Data Breaches & Security: What You Need to Know About Payment Gateway Solutions

by Ravi Angadi

There’s a lot of talk in the hospitality industry these days about data breaches. Unfortunately, hotels are particularly attractive targets for data thieves because of an increase in online bookings, the number of collection channels available to consumers, and the large volume of guest information that resides on hotel systems.

The cost of a breach can be astronomical. It not only exposes the hotel to regulatory scrutiny, but also to lawsuits that may arise from local and federal regulators, banks and guests. Then, of course, there is the loss of consumer confidence and damage to the corporate brand, which may be impossible to regain.

So, how can you minimize the risk of a data breach at your property? The first and most important step is to implement a secure payment gateway solution, which protects guest credit card data in both card-present and card-not-present scenarios. It uses encryption and token-based obfuscation to ensure that data is passed securely between the guest, the hotel and the payment processor. It integrates with your property management and point-of-sale systems to provide seamless payment services.

What to Look for in a Payment Gateway

Although many providers claim to leverage secure technology for payment transactions, hotels should be cautious about false claims and misstatements. When shopping for a payment gateway solution, look for the following six features:

• **Point-to-Point Encryption** – A point-to-point encryption (P2PE) solution uses a combination of secure payment devices, applications and processes to transform data into an unreadable code from the point-of-interaction until it reaches the solution provider’s secure decryption environment. P2PE essentially protects cardholder data transmitted from the hotel’s network, thus offering the greatest possible security for guest information and reducing the potential for data breaches.

• **PCI-Validated P2PE Security** – With the proliferation of P2PE solutions in the market, the Payment Card Industry (PCI) Security Standards Council stepped in to specify criteria that would ensure PCI scope reduction. Only solutions that adhere to the strict requirements of the latest specification are deemed to be validated by the PCI Council, and only those solutions can guarantee scope reduction without the additional burden of a full PCI audit. For example, only hardware-based encryption methods are acceptable for guaranteed scope reduction. Validated solutions are listed on the PCI Council website.

• **Tokenization** – In addition to the encryption of card data, tokenization can completely eliminate storage of card data within the hotel system or network. Encrypted card data sent to the gateway is replaced by a secure token, which is then used as a stand-in for future payment transactions for that specific card. Tokenization allows the hotel to safely store card data for future use, including returns and incremental authorizations, without the risk of compromising guest information.

• **Payment Information Proxy** – In a complex payment environment, such as exists in the hospitality industry, even validated P2PE protecting on-premises systems may not be sufficient to secure cardholder data collected via third-party e-commerce interfaces, such as online travel agents. A payment information proxy, or Pip, secures these transactions by not only encrypting all data transmission but also by intercepting e-commerce messages containing card data, extracting the card data from the message and replacing it with a token. The ‘sanitized’ message is then forwarded to the property management system or POS system, ensuring that the property’s infrastructure remains secure.

• **Multiple Payment Device Support** – The payment landscape is shifting quickly, and a payment gateway must be able to keep up with the changes. It should support a full range of fixed and mobile EMV-ready and contactless payment terminals (such as for Apple Pay™). ‘EMV’, which stands for Europay, MasterCard and Visa, refers to a specification for the technical requirements of chip-enabled payment devices. The range of devices supported by a gateway should also integrate with point-of-sale applications so that it covers a variety of scenarios, including lodging, food and beverage, back office and mobile (both staff and guest-facing, such as pay-at-table). Remember that with EMV, the card remains with the guest; thus, the guest becomes an integral part of the payment flow. Make sure the solution accommodates both chip-and-pin and chip-and-signature situations while avoiding delays and awkward guest interaction.

• **Processor Coverage and Flexible Integration** – One of the advantages of a payment gateway is being able to seamlessly switch processors. Make sure the gateway has broad coverage for preferred processors. Also, a payment
gateway device should be able to integrate with key property management and point-of-sale products. This allows for unified and secure payment processing across the entire enterprise.

**Common-Sense Strategies**

Aside from implementing a secure payment gateway, there are some common-sense strategies that can help guard against a data breach.

One of the top strategies is employee education. Staff is the first line of defense against data breaches, and all employees should understand their responsibility in protecting the hotel. Another advantage of a PCI-validated P2PE solution is that it requires the gateway provider to supply a P2PE Instruction Manual (PIM), which outlines the administrative tasks staff must perform in order to ensure guaranteed PCI scope reduction.

Also, include security training in new employee orientations and offer an annual refresher course for all staff. Keep data security policies on the network so employees can access the information quickly and easily.

Prohibit staff from visiting social media and other personal websites while at work. Many sites – even some that look legitimate – create a means for hackers to infiltrate a network. To ensure compliance, you may want to install software that tracks employees’ internet usage.

Understanding the complex merchant environments common to the hotel and casino market is important when selecting a payment gateway solution.

*Ravi Angadi is Vice President of Product Management for Agilysys. He can be reached by calling (800) 241-8768 or email ravi.angadi@agilysys.com.*