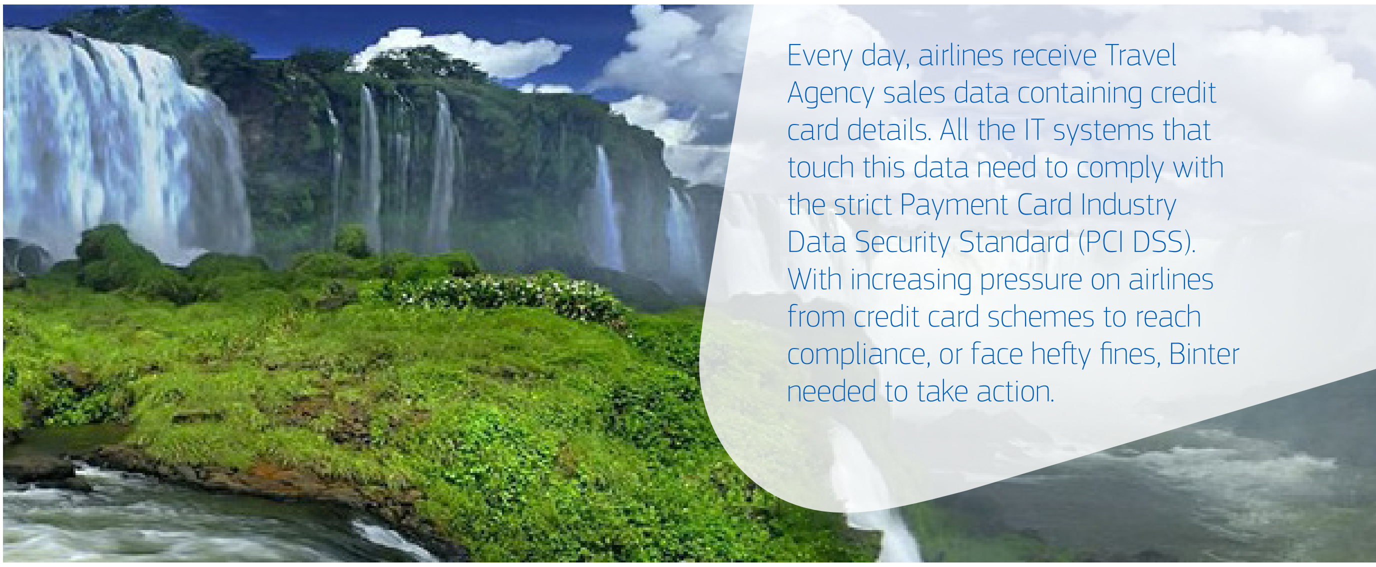
Binter Canarias cut PCI compliance costs with Amadeus



Every day, airlines receive Travel Agency sales data containing credit card details. All the IT systems that touch this data need to comply with the strict Payment Card Industry Data Security Standard (PCI DSS). With increasing pressure on airlines from credit card schemes to reach compliance, or face hefty fines, Binter needed to take action.

The Challenge

Securing credit card data for website sales is extremely important, but it's not the whole story. For airlines, Travel Agency sales are a significant part of the pie, and most of those tickets are paid for with credit cards. Data from the indirect channel is just as important to protect as any other source of data.

Every day, Binter receives files with details of their travel agency sales: the HOT files. These files contain full credit card details of their customers in a clear and fully readable format. They need these files to send to their Revenue Accounting system for revenue recognition and then to their credit card billing system to prepare invoicing details for submission to their bank.

But receiving this credit card data, and handling it within their own IT systems, left Binter exposed to either hefty fines from credit card schemes for non-compliance of PCI DSS data security standards, or the significant expense of reaching PCI compliance.

> *"Amadeus Travel Payments' tokenization service keeps our customer data safe and our information systems fully PCI DSS compliant, while allowing us to maintain our IT infrastructure the way we want. There are 3rd parties that offer similar solutions, but Amadeus knows our infrastructure, which meant we were able to identify the many credit card data touchpoints quickly and exhaustively."*

Hector Reboso
IT Systems Director
Binter

Weighing the options

Before deciding on a course of action, Binter needed to build a true picture of the total cost of securing their customer data and achieving PCI compliance. The costs are grouped into three key areas:

1. IT Infrastructure

For IT systems that store or touch credit card data, PCI DSS requires robust hardware and software systems to ensure the security of the data. In Binter's case, the cost of additional IT hardware and software ran into the hundreds of thousands.

2. External Services

Most airlines don't have the in-house expertise necessary to assess the requirements for PCI compliance. External consulting services are essential to ensure certification is achieved. On top of this, the cost of compliance includes regular vulnerability testing, as well as business process changes, staff training and user education during change management activities.

3. Staff Time

Ongoing upgrades and changes to security frameworks are a cost not just in monetary terms, but also in terms of the time dedicated to non-core tasks by an airline's IT and business staff. Binter staff would have to devote a lot of their time to PCI DSS control activity, instead of doing their 'day job'.

With an initial outline of potential costs taken into account, Binter took the logical next step of investigating ways to reduce the expense associated with PCI compliance.

Industry Context

According to data from the Payment Cards Industry Data Security Standards council, cybercrime costs the victim company an average of USD $2.6 million.

To combat the growth of data security breaches, the Payment Card Industry established a standard for handling sensitive card data: the Payment Card Industry Data Security Standard (PCI-DSS).

This standard is undoubtedly good business practice, but achieving and maintaining compliance is surprisingly difficult... and expensive. This difficulty is borne out by a recent finding by Verizon, which assesses companies for compliance against the standard, that only 20% of companies tested are fully PCI-DSS compliant.

Remove, reduce, reassure

Instead of creating an expensive IT fortress, an airline can minimise the cost of compliance by removing credit card data from their information systems altogether.

By storing credit card data as “tokens”, sensitive credit card data is removed from the airline’s system, significantly reducing the scope of PCI compliance.

Removing credit card data from parts, or all, of an IT system also minimises the airline’s exposure in the event of a security breach, reassuring their customers that their data is safe.

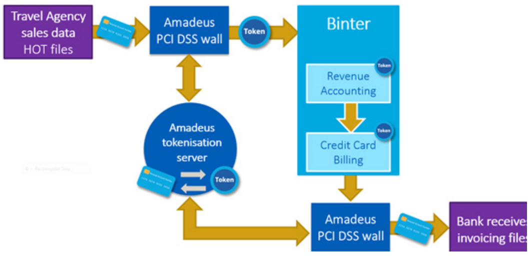
Travel Experts

Amadeus was the logical choice for Binter, as the first and most crucial step in achieving PCI compliance is to identify all credit card data touch points within an IT infrastructure. As Amadeus is uniquely positioned with a vast knowledge of airline IT infrastructure, coupled with travel payment expertise, they were able to identify all credit card touch points within Binter’s information systems quickly and completely.

The Solution

With Amadeus Card Data Security suite in place, the HOT files containing credit card data are automatically filtered by Amadeus before they ever reach Binter. Credit card details are replaced with tokens and the files are then sent on to Binter for processing in their revenue accounting system and their local credit card billing system.

When Binter needs to send invoicing files to their bank, Amadeus intercepts the file and replaces all the tokens with real credit card data. Once the acquiring bank communicates back to Binter with an acknowledgement file (containing credit card data), again, the PCI security suite swaps all credit card data for tokens before it reaches Binter’s information systems.



Now, thanks to the Amadeus Card Data Security solution, Binter does not handle any credit card data from Travel Agency sales, considerably reducing PCI compliance scope.

And as Amadeus card data tokens are compatible with the full suite of Amadeus products, Binter can easily invest in innovative ways to reach their customers across all sales channels, including online and mobile, without any additional effort required for PCI compliance.

What is tokenisation?

A method of converting real credit card data into a token.

A token is a representation of the credit card number that maintains the same format as the credit card, but has no meaning or value to a hacker.

Binter | amadeus

Amadeus Card Data Security Suite overview

Amadeus Card Data Tokenisation

is a method developed by Amadeus of converting real credit card data into data that looks like a real credit card but isn't. If this data is stolen, no transactions can be made. To interface with external 3rd party systems, the token is converted back to the real credit card data.

Amadeus Data Security Wall

is a firewall-like system which filters out credit card details from data entering or leaving the airline's IT environment. Credit card data entering the airline's system is replaced with a token, securing it against data breach. Tokenised data leaving the airline's system is replaced with encrypted credit card data.

Amadeus Data Collection Pages

is an Amadeus controlled page designed to collect credit card data from an end user in a PCI-DSS compliant way.

Offering customers the best service

Binter provides the Canary Islands with 8 inter-island routes and 11 international destinations. As an airline that tries to stay at the forefront of using technology to enhance the customer experience, they were the first airline to introduce electronic certification of residence status. It was a logical evolution to protect all the data of their customers with Amadeus PCI Security Suite.

Find out more

For further information, visit amadeus.com/travel-payments or speak to your Amadeus Account Manager today.

Amadeus Travel Payments for Airlines
Reach, Convert, Control