PCI DSS – Q & A to get you started

The Association of Canadian Travel Agencies (ACTA), in cooperation with a technical and training company Accel PCI, has produced a Question and Answer (Q & A) document to get you started on becoming Payment Card Industry Data Security Standard (PCI DSS) compliant. The Q & A will give a brief history of what PCI DSS is, who must comply, definitions to assist with understanding the terminology, the role of the International Air Transport Association, and what you need to do to become PCI DSS compliant.

Q: What is PCI DSS again?

A: In 2006, a consortium of 5 major card brands (Visa, MasterCard, American Express, JCB and Discover) united to form the **Payment Card Industry** council, hence the abbreviation of **PCI**. Concerned about the rising rate of fraud and theft of credit card data, they worked together and produced the **Data Security Standard**, or **DSS** for short. This effort was necessary to counter new levels of crime introduced with the Internet and processes linked to cyber security. **PCI DSS** is therefore the council's response to this type of crime.

The mission of the council is to make sure that card data is properly protected in each of the steps of a payment transaction. This includes the merchant premises where credit card payments are made, and any system that can affect the security of credit card data.

The standard that applies to all merchants is available to review at no cost at: https://www.pcisecuritystandards.org/pci_security/

Q: To whom does the PCI DSS apply?

A: PCI DSS has been in place since 2006. It was not mandatory for smaller merchants until January 31 2017 https://www.visa.ca/en_CA/support/small-business/security-compliance.html#1.

The PCI DSS applies to ANY organization, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data.

Definitions: *While the PCI DSS website provides an extensive glossary, there are only five key terms that you will want to understand as you get started.*
Q: What does the term "Merchant" mean?

A: For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.

Q: What does the term "Acquirer" mean?

A: Also referred to as "merchant bank," "acquiring bank," or "acquiring financial institution". An acquirer is an entity, typically a financial institution, that processes payment card transactions for merchants and is defined by a payment brand (one of the five major card brands) an acquirer.

Q: What is a "Payment Processor"?

A: Sometimes referred to as "payment gateway" or "payment service provider (PSP)". A payment processor is an entity engaged by a merchant or other entity to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers unless defined as such by a payment card brand. A payment processor would include SecuTrans, a company that offers ACTA members preferred merchant rates.

Q: What is a "SAQ":

A: Acronym for "Self-Assessment Questionnaire." Reporting tool used to document self-assessment results from an entity's PCI DSS assessment.

Q: What is a "QSA":

A: Acronym for "Qualified Security Assessor." QSAs are qualified by PCI SSC to perform PCI DSS on-site assessments. Many small to medium size travel agencies may not require a QSA to validate their SAQ but this is dependent on the transaction level (the type of SAQ that must be completed) or specific requirements of their acquirer.

Q: What type of Payment Cards does PCI DSS cover?

A: For purposes of PCI DSS, any payment card (credit or debit)/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard, or Visa, Inc.

Q: So why now? Why do we need to be PCI DSS certified?

A: There has been a continual increase in credit card crimes linked to the travel industry. In an effort to curtail this, the **International Air Transport Association (IATA)** has made it mandatory that all IATA appointed agencies become PCI DSS compliant prior to March 1, 2018. Failure to comply could mean the removal of the capability to issue airline tickets. IATA appointed agencies must provide IATA with a copy of their SAQ Attestation.

In addition to this requirement by IATA, you may also be contacted by credit card companies such as Visa and MasterCard. These credit card companies are asking acquirers to ensure that their merchants, regardless of size, are PCI DSS compliant.

For more information, visit the following link:

https://www.visa.ca/en_CAsupport/small-business/security-compliance.html

Q: What if the travel agency does not an IATA appointment and nor a merchant number? Does the travel agency still have to be PCI DSS compliant.

A: Yes. If the travel agency accepts payment and passes on the card information to a supplier who is the merchant that must meet the PCI DSS requirements, it is the supplier that will need to have proof (the SAQ Attestation of the travel agency) that your travel agency is compliant.

Q: How do I achieve compliance for my travel agency?

A: To become compliant, a merchant needs to achieve the following:

a.   Deploy a certain set of documents on how to react and protect confidential data,
b.   Get their personnel trained yearly towards security awareness and on modern crimes,
c.   Make sure that adequate controls are in place based on how cards are accepted.

Merchants need to demonstrate once a year to its credit card processor (acquirer) that they have deployed the appropriate measures. They do this by providing to their acquirer a Self Assessment Questionnaire (SAQ).

Q: Where do I start?

A: As you may know, ACTA hosted a webinar in May 2017 on PCI DSS COMPLIANCE, which overviewed the background and processes within the travel agency community. Although informative, this webinar did not provide a 'step-by-step' guide to becoming PCI DSS Compliant. This tool was not yet available.   If you have not yet listened to this webinar, you could start here with the overview that is hosted on demand in the ACTA Campus.

Since that time, ACTA has met with several payment processors and discussed the creation of a 'tool kit' that would provide a step-by-step guide to becoming PCI DSS Compliant. Most recently, Accel PCI has presented a viable option and we are pleased to introduce such a 'tool kit' to assist your agency to becoming PCI DSS compliant. A live webinar will be hosted by ACTA on Tuesday January 30, 2018. The webinar will be recorded and hosted on the ACTA Campus for your review at a later date. This webinar will be conducted in both English and French.

Q: Why Accel PCI?

A: Many merchants, including travel agencies, have found it difficult to become PCI DSS compliant or even to start the discussion with their acquirer about how to start. Most acquirers do not know enough about the merchant environment to optimize your choice of the initial step of the Self Assessment Questionnaire (SAQ) or how to find a solution to becoming PCI DSS compliant that is easy to follow.

This is why the PCI Security Standard Council has created a network of QSAs. Accel-PCI is not a QSA but does work with many QSAs. These companies assist merchants in their deployment of the controls required to obtain compliance.

Accel PCI provides services (portal, orientation questionnaire, example of documentation, training and maintains partnerships with QSA or test companies) that were created with the small merchant in mind. Particularly those in the travel industry and who rely on secure systems to ease their payment process. Furthermore, **Accel PCI** maintains an agreement with a team of Qualified Security Auditors (QSAs) that provide support to the **Accel PCI** merchants on an as needed basis.

Q: What is Accel PCI?

A: Accel PCI is an on-line service for merchants (including travel agencies) with a built-in, step-by-step guide to become PCI Compliant. Each merchant that registers to **Accel PCI** will have access to a dashboard where it will find:
- The proper SAQ level – easy to follow questionnaire
- Videos – a 'How to' guide to understand and complete your SAQ
- Examples of documentation necessary
- Access to an eLearning system for IT personnel
- A 'How to get compliant' course for the manager taking care of filing the SAQ

When you hit 'submit' a technician at **Accel-PCI** will make sure that all of steps were followed before submitting the final SAQ to the acquirer. Then quarterly or yearly, you will receive notification on what is required to maintain your compliance.

Q: How do I know which SAQ I need to complete for my agency?

A: The first step is to understand your obligations and to find which SAQ applies to you. This is done by completing the orientation questionnaire built into **Accel-PCI.** As well at the end of this first step, **Accel-PCI** will provide answers to all of your questions. This information can be shared with your acquirer to provide assurance that you are indeed at the correct SAQ level. The questions also are designed to value any partner of importance that you may have that will allow you to have a lighter SAQ. When combined with our 'How to get compliant' training, your certification process will be accelerated year after year.

Q: How long does this process take?

A: The initial questionnaire takes approx. 30-35 minutes. From this questionnaire, you will then be assessed to your corresponding SAQ level. The next component of the process will take between 8-10 hours to complete. The team at **Accel-PCI** will be there to assist you along the way.

Q: What if I have already started the process and have a QSA?

A: Accel-PCI provides examples of documentation and eLearning that is applicable in any case. As well, **Accel-PCI** negotiates cost reduction measures with partners that may be further beneficial to your organization.

Q: Is there a discount offered to ACTA members?

A: Yes! As part of our introduction of **Accel-PCI** to the travel industry, we are pleased to offer ACTA members a **20% savings** to both the initial questionnaire step and the corresponding SAQ that fits your agency's profile.

Should you have additional questions, please feel free to contact a member of the ACTA Team at 888-257-2282. ACTA's Member Services Coordinator, Julia Clarke ext 132, would be pleased to assist!

To know more on **Accel-PCI** contact Ryan Rees at ryan.rees@accel-pci.com - 438-821-0486.