By Tia D. Ilori

myth BUSTERS 2

Common Payment Card Security Myths Dispelled

Given the complex nature of the typical hospitality industry payment system, it's not surprising that some confusion may arise about acceptance practices and their implications on security. Nevertheless, when it comes to protecting your operation and your guests from data theft it's important not to be taken in by myths. Let's take a look at three common payment card misconceptions in the hospitality industry.

Myth 1

The card verification code should be collected during the outset of a reservation, in the event of a no-show.

It is normal for a hotel to charge a guest's payment card when they check in rather than at the time the reservation was booked. Under the mistaken belief that they can better protect themselves against a no-show, some operators will store the card verification code along with the cardholder's other account details, holding it until the cardholder's actual arrival.

The card verification code is the three-digit or four-digit number usually printed on the back of a payment card. It is used to help verify that the user is in actual possession of a valid card in transactions for which the card is not actually present (such as online or over the telephone). Visa refers to the code as the CVV2. Criminals covet the card verification code because if they can pair it with a valid account number, they can then use it to commit fraudulent online, phone or mail purchases.

If the card verification code is collected and stored during the reservation, the data creates a significant security risk during the subsequent days or weeks leading up to the cardholder's check-in. Hackers are adept at extracting this sensitive data, which is why Payment Card Industry Data Security Standard (PCI DSS) requirements prohibit its storage.

Any hotel that stores the card verification code runs the risk of data compromise without any potential benefit. The fact is that in the event of a no-show, the hotel may charge the guests for the stay in accordance with Visa's rules. Further, storing the code for subsequent processing will not remedy a fraud chargeback.

The bottom line: Collecting and storing the card verification code during the reservation process provides no protection against no-shows and places hotel payment systems at risk for exploitation by data thieves.

Myth 2

It's preferable to have guests fax in a copy of their credit card information to reserve a room.

What we hear from time to time is that hotels mistakenly believe they are obligated to obtain a fax copy of a cardholder's credit card information in order to validate the authenticity of the card for a phone reservation. This is because some hotel operators believe that a fax serves as extra protection in case the guest is a no-show.

> Collecting and storing the card verification code during the reservation process provides no protection against no-shows and places hotel payment systems at risk for exploitation by data thieves.

This is problematic from both a business and a data security standpoint. First, the merchant will likely key-enter payment details into the property management system. Because the sale is processed as key-entered, but not electronically read, the merchant would not be protected against a fraud chargeback. Additionally, a fax containing payment detail would not be viewed as evidence that the cardholder participated in the transaction.

Should a hotel wish to protect itself against a fraud dispute, it should consider electronically reading the card once the guest has checked in. Hotel operators may also use technologies such as Verified by Visa that can authenticate the cardholder during an online transaction.

Secondly, requiring a guest to furnish payment card information through a fax transmission provides another stream of sensitive payment data that needs to be protected by the merchant. Fax transmissions sent or received through the Internet must be encrypted. Additionally, any systems such as a fax or email server that cardholder data passes through must be secured according to PCI DSS requirements. In addition to creating an unsecured channel, paper printouts sitting on a fax machine typically lack the physical protection necessary to ensure that only authorized personal are able to access sensitive data. Hard-copy records with payment card details must be handled with appropriate caution.

In some instances, hotel operators have requested not just a typed fax of the standard payment card details, but have asked for an image of the front and back of the card. In doing so, the hotel operator is receiving the card verification code or value printed on the back, or possibly the front of a payment card. Any merchant that stores a copy of that code – even if it's a printed copy – does so in violation of the PCI DSS requirement that prohibits storage of this code.

Faxing payment card information is not just unnecessary, it's a bad idea that puts your hotel at needless risk of data exposure.

Myth3

If I use the online reservation system offered by my franchisor, they'll cover me if their system is breached and my guest's personal information is compromised.

That could be a dangerous assumption. Whether or not a franchisor assumes liability in the event of a breach of its systems depends on the contract between the franchisor and the franchisee. It's important to be aware of all the terms of the contract as it pertains to the responsibilities for maintaining the security of the payment environment.

The potential exposure is even greater for non-franchised properties using third-party reservation system providers or wholesalers.

In addition to knowing their responsibilities, franchise operators should know the technology they are using and familiarize themselves with the vulnerabilities and mitigation strategies common to their payment environment. For example, they should use firewalls, and ensure that their payment card processing system is completely segregated from public networks and other business systems, including their franchisor or service providers. Usernames for payment processing systems and other business applications should be unique and not shared by employees. Passwords should follow the PCI DSS password guidelines. All systems should have security patches or updates applied as soon as possible.

Don't assume that your franchisor is protecting your operation from a data compromise or subsequent financial liability in the event of a breach. Become familiar with your payment system technology, vulnerabilities and mitigation strategies, and liability provisions of your relevant contracts. If you are using a third-party service provider, you can refer to Visa's approved list at http://www.visa.com/splisting/LearnMore.html.

TIA D. ILORI *is a business leader of the Americas Payment System Security group with Visa Inc.*

Mag.hospitalityupgrade.com

Go to our digital edition or our app version for the following hyperlinks.

See storage restriction requirement 3.2.2 at https://www.pcisecuritystandards.org/security_standards/documents.php)

Visa's rules about storing card verification code: http://usa.visa.com/download/merchants/visa-acceptance-guide-lodging-industry.pdf

For more information on common vulnerabilities and mitigation strategies: http://usa.visa.com/download/merchants/bulletin-ecommerce-vulnerabilities.pdf and http://usa.visa.com/download/merchants/targeted-hospitality-sector-vulnerabilities-110609.pdf