EU were no longer allowed to self assess their compliance. In advance of the new legislation hotels were anticipating the new European Data Laws would change this ruling and permit companies to go back to self assessment. This has not happened.



If data is being collected in the EU in relation to a hotel customer but then it is transferred to the US to make the booking, the consent requirements have been made stricter.

- **Binding corporate rules.** These apply if a chain of hotel wishes to make inter-group transfers of data.
- **"One-stop shop."** The laws represent one set of regulations for all, including a person's right to request that data to be deleted when no longer required.
- **Extensive audits.** Practically speaking, businesses that process data in relation to EU data subjects must undergo extensive audits to ensure compliance with EU Data Protection Laws. They must be able to demonstrate that they have proper policies and procedures in place, that data within an organization is properly classified and that only the relevant individuals have access to each class of data. Standards such as PCI DSS provide additional requirements on what type of cardholder data may or may not be stored and how it must be protected.

To avoid penalties, most hotels will need to review all their current business practices to ensure they are PCI compliant at all times. Thus, the focus needs to be on all vulnerable aspects of the hotels operations – not only PoS systems – but also e-commerce, fax, email and internal, telephony, front-desk and back office operations.

"not only do staff process a very high volume of card transactions daily, **but they also generally store payment card data in several places and in several formats"**

Size does not matter: Small-to-medium-size hotels are not immune either. While they may have relied on self assessment in the past, they won't be able to, now: VISA has recently announced that acquiring banks must get proof, that even very small level 4 merchants are using PCI accredited solutions.

It's clear that many hotels will need to find a sustainable solution appropriate to their business size and one that can ensure complete round-the-clock compliance.

But where are the risks lurking?

In the hotel industry, not only do staff process a very high volume of card transactions daily, but they also generally store payment card data in several places and in several formats. This sensitive information is also often held for long periods of time.

But let's start at the booking intake, because hotel guest payment card data can enter the hotel supply chain via several methods:

- Automated, third-party booking systems from channel managers, CRS systems and booking engines
- The hotel's own e-commerce website, including guaranteed and prepaid bookings
- Email and fax bookings at the hotel property level, and within hotel booking call centers for non-automated guaranteed bookings and payment authorizations
- Phone and walk-in bookings at the front desk for rooms, conference facilities, catering, meeting room and spa services often confirmed by email or fax
- PoS systems, PMS systems and payment terminals

With all these vulnerable entry points, it's no wonder that hotels are concerned about data breaches. Yet, when you mention the subject of PCI compliance, hotel management can be fairly reticent. And when it comes to front-desk staff? They are barely aware of PCI-DSS's full requirements.

It is also unlikely that staff will even be authorized to talk openly about company specific non-compliance issues, without their very senior management giving the go-ahead. And even then, only under the protection of a non-disclosure agreement *(NDA)*.

Our own anecdotal research yielded a list of the top reasons many companies decide not to go ahead with full PCI compliance **– when all the evidence suggests they should:**

- Very high cost expectations
- Fear of losing business from suppliers down the supply chain, due to non-compliance, such as a hotel chain demanding that their bookers be compliant to safeguard guest's card data
- Confusion about PCI requirements
- False belief that self assessment will be enough
- Conscious decision that the risk of a breach is worth taking

Whatever the reason, there's a lot of misunderstanding surrounding PCI compliance and possible solutions. Hotels don't realize that they can be fully compliant, without investing in lengthy, costly processes.

What your PCI compliant solution should do for you

The tools used by any system will vary according to the organization workflow and size, but the endgame's the same. Most leading commentators in this field agree that a PCI compliance solution should offer:

- **A safe, secure environment:** Ensure that all payment data is stored in one secure place for easy management and retrieval
- **Affordable options:** The service needs to be cost-effective and scalable
- **Flexible, simple, quick deployment:** There should be minimal to no changes necessary to existing business processes, workflows and systems; deployment should be quick, minimizing internal resource requirements
- **Auditing:** The service should be fully compliant with the latest version of PCI standards, with documented and contractual agreements clearly defining areas of responsibility between the hotel and the service provider for all elements that define the PCI DSS standard

Securing guaranteed booking uploads

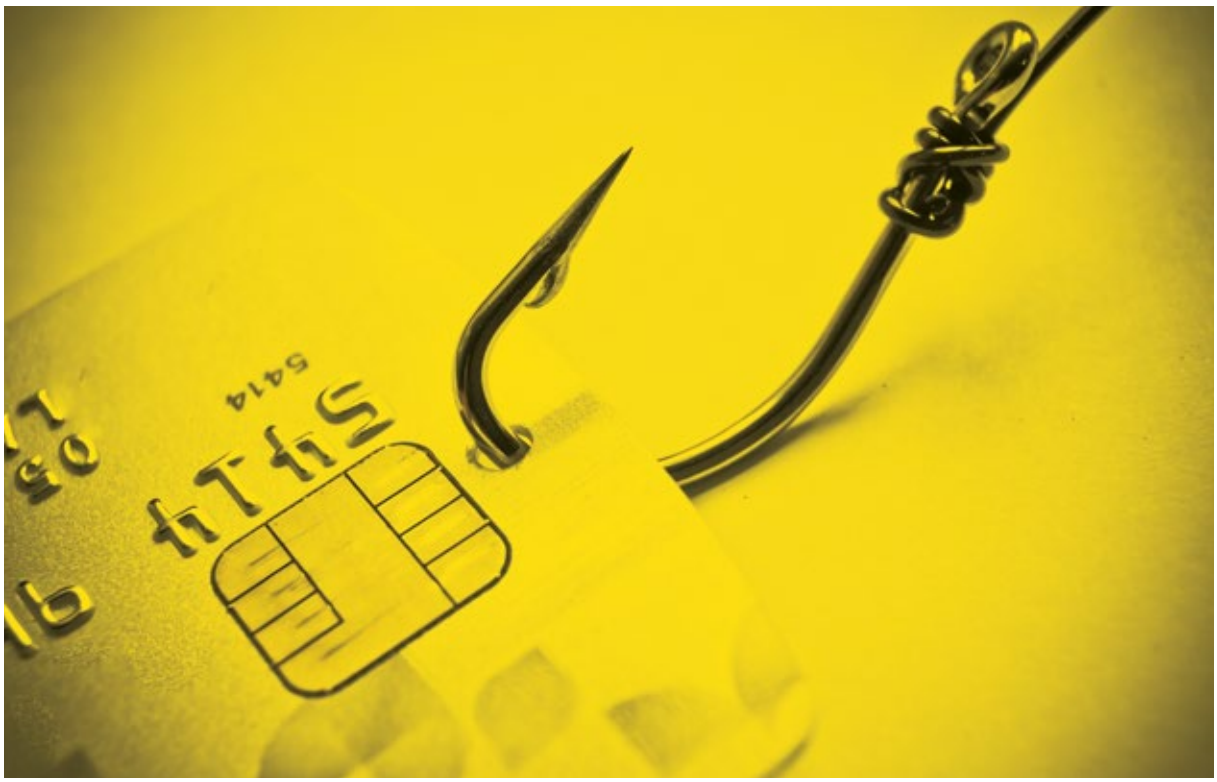
A particular challenge for hotels is the management of "guaranteed bookings" made online on either their website, or an OTA website providing them with bookings. OTAs such as booking.com have always taken such bookings – where payment card data is used as security for reserving in advance – via their websites. This is now becoming much more widespread among OTAs of all sizes, as well as hotels themselves, because consumers demand more choice and flexibility in making bookings.

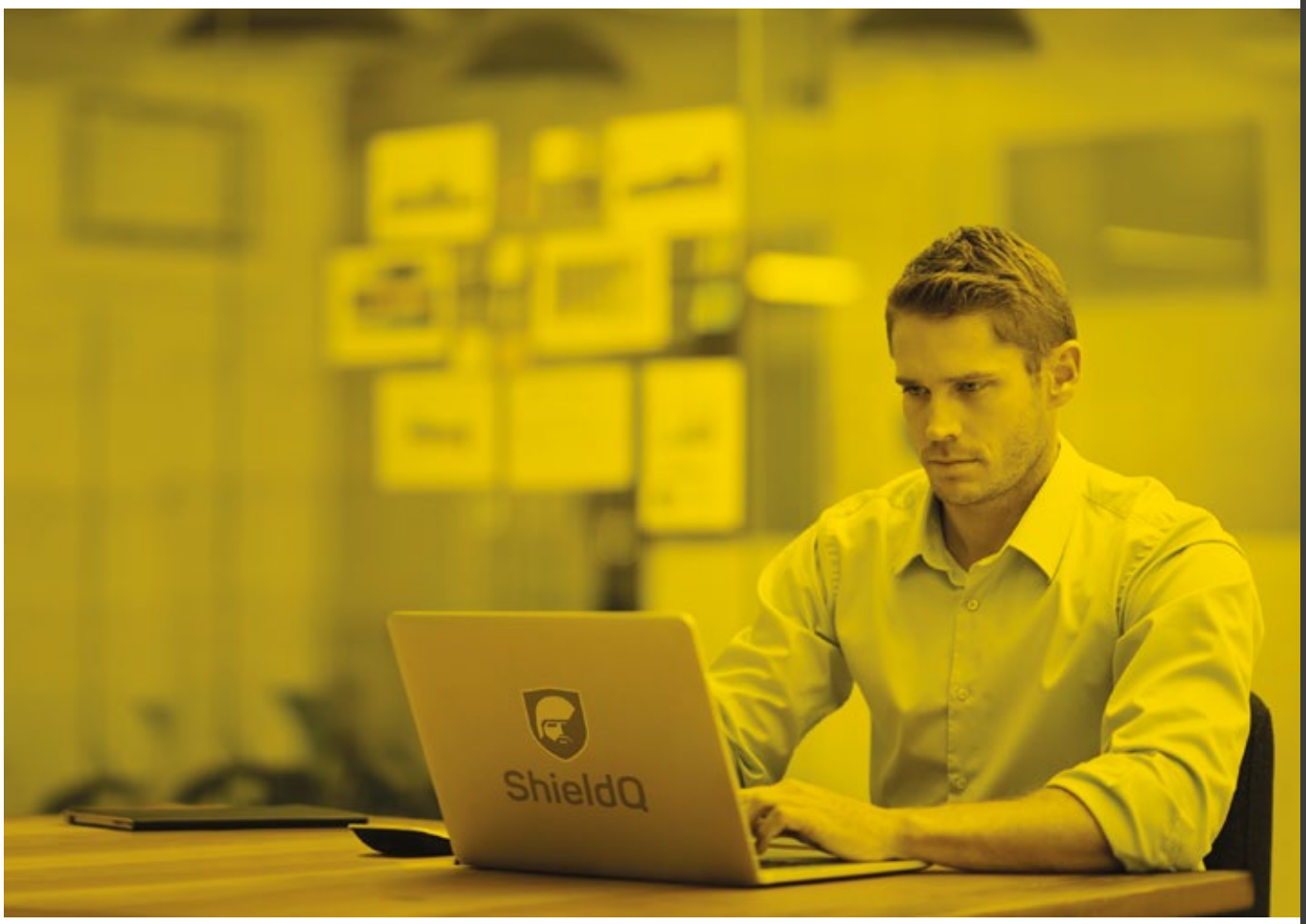
However, guaranteed bookings place considerable demands on whoever holds payment card data for any length of time and makes the cardholder an attractive target for any cyber attack. Whether it's a payment card or virtual card, this data must be captured, transmitted and stored, either by the hotel or via a third party, so that they can process transactions potentially many months or even years after they are first submitted.

For example, the card data must be stored until the guest checks out and usually for a short period afterwards. Unless adequate security measures are in place, hotels and third parties holding card data on their behalf expose themselves
as a prime target for a data breach.

Because even a single card number incorrectly stored, places a hotel in PCI scope.

Despite these real risks, many players in the supply chain and hotels have taken a relaxed attitude to securing this data.





Channel partner accreditation

Service providers play an invaluable role in capturing and storing prepaid and guaranteed bookings from hotel websites, online travel agents, GDSs, travel management companies and event organizers.

The question is, how much do hotels know about these providers' PCI credentials? Based on recent studies, the answer appears to be: not much. Only very recently are hotels demanding that these organizations prove they are PCI compliant. And whenever hoteliers discover that providers are non-compliant, they are finally making sure that something's done about it. We're seeing more contracts being drawn up that attest to PCI compliance.

And it's just in time. With PCI DSS Version 3.1 and the real prospect of higher non-compliance penalties *(either through Visa or through planned changes to legislation within Europe, via the EU Court in 2018),* it's becoming more important than ever for hotels to evaluate service providers' compliance in handling payment card data.

This latest version of the PCI DSS standard delves into the relationship between service providers and their clients, demanding documentation that proves compliance and also drilling deeper, requiring a "Supplier Responsibility Matrix," where the two parties agree precisely which party takes responsibility for each element of PCI compliance and whether their Qualified Security Assessor's *(QSA)* Attestation of Compliance *(AOC)* covers those areas of responsibility.

Each service provider must state in writing their liability for securing the payment card data they hold for the hotel in question. For example, a third party like a CRS must acknowledge responsibility for all card data they hold on their servers for the hotel and must state the method used to capture, process and display card data to the hotel.

These requirements are certainly very demanding. But the reality is, there is no reason why any supplier can't comply, although some have been extremely slow to take action.

Securing faxes: still necessary?

Ask any hotel how many faxes they receive daily and the answer will largely be – very few, or even none at all. But that's not really true. Depending on the hotel location and its status *(independent, part of a larger group),* most hotels grossly underestimate the number of faxes they receive. Generally, individuals fax hotels when they need to make specific requests, which cannot be made online. Other bookings commonly made via fax are for conference/ banqueting facilities or for spa bookings. All these bookings are confirmed using payment card data, either at the time of the booking, or subsequently, using the hotels' credit card authorization form.

And while the entire hotel industry has been saying for years they must stop using faxes, the actual volume in some quarters is now increasing. This is largely due to the rapid growth of virtual cards, which require that faxes be used to "visualize the card," making it easy for front desk staff to identify a virtual card from a regular payment card.

Thus, faxes seem here to stay for awhile. But handling them is a very manual process, requiring printing the fax, punching or masking the CVV number, filing in a binder, and storing it in a locked cabinet for long periods. Some hotels have a locked room dedicated exclusively to the fax machine and the storage cabinets. Unsurprisingly, many faxes simply get lost, wasting hours of staff time to find them.

Despite this activity, and despite some of the safeguards mentioned here, from our extensive experience in the field, we have found that fewer than 5% of hotels make any serious effort to remove faxes entirely from scope and less than 1% are actually PCI compliant. And what most hotels fail to grasp is that a single fax containing payment card details effectively annuls the claim to 100% PCI compliance.

"Depending on the hotel location and its status *(independent, part of a larger group),* **most hotels grossly underestimate the number of faxes they receive"**

With so many data breach risks, both internal and external, it makes sense to make faxes PCI compliant. One solution enables the front desk to capture and store the fax image in a centralized, PCI DSS Level 1 queue. Staff access faxes using two-factor authentication. The solution also provides a full audit trail of who views a fax and when. To further comply with PCI DSS, the fax image is displayed in a browser, with no print or download allowed.

Other PCI inbound fax solution functions are available, much like a PCI DSS document management system in the cloud, where one can share, forward and tag documents. Faxes can be renamed, assigned unique reference details *(such as CRS or booking engine reference numbers)* and then subsequently archived and easily retrieved.

Such solutions – costing no more than a regular fax machine to maintain – are simple and fast to deploy.

Several large hotel groups, including Travelodge in the UK, have implemented such services and have saved tens of thousands of British pounds in labor costs, while vastly improving operational efficiency.

Securing inbound payment card data in emails

Another vulnerability in hotel data security, which may be overlooked but is no less critical, is inbound email management. Even though hotels instruct guests not to send bookings with payment card data via email, many guests still do. To prevent any data leakage issues, some hotels have set up their email servers to filter inbound emails, so that they are quarantined or rejected outright.

While this measure does limit risk in almost all cases, emails still remain in PCI scope: the emails remain "at rest" within the hotel system. The solution is to leverage the existing email application's optical character recognition *(OCR)* and filtering properties to identify inbound emails containing payment card data in the body copy and attachments and to automatically route these messages while they are still in motion *(not at rest)* to a PCI compliant environment. Upon arrival, they can be manually or automatically distributed to users of the service and displayed in a secure inbound queue.

Thus, the email could be automatically delivered, either to hotel booking call centers or to a group of staff at an individual property. Similar to fax management, the authorized user would be required to login to view the email before being able to assign a unique ID, tag, rename, share, forward and archive the document.

However, several alternative solutions can effectively and inexpensively remove emails from PCI scope. One option leverages the existing email application's optical character recognition *(OCR)* and filtering properties to identify inbound emails containing payment card data in the body copy and attachments. This service then automatically routes these messages while they are still in motion *(not at rest)* to a PCI compliant environment. Messages can be manually or automatically distributed to hotel booking call centers or to a group of staff at an individual property, displayed in a secure inbound queue.

Similar to fax management, the authorized user would be required to login to view the email before being able to assign a unique ID, tag, rename, share, forward and archive the document. It's important to note that filtering features available from suppliers such as Microsoft, Symantec and Barracuda vary considerably; not all systems will be suitable for this type of use. A hosted service provider like ShieldQ can provide guidance on whether your legacy system meets your hotel requirements.

Other solutions include:

- Using a mailbox, hosted by a PCI accredited mailbox provider such as ShieldQ, to receive all incoming messages, regardless of content, before delivery to the inbound message queue over the TLS channel. This solution is viable when all messages are processed as being secure, regardless of the content. The primary limitation: the hotel does not maintain its domain name.

- Using a PCI hosted provider, create a new company domain just for secure communication. Thus, hotels can receive all incoming messages, regardless of content, before delivery to an inbound queue over a TLS channel. This solution lets hotels maintain their own domain names. Note: Hosting the domain typically incurs higher setup and account administration fees than the previous options.

This type of solution is ideally suited to hotels, both small and large hotels and is very quick and easy to deploy.

Handwritten notes no more

Large hotels in particular are regularly capturing payment card data manually for long-term safekeeping. In fact, handwritten notes are standardly used for front desk, conferencing and banqueting operations. This card data is held in binders, stored in hotel back offices, where they can usually be accessed by many unauthorized staff. Clearly, this is not PCI compliant and should have been stopped long ago. Yet, this practice remains commonplace in many hotels.

An effective, inexpensive solution lets booking forms, payment card authorization forms and even scraps of paper with sensitive data, be stored permanently in a PCI DSS Level 1 environment: ShieldQ. Using this secure inbound acceptance and storage service, hotel staff and guests can scan or *(more conveniently)* photograph the document using a smartphone, and then immediately upload the image through a document capture iFrame, which allows the PCI DSS service provider's webpage to be embedded on the host's PCI compliant website. The document is then forwarded instantly into a compliant, document management queue. Once safely in the queue,

users can rename, share, tag and archive documents in exactly the same way as fax and email, described previously. Original documents can then be shredded, while the image is permanently deleted.

Hotels may create multiple URLs with the iFrame. The service
is also supplied with CSS files to enable hotels to custom design and integrate each URL into the hotel's website.

Call centers need to be PCI compliant, too

The removal of hotel call centers from PCI scope should be a major priority of all hotels, yet many well-known brands do not currently fully meet the PCI DSS standard. Since the huge increase in online bookings began ten years ago, there has not been much investment in call centers to make them PCI compliant; perhaps because hotels were thinking that they would no longer be needed.

In the past few years, however, both premise-based and cloud-based solutions are available that let customers provide payment card data without the hotel operator seeing or hearing the digits as they are entered into the payment iFrame.

Alternative call center technologies

Pause and resume recording

Pause and resume call recording technology was developed soon after the PCI DSS standard was introduced. This technology pauses a call recording once the payment card segment comes up, to be resumed immediately afterward. Pause and resume minimizes disruptions, while preventing the recording from storing payment card data.

Pause and resume technology can help call centers comply with both PCI DSS and business requirements. However, fundamentally, these solutions are a crude approach to PCI DSS compliance, addressing non-compliance for call recording and storage systems only.

Interactive voice response *(IVR)* payment processing

An IVR solution is not a customer-friendly solution. Guests may view it negatively. But this disadvantage may be offset by significant cost savings. Ultimately, the decision between live agent or IVR payment processing is an individual one, determined by hotel requirements.

But, because hotel agents are removed from PCI scope, IVR payment processing can reduce the hotel call center's compliance burden and fraud risk.

Unfortunately, many IVR payment processing solutions still leave parts of the call center infrastructure exposed to payment card data, requiring additional compliance measures.

Hotels using a hosted or cloud IVR payment processing service can remove payment card information entirely from the call center. This capability decreases call center PCI scope dramatically, as well as reducing compliance cost and complexity.

Dual-tone, multi-frequency *(DTMF)* suppression payment processing

Many think that DTMF suppression payment processing represents the most secure, customer-friendly solution available. Like IVR payment processing, this approach separates payment card data from the voice conversation, to remove call recording archives from PCI scope. However, unlike IVR payment processing, it allows a conversation with a hotel sales agent to continue while payment is made. With this technology, customers enter payment data using their telephone keypad; the resulting tones are suppressed before they reach the call recording system, to prevent storing card information. More sophisticated solutions will suppress the tones before they reach the agent, or with a cloud service, before they reach any contact center infrastructure.

Scalability

A disappointing feature of all current call center technologies is their lack of scalability. Any of the four available solutions can accommodate a hotel call center with 150 desks or more, but are not suitable for an individual property or a small cluster of hotels, where only a handful of staff process inbound calls. And while some suppliers will disagree, there is really no cost-effective solution for this sector.

The challenge to all PCI related service providers, will be to bring PCI compliant telephone payments to the mass market at a reasonable price.

Last, but not least: PoS protection

The primary cause of PoS breaches appears very simple to fix, but is actually more difficult to resolve. Many PoS systems operate using unsupported Windows versions, which are easy, lucrative targets for cybercriminals. Malicious software like ALINA, vSkimmer, Dexter and FYSNA target PoS devices and are widely available in the cybercrime community.

For optimum PoS security, prevention should include *(but should not be limited to)* the following:

- Deploy the latest operating system on all PoS devices with the latest patches
- Limit access to the Internet
- Implement hardware-based point-to-point encryption
- Institute an IP lockdown on PoS terminals
- Auto-delete payment cardholder data from terminals
- Employ PCI access control procedures to restrict PoS systems only to their intended uses
- Limit internal access to physical PoS devices
- Enforce policies regarding PoS physical repair and/or upgrade
- Deploy security software and keep it updated with the latest signatures

Network security measures should include:

- Maintain regular checks to identify if devices have been tampered with or have been replaced with bogus devices
- Patch vulnerabilities and monitor for changes in system components
- Ensure that the hotel is constantly protected against vulnerabilities in both systems and applications, even in-between patch cycles
- Protect against malware and malicious URLs
- Encrypt communication between applications and data
- Restrict two-way communication to only what is required

Conclusion

It may seem daunting to become 100% PCI compliant, given all the complex issues. But now more than ever before, it is achievable and easier than you can imagine. All the required tools are readily available at low cost and are simple to implement – if you know where to look.

Yet, you still may have many questions. Contact us about any of the topics discussed in this document and we'll do our best to answer as fully as possible.

ShieldQ

Delivering data compliance

Contact us

Global offices:

Interfax Communications Limited
Unit 7, Coolport
Coolmine Business Park
Blanchardstown, Dublin 15
Ireland, D15 HC91

Phone: +353 1 905 8968
Email: sales@shieldq.com

UK offices:

Interfax Communications Limited
85 Tottenham Court Road
London,
W1T 4TQ,
United Kingdom

Phone: +44 (203) 3550 869
Email: salesuk@shieldq.com