By Tia D. Ilori

MOBILE EVOLUTION

Securing the Next Wave of Payment Innovation

image © audioundwerbung

Over the years, cash yielded to travelers checks. Then it was payment cards that were passed across the check-in counter. Then came the proliferation of the computer, allowing bookings through hotel websites and third-party travel sites to take off. And right now, in your lobby, the payments evolution continues as guests arrive, busily typing away on their tablets or mobile devices.

Instead of using a plastic card, many guests soon will be using their mobile devices to make payments too. Understandably, many hotel operators want to keep in step with their guests and are evaluating how best to implement these emerging payment forms by making online apps available, installing contactless readers or even by accepting payments via tablets, through a device like Square Reader.

The potential value of mobile payments is remarkable, as evidenced in other areas of the globe. In 2005, the British marketing research firm Juniper Research predicted that total transactions via mobile devices would be $155 million that year and top $10 billion by the end of the decade. Not only did mobile payments exceed that forecast tenfold, reaching $100 billion in 2010, but the total for digital and physical goods is expected to reach $630 billion by 2014. As the proliferation of mobile, and specifically mobile payment technologies continues, security will need to be a top consideration for long-term success.

Before we jump into the security guidelines, it's important to first define what we mean when we talk about mobile payments. There are two primary types of mobile payments; those made at the physical point of sale (POS), and in the e-commerce environment, defined by the industry as proximity payments and remote payments, respectively.

Some hotels are leveraging NFC technology to allow their guests to make proximity payments in which a short-range radio signal is transmitted between the mobile device and terminal, initiating the payment and allowing it to be processed through the traditional card processing networks and systems. Some hotels may use the technology to serve multiple purposes such as allowing a customer to pay for a stay while also enabling his or her mobile device to serve as a room entry device.

Unlike proximity payments, remote payments do not require the consumer to be in the store or even in the same country as the merchant. Instead, remote payments bring the convenience of online shopping to a person's mobile device. Remote payments include browser-based payments, similar to a computer-based e-commerce experience, and app-based payments, when the consumer uses a vendor-sponsored application or wallet to find and purchase goods or services. A number of companies offer mobile wallets, including Visa's product V.me.

On the merchant side of the equation, mobile is also changing the way hotel operators can accept payments. Mobile phones are beginning to be used as portable POS devices. In the world of smartphone applications, software is emerging to allow small merchants or individuals to subscribe to payment services where they accept card payments via key-entered card data on their mobile phones. Mobile phone accessories are also emerging that add a magnetic stripe or chip reader to a mobile phone, so that card data can be entered electronically as with a traditional POS device.

> Not only did mobile payments exceed forecasts tenfold, reaching $100 billion in 2010, but the total for digital and physical goods is expected to reach $630 billion by 2014.

The future of mobile payments offers unrivalled opportunity for the hospitality industry, but ensuring the security of these new forms of mobile payments will be critical if they are to take root. As hoteliers harness the power of mobile technology to accept payments and grow their businesses, secure merchant acceptance practices are critical to maintain guests' trust.

Visa recommends the following mobile payment acceptance best practices

Only use Mobile Payment Acceptance Solutions as originally intended. To prevent unintended consequences from the misuse of a mobile acceptance solution, ensure that the solution is used in a manner consistent with guidance provided by an acquiring bank and solution provider. This includes ensuring that any software downloaded onto the consumer mobile device comes from a trusted source.

Limit access to the Mobile Payment Acceptance Solution. Ensure that only authorized users (i.e., designated employees) have physical/logical access to the payment functionality of the solution. Merchants are encouraged to use a passcode, password or security pattern to lock their consumer mobile devices when not in use. The consumer mobile device should be configured to auto-lock after a number of minutes of inactivity.

Immediately report the loss or theft of a consumer mobile device and/or hardware accessory. Contact the acquiring bank immediately to help report the loss or theft of a consumer mobile device and/or hardware accessory to ensure the prompt implementation of any necessary actions. *Consult Visa's guide on What To Do If Compromised at www.visa.com/cisp for step-by-step instructions on how to respond to a security incident.*

Install software only from trusted sources. Merchants should not circumvent any security measures on the consumer mobile device. To avoid introducing a new attack vector onto a consumer mobile device, install only trusted software that is necessary to support business operations and to facilitate payment.

Protect the consumer mobile device from malware. Establish sufficient security controls to protect a consumer mobile device from malware and other software threats. For example, install and regularly update the latest anti-malware software (if available). Merchants should regularly update the firmware of their devices and install any application updates whenever a new update becomes available.

The first and most important security consideration is making sure that hotels consider the security of these new payment channels and that they meet the applicable Payment Card Industry Data Security Standards (PCI DSS). Furthermore, the Payment Application Data Security Standards (PA-DSS) applies to software applications used to accept payment data. The fundamental principles behind these standards would be equally applicable to the mobile space. Additionally, the PCI Council also released some recommended mobile guidelines. (https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf)

Merchants who choose to deliberately subvert the native security controls of a consumer mobile device by jailbreaking or rooting the device increases the risk of malware infections.

Adhering to the best practices outlined above can help limit the exposure of account data that may be used to commit fraud and prevent software attacks on consumer mobile devices.

Visa is helping support secure mobile payment innovation through its newly launched Visa Ready Partner Program. The program is designed to provide innovators a path to ensure that devices, software and solutions used to initiate or accept Visa payments are compatible with Visa's requirements.

Keeping security top of mind when upgrading to new payment acceptance solutions will provide new opportunities to you and your guests while closing the doors to criminals.

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

HU SCAN THE IMAGE ON PAGE 140 with the Layar app to launch the PCI Council's recommended mobile guidelines.