

by Michael E. Smith

# Unwanted Data Retention Can Hurt Your Customers and Your Business

Hotels, resorts, restaurants and travel agents aim to provide their customers with memorable experiences: a gorgeous view, an unforgettable seven-course dinner, a unique riverboat tour or just a good night's sleep in a comfortable bed. Unfortunately, these good memories and all the goodwill that comes from them can be erased in an instant – if you let your customers' non-public personal information slip into the hands of criminals.

In recent years, there have been a number of high-profile thefts of customer information. These crimes have rightly alarmed merchants, financial institutions and consumers. If consumers lose confidence in a merchant's ability to protect non-public personal information (including payment card data) they are more likely to limit transactions or conduct their business elsewhere.

If your company exposes sensitive payment card data to compromise, the cost to your business can be considerable. At the most basic level, depending on the agreement with your merchant bank, you can be held liable for losses associated with compromised card data, including fraud and fines. However, merchants may also be exposed to government and bank fines and unwanted media attention.

But more importantly, data compromises can lead to a loss of customer loyalty and unfavorable brand reputation – even if those compromises never result in financial losses. And for many in the hospitality business, brand reputation is critical for bringing in new customers.

Fortunately, taking just a few actions can greatly minimize your business' vulnerability to data theft. By limiting the informa-

tion your business stores you can prevent becoming the target of a data criminal.

## Misperceptions Drive Risky Data Retention

In the hotel industry, several misconceptions about card processing requirements can increase a merchant's data retention risks. Foremost, many hoteliers mistakenly believe they must retain all payment card data as a security deposit during the duration of a guest's stay. This practice is not only unnecessary, but can also cause a merchant to unknowingly violate the Payment Card Industry Data Security Standard (PCI DSS).

Alternatively, upon checkin, a hotel should swipe a guest's payment card and submit an authorization request for the estimated cost of the stay. Once authorization is received – almost immediately – full track data provided by the magnetic stripe should be removed from all locations, including point-of-sale (POS) terminals and host servers. The only data that can be held is the cardholder's name, the primary account number (PAN, the number embossed on the card), and the expiration date. Following the initial authorization, this information is sufficient to settle the transaction when the guest checks-out.

In other instances, some travel agents and hotels will unnecessarily retain a customer's card verification value (CVV2), the visible three-digit number that usually appears on the back of a card to the right of the signature strip. This number is often used to authenticate a card when a customer is not present, usually through telephone or online transactions. The CVV2 may be needed to authorize a transaction, but once that transaction is completed, CVV2 data should not be retained or stored.

Similarly, personal identification numbers (PINs), generally used with debit cards, should not be stored in any form – encrypted or unencrypted. Merchants sometimes retain PINs or encrypted PIN

blocks, erroneously thinking that this information must be retained to process or contest chargebacks. However, chargeback processing never requires the use of PINs, full track data or CVV2 data.

While CVV2, full track and PIN data are of no use to a merchant once a transaction has been completed this information represents the crown jewels for data thieves. With this data in hand, skilled criminals can rapidly produce counterfeit cards and engage in fraudulent transactions. Instead of helping your business or your customers by retaining this data, you place both at risk.

## Card Data that Should Never be Stored

Three key pieces of payment card data should never be stored by any merchant:

- 1| Full track—the encoded data provided by the magnetic stripe
- 2| Card Validation Value (CVV2)—the three-digit number printed unembossed on the front or back of a payment card
- 3| PIN or encrypted PIN block—the personal identification number used with debit and some credit cards

Some or all of this sensitive data must be transmitted to receive authorization, but once a transaction has been completed, this information should be completely removed from POS systems and backend servers.

## Review Your Data Security with Expert Guidance

To enhance customers' experience, members of the hospitality industry draw on experts from many fields. A dietician improves a spa's menu, a top-notch designer adds fine touches to a luxury hotel and an architect redefines a company's brand with a new building.

Payment card security, especially when it breaks down, also contributes to a hospitality customers' experience – and so it similarly deserves an appropriate investment in expert guidance. Contact your POS or payment software vendor, your reseller or system integrator, and have an expert

confirm that your system is not storing full track, PIN or CVV2 data. If necessary, upgrade or patch your software.

Visa also maintains a list of payment software systems that have been validated under the Payment Application Best Practices (PABP) program as not storing prohibited data when implanted properly, available at [www.visa.com/pabp](http://www.visa.com/pabp). Businesses should also contact their merchant bank to discuss payment security and compliance with the PCI DSS. Merchant banks can help determine if you are using a vulnerable payment application that may cause the unintended storage of sensitive cardholder data and increase your risk of compromise.

Many hotels and restaurants operate as franchises, and all parties involved must rely on one another to maintain the value of the brand. If you operate a franchise, reach out to your franchiser for assistance in evaluating your payment card security practices. In turn, corporate entities can provide a valuable service to franchisees by helping them comply with data security best practices.

Without a doubt, payment cards play an integral role in the operations of the hospitality industry. With the possible exception of e-commerce, no other sector transacts such a high percentage of its business with credit and debit cards. Payment cards have especially facilitated the automation of booking and sped up the checkin and checkout process.

Storable cardholder data combined with other information, notably purchasing history, can also be a powerful tool in marketing programs that increase your business and provide value to your customers. In other words, when properly managed and utilized, cardholder data can improve your bottom line. But before you leverage legitimately retained data, take steps to protect your business and customers by verifying that your POS systems are not storing the same sensitive cardholder data sought by criminals.

*Michael E. Smith is senior vice president, enterprise risk and compliance at Visa USA.*

## Key Steps to Eliminate Data Retention

A few steps – usually easy and affordable – can help ensure that you are not storing vulnerable security data and confirm that you are adequately protecting the cardholder data that you do store:

**1. Consult with your technology vendor.** Have your technology vendor confirm that you are not storing full track, CVV2 or PIN data. Update, patch or change software if it is not PABP-validated.

**2. Contact your merchant bank.** Use your bank as a resource for reviewing your technology and data storage practices.

**3. Visit [www.visa.com/pabp](http://www.visa.com/pabp).** View the list of payment applications that have been validated as being PABP compliant and will help support your compliance.

**4. Confirm PCI DSS compliance of your agents.** Verify that third-party agents handling cardholder data on your behalf are PCI DSS compliant and listed on Visa's Web site at [www.visa.com/cisp](http://www.visa.com/cisp).

# get PROTECTED

...with **TransactionVault™**

TransactionVault reduces the risk of credit card fraud by eliminating the data that hackers want to steal while helping you process credit, debit and gift card transactions quickly and efficiently. With TransactionVault, you can focus on building your business, without worrying about credit card fraud. TransactionVault is offered exclusively by Merchant Link.

SECURE YOUR PAYMENTS WITH Merchant  Link

Stop by Merchant Link **booth #3562** at FS/TEC for a **FREE** gift while supplies last and register for a chance to win a **FREE iPhone®**.

For more information, check out [www.merchantlink.com](http://www.merchantlink.com) or call **301.562.5049**

