By Tia D. Ilori

SECURITY OPTIONS

To Future-proof Merchant Investments

Online reservations made though hotel websites and online travel agencies represent the largest and fastest-growing channel for hotel bookings according to TravelClick. The trend is extending beyond the desktop to mobile. According to market research firm IDC, by 2015 more users will access the Internet through their mobile devices than any other device.

The growing sophistication of Web solutions and proliferation of mobile technologies is opening up new frontiers in the hospitality industry. Enterprising hotels are using the Internet not only to facilitate guest booking, but also to better engage customers in loyalty programs and guest services during their stays. With all the promise that lies ahead, hotels need to ensure that they are taking steps to properly secure these new payment channels.

Some hotels are evaluating forward-looking investments in encryption and tokenization as measures to protect and even eliminate sensitive payment card data. The two security technologies can work together harmoniously or even independently. Although they should not be regarded as a substitute for the Payment Card Industry Data Security Standards (PCI DSS), encryption and tokenization are complementary solutions that provide an additional layer of security. Beyond the added security benefits, they may also help reduce a company's PCI DSS compliance scope, by reducing or eliminating the sensitive payment card data present in its environment.

While hotel booking trends underscore the need to secure online channels, it is important not to forget point-of-sale transactions. A third security technology for hotels to consider is EMV chip technology. The trifecta of encryption, tokenization and chip can work together in conjunction with one another to form a strong defense to protect payment card data in the online and point-of-sale channels.

Tokenization is the process through which a payment card's 16-digit primary account number (PAN) is replaced by surrogate values.

Point-to-point Encryption

Point-to-point encryption, also called end-to-end encryption, protects card information from the initial card holder swipe until it reaches the acquiring bank or credit card processor. It applies both to transactions initiated over the Internet and with the card physically present. One of the attractions to hotel operators is that there is no need for the hotel to process or transmit payment card data in the "clear." The fact that it eliminates any clear text data either in storage or in flight means that it would render payment card data useless to criminals in the event they successfully penetrated a hotel's payment system.

In an effort to enhance overall data security in the payment industry and to further the development of point-to-point encryption, Visa developed best practices to assist merchants in evaluating encryption solutions emerging in the marketplace. Point-to-point encryption, where implemented in accordance with these best practices, may help simplify PCI DSS compliance. Merchants should work with their qualified security assessor to determine the impact of a point-to-point encryption solution.

Several companies offer encryption services, and Visa is planning to launch its own point-to-point encryption service later this year.

Tokenization

Another security solution hotels should consider is tokenization. Tokenization is the process through which a payment card's 16-digit primary account number (PAN) is replaced by surrogate values. Hotel operators using tokens in accordance

In an effort to enhance overall data security in the payment industry and to further the development of point-to-point encryption, Visa developed best practices to assist merchants in evaluating encryption solutions emerging in the marketplace.
http://corporate.visa.com/_media/best-practices.pdf

Visa plans the launch of its own point-to-point encryption service.
http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1727178&highlight=encryption

Tokenization best practices to avoid common implementation pitfalls
http://usa.visa.com/download/merchants/tokenization_best_practices.pdf

with best practices will limit PAN storage, significantly decreasing the risk that sensitive payment card data may be stolen by data thieves.

Tokenization may also simplify compliance with the PCI DSS requirements. It's a versatile security technology in that it can be implemented by itself or as a complement to point-to-point encryption. Encryption protects data in flight from the swipe to the acquirer processor and tokenization protects data stored in the merchant's environment.

Tokenization is an effective anti-fraud technology when implemented correctly. To help merchants, Visa has released tokenization best practices to avoid common implementation pitfalls.

A dual-interface chip terminal (shown) can accept contactless card and NFC payments. They also include a slot where the chip card can be inserted.

Chip-enabled, Dual-interface Terminals

While bookings through online channels are growing, it is important to remember the importance of securing the point of sale. The human touch is an important part of the hospitality experience and hotels are likely to move away from in-person check-ins and payment.

In the course of the regular replacement cycle, savvy hospitality industry operators should deploy dual-interface terminals (which support both contact and contactless chip acceptance) in order to accept EMV chip-enabled cards, contactless payments (including mobile) and other emerging payment technologies.

An important advancement coming to the United States is the migration to EMV chip technology. EMV adds an extra layer of security to point-of-sale payments by introducing dynamic authentication values that change with each transaction. This means even if payment card data is compromised, a counterfeit card would be unusable at the checkout counter because the authentication data stolen will no longer be applicable.

In the course of the regular replacement cycle, savvy hospitality industry operators should deploy dual-interface terminals (which support both contact and contactless chip acceptance) in order to accept EMV chip-enabled cards, contactless payments (including mobile) and other emerging payment technologies. Merchants with at least 75 percent of their Visa transactions originating from dual terminals that support both contact and contactless chip acceptance will no longer be required to undergo annual revalidation of their PCI DSS compliance as part of Visa's Technology Innovation Program (TIP). Additionally, using these terminals provides protection under the counterfeit fraud liability shift, which will become effective in the United States in October 2015.

Emerging technology is providing a new wave of opportunities for the hospitality industry. Point-to-point encryption, tokenization and EMV chip technology are three harmonious security solutions hotels should consider when evaluating their payment security approach. They work together to form a strong defense that builds on the foundational security layer provided by PCI DSS compliance. By making shrewd investments in these security solutions, hospitality industry operators can help protect their guests' personal information across payment channels.

Tia D. Ilori is a business leader in the Americas Payment System Security for Visa Inc.