



## Protecting Guests, Protecting Reputations: The Risks of Not Securing Guest Transactional Data

By Edward St. Onge | Executive Chairman | EZYield

In a world where everyone is increasingly engaged with online transactional systems, it is readily apparent that the convenience afforded by live information sharing and online payment services must be balanced and underscored by a solid security framework. In the hotel sector, where card payment technology to book rooms and for actual transactions during guest stays is common, it becomes a much higher priority. Smart hoteliers can combat this risk by adhering to the Payment Card Industry Data Security Standard (PCI DSS).

**PCI compliance** is a hot issue especially in the world of reservation processing. As the online travel industry moves away from manual data entry towards automated reservation delivery, many hotels and vendors are finding themselves having to comply with data protection standards that rival those that need to be met by governments and international banks.

The need for security compliance in the hospitality sector was recently highlighted by Trustwave, a Visa Qualified Forensic Investigator (QFI), who stated, "research investigated more than 210 card compromise incident investigations, of which 38% occurred in the hospitality sector."<sup>(1)</sup> This figure is alarming, and highlights the particular vulnerabilities the hotel sector faces around guest data security and how attractive the sector is to hackers.

### Protecting Vulnerabilities

For too long, the hotel sector has been viewed as a soft target by hackers seeking to steal guest data. While some hoteliers are taking guest data security seriously, there are still too many operators using inadequate technology and processes to fully protect data. Indeed, even in sectors where it is thought that a PCI DSS would be level one, this isn't always the case, and we've seen

fairly simple security flaws highlighted earlier this year with attacks on Citigroup, Sony and security company, Lockheed Martin.<sup>(2)</sup>

Any breach of data security is serious, and can have severe consequences in terms of loss of revenue, but also for the business's reputation and customer loyalty. It goes without saying that no guest wants to risk staying at a hotel if they are not confident that their personal information is safe. As a result, it is more important than ever to reassure customers that there are solid security measures in place to protect their information through online booking tools and when using credit cards within the actual hotel.

### Minimizing Fear is as Important as Eliminating Risk

Research put out by the US Federal Trade Commission has stated that "six times as much revenue is lost each year to fear of fraud than to actual fraud."<sup>(3)</sup> Credit card fraud is a growing concern for customers, with a CyberSource survey conducted in 2009 revealing that "71% of consumers are concerned with the level of risk when shopping over the web, an increase of 5% over 2008"<sup>(4)</sup>. These concerns are not surprising considering there are several factors that can undermine security efforts, including weak default system passwords, inadequate firewalling and insecure remote access applications. Hoteliers have to recognize the concerns of customers around the risk of fraudulent activity and make it a priority to focus on developing trust and loyalty. This is often done by ensuring they operate at the highest level of security compliance.

To adequately protect guest data, it is not enough to simply purchase new technology. Software, hardware, firewalls and encryption programs are important, but without proper staff training, constantly monitoring of



transactions and data access, and ensuring that all hotel vendors operate with proper security systems themselves, guests can still be left at risk.

### Understanding Regulations

To protect the viability of a hotel business and manage customers' interests, it is imperative that hoteliers understand how the payment card industry is regulated. The chief body in charge of monitoring and assessing security in the field is the PCI Security Standards Council. This body was established by the major credit card companies in September 2006 as an independent organization to manage the Payment Card Industry Data Security Standard (PCI DSS). According to the Council, "compliance with the PCI Data Security Standard (PCI DSS) is vital for all merchants who accept credit cards, online or offline, because nothing is more important than keeping your customer's payment card data secure."<sup>(5)</sup> While security compliance (and non-compliance penalties) ultimately come under the banner of individual payment brands' protocols, rather than the Council, the guidelines established by the Council provide a firm framework for hotel businesses to operate within. While most hoteliers realize some level of security compliance is necessary for effective operation, the decision as to what level of security is provided still comes back to the individual hotels and vendors. The compliance process is assessed and adhered to at a particular level depending on the needs and priorities of these individual businesses. There are four levels of compliance outlined by the Council, each with specific adherence requirements. Level one merchants are those that process over six million Visa or Mastercard transactions per year. The levels are tiered to down to four, where the merchant processes no more than 20,000 e-commerce transactions annually.<sup>(6)</sup> Therefore, the size of the business will determine which level it falls under, as self-evidently a larger hotel is likely to process more transactions. Until a vendor is processing several million credit card transactions per year, the level of compliance they are expected to meet is rather subjective.

In order to be classed as a Level One PCI compliant vendor, an independently authorized auditor must

assess the vendor annually. As part of this process, an auditor will perform several independent scans of the vendor's environment and will require regular internal and external scans. These people verify that all requirements have been met by collecting documented evidence for each and every requirement. They also verify that the vendor has regular reviews of its compliance procedures throughout the year and has mechanisms in place to detect and respond to potential threats both from the outside world, and from within the company itself. Since it requires the most rigorous monitoring, Level One compliance constitutes best practice and makes sense that businesses that operate at the highest security level are expected to be more reputable and yield higher profits.

The PCI Security Standards Council offers training and advice to hoteliers to assist with ongoing compliance within the business framework and there are self-assessment questionnaires readily available that hotels and vendors can engage with to assess compliance. What this means for hotels that rely on vendors to handle their most sensitive data is clear: a vendor can claim PCI compliance by filling out a self-assessment questionnaire and performing an automated software scan every three months. This level of compliance may just be suitable for a small e-commerce store but it could mean disaster for hotels that rely on secure processing of sensitive data and who process thousands of credit card transactions on a daily basis. Using a Level One compliant vendor such as EZYield for critical business needs is the smartest way to ensure that the data is safe.

### Building a Secure Culture

The risks and reputation damage to the business in the event of a security breach should be weighed up as significant motivation for engaging with security processes of the highest level. However, a culture of security awareness at all levels of a hotel business will go a long way towards counteracting breaches. The risk to reputation and revenue should provide the incentive for large (and ultimately all sizes) businesses to operate at the highest level to ensure security best practice. However, true security is not only about having a seal of



approval: it also demands the establishment of a culture of protecting your customers and your data. To have real peace-of-mind, data security should not just be an annual or quarterly review but instead a mission embraced by all ranks within an organization and its partners. Several layers of security should shield sensitive data and multiple steps should be required when accessing data in its raw unencrypted form.

**Practical Advice**

There are a series of steps that hoteliers should look to take to maximize security around guest data (that doesn't involve turning your facility into Fort Knox) and these are:

- *Create a proactive security protocol: It's important to ensure that there are the right supporting protocols to complement the technical aspects of compliance. Ensuring that your staff is aware of not only how things work, but how it is implemented at a practical level, and how it affects their roles will ensure that the system is easily integrated into the operation.*
- *Know your vulnerability points: Whether it's making sure that all your web transactions and connections are secure, or simply ensuring that the brand website is as protected against hacking as possible, get across it. Additionally, with external providers and in-house operations such as CRS/PMS; CRM systems and connections between OTAs and PMS, ensure that they're as secure as you are.*
- *Ensure PCI level one security from all transaction vendors: While this seems to make sense, if you're only finding out that your transaction vendors are level two or below after an event, it's far too late.*
- *Periodic reviews: While it's a step in the right direction to implement these processes, it's just as important to maintain them. Just because you've bought the car, doesn't mean that you shouldn't take it in for a service to keep it running at its best.*

The hotel sector is particularly at risk because there are often outside vendors involved in the card payment process. If security guidelines are adhered to across every department of the business, and a security conscious culture is reinforced, then a comprehensive approach to maintaining appropriate compliance will be achieved. The benefits of utilizing online payment methods are clear. However, to be truly competitive and safeguard a reputation for being secure, hotels need to actively engage with credit card security compliance measures (or at least employ partners who do) and make an effort to keep updated on the current standards that are in place. For the hospitality industry, the jump to automating data delivery to property-level systems means sharing critical data across multiple vendors. This leap, however, does not have to mean greater risk for hotels and their customers. By utilizing PCI certified partners, hoteliers around the world can be confident that not only is guest data protected, but their own hotels reputations are safeguarded against the growing threat of fraud in the hotel sector.

**References:**

1. "Protecting Cardholder Data for Hospitality Businesses Accepting Payment Cards Through Multiple Channels: Hotels, Motels and Lodging"
2. [http://www.theregister.co.uk/2011/06/14/citigroup\\_website\\_hack\\_simple/](http://www.theregister.co.uk/2011/06/14/citigroup_website_hack_simple/)
3. <http://www.ethoca.com/fraud-intel/bid/36951/Fear-of-Online-Credit-Card-Fraud-Shrinks-Pool-of-Good-Customers>
4. <http://www.ethoca.com/fraud-intel/bid/36951/Fear-of-Online-Credit-Card-Fraud-Shrinks-Pool-of-Good-Customers>
5. <https://www.pcisecuritystandards.org/merchants/>
6. "Protecting Cardholder Data for Hospitality Businesses Accepting Payment Cards Through Multiple Channels: Hotels, Motels and Lodging" <https://www.trustwave.com/whitePapersRequest.php>



*Edward St. Onge currently holds the position of Executive Chairman at EZYield, the premier global provider of online distribution management solutions for the hospitality industry. A recognized technology innovator with a passion for service, he co-founded EZYield in 2002 and over the next 9 years established many of the channel management and automation best practices that are embraced by the industry today. Mr. St. Onge can be contacted at 321-765-8419 or edwards@ezyield.com*