BIZCOMMUNITY

Travel agents must comply with IATA's PCI DSS deadline

Travel agents must comply with Payment Card Industry Data Security Standards (PCI DSS) by March 2018.

Simeon Tassev

Travel agencies that have not yet started this process may find themselves behind deadline, with potentially severe consequences.

Since 2006, PCI DSS compliancy has been a requirement that has been driven across all industries that accept card payments. As a minimum global data security standard, it stands to protect confidential card and payment information against theft, fraud and other forms of data misuse. IATA's endorsement of PCI DSS seeks to minimise the negative impact of data security breaches in air ticket sales by placing the onus on their distributors to comply or cease trading via card transactions.

The need to be cognisant

"PCI DSS compliance on its own is not a complex matter, requiring that a company completes a questionnaire designed specifically for their business size and types of card transactions handled. However, it can be a lengthy process for agencies that accept multiple types of card payments, or that have large volumes of card details stored manually. Larger agencies, in particular, need to be cognisant of the impact of non-compliance if they have not yet started with this process," says Simeon Tassev, managing director and QSA at Galix Networking.

The questionnaire referred to by Tassev ranges from a twenty-one-page document for smaller organisations that handle singular card transaction methods, such as online only, to eighty-five pages for those companies that handle all types of card transactions.

There are nine versions in all, increasing in requirements based on company complexity.

"The questionnaires are designed to simplify compliancy for the agencies, however, they need to be aware that, in some instances, compliance may require complete changes in their systems and processes. This is the component which takes up the most time as changing operational structures can have a substantial impact on the way the company does business. It also demands a dedicated investment of time and resources," explains Tassev.

Streamlining the compliance process

According to Tassev, many organisations avoid undertaking the process of compliance as they perceive it to be a strenuous endeavour and a drain on resources. Although it can be complex if operational changes are required, Tassev says that there are organisations' that provide guidance and offer compliance services which streamline the process and reduce the strain on businesses.

"Compliance becomes a question of weighing up the risks against the costs. Many organisations may choose to simply tick the right boxes on the questionnaire without actually confirming compliance. The risk of this is that, if an issue arises and the organisation is audited, their lack of compliance will come to light, resulting in severe penalties and, even, cessation of business altogether."

Payment security should be a priority for any organisation, regardless of the industry they play in. PCI DSS compliance shows a public commitment to the protection of customer card information. With the rise of cybercrime, including theft, fraud and misuse of information; it is vital for organisations to put the security of their customers first, while simultaneously protecting themselves through risk mitigation.

“Compliance with PCI DSS is a growing trend. We have seen many industries adopt this standard, with governing bodies and trade associations such as IATA spearheading the uptake. This backing of massive industry players such as IATA raises the benchmark for more industries to follow suit and achieve compliance, which stands as testament to an organisation’s commitment to protecting their customers,” concludes Tassev.