Data Breaches at Major Hotel Chains Hit the Travel Industry

Hardly a week goes by without a major company announcing that their customers have been impacted by a credit card breach. The travel industry is far from immune; in 2016, a number of wide-spread data breaches affected the hotel industry, resulting in thousands of customers having their credit card information stolen. As a travel company, you're likely concerned about protecting your company and your customers from these types of incidents.

Examples of recent data breaches that have hit hotels
To understand how to best protect yourself, it's important to understand how fraud is taking place. Three of the major fraud cases affecting hotels recently involved credit cards and point-of-sale terminals.

A data breach reported at the end of last year that was caused by malware set up to gain access to credit card information swiped at the front desk of affected hotels:

- **Hotels/customers impacted:** 1,175 hotels in the US, Canada, and Puerto Rico
- **Data stolen:** Debit and credit card information, including numbers, expiration dates, and security codes
- **How:** Malware installed that gathered information from the magnetic stripe on the back of cards

From late 2015 to mid 2016 point-of-sale systems were attacked, impacting physical credit cards used at hotels:
Hotels/customers impacted: 49 locations in North America, impacting more than 50,000 customers

- **Data stolen:** Debit and credit card information, including numbers, expiration dates, and security codes
- **How:** Malware installed that gathered information from physical cards used at the register

In early 2016 an owner of upscale hotel brands was subject to a data breach affecting point-of-sale terminals.
Hotels/customers impacted: 20 hotels in the US

- **Data stolen:** Customer names and associated debit and credit card information, including numbers, expiration dates, and security codes
- **How:** Malware installed on payment systems used onsite at hotel properties

While it's impossible to protect your company against all fraud threats, there is a way to increase the security of your payment information and help protect your company's and your customers' data. Virtual card numbers (VCNs) are being widely adopted throughout the travel industry, with good reason. VCNs work just like traditional credit cards by using a 16-digit number, an expiration date, and a security code. However, unlike traditional credit cards, they're set up for one time use and they offer a number of built in controls that can help protect against fraud.

How VCNs work
Say you have a customer who would like to book a hotel and flight to Florida. You provide a quote and they give you their credit card number to complete the booking. Instead of sending their credit card number to the hotel and airline, where it could easily be hacked, you keep it safe inside your own system. Then, you generate a VCN to send to the supplier that can only be used once and that you can put safeguards on, as outlined below.

Safeguards you can put in place using VCNs
VCNs have a number of useful features, but the most important is that you can specify exactly what the card can be used for, when, by whom, and for what amount. Setting up these parameters makes it highly unlikely that the card will be used for anything other than what you expect. These are the fields you can, and should, set up when using a VCN:

- Start and end dates: You can specify a date or a range of dates that the card can be used for, which helps tie the VCNs to a specific transaction.
- Spend limit: You should always set a spend limit, which is the maximum amount that can be charged for a transaction.
- Merchant Category Code (MCC) restrictions: You can designate what category of vendor is able to charge the card. Therefore, if you're booking a hotel, then only a hotel will be able to use the card.
- Unused funds: If the transaction is below the spend limit you set, you can also remove any unused funds from the card.

With data breaches and subsequent credit card fraud prevalent, VCNs are one of the easiest ways to avoid exposing your customers to data breaches while protecting your own business against unauthorized transactions. Learn more about virtual card numbers.

Posted September 11th, 2017 by Mark Mullis
Filed under Consumer, Hotels, Security
Tags: data breaches, secure payment solutions, virtual card numbers

Follow

WEX Travel

Free Downloads


6 Ways to Optimise Your Payment Strategy for 2016 Whitepaper


North American Business Traveler Trends Infographic


Global Travel Trends


4 Ways to Win Customers

Industry Events

IFTM, 26-29 September, Porte De Versailles, Paris, France

eTravel Europe, 3 October, Park Inn, Amsterdam, Netherlands

Categories

Airlines
Alternative Payments
Analytics
Big Data
Business Models
Business Travel
Car Rental
Consumer
Cruises
Currency
Ecommerce
Future of Travel
Hotels
Innovation
Leisure Travel
Mobile
Online Booking Tools
Online Travel Agents
Payment Technology
Resources
Security
Social Media
Tour Operators
Travel Management Companies
Travel Trends
Uncategorized
Virtual Cards