THE EUROPEAN TRAVEL AGENTS' AND TOUR OPERATORS' ASSOCIATIONS

Ref.: EG17-001/94170

From: Ewa Grabiak

To: Members

Members of Air Matters Committee

Date: 13 March 2017

Re: Guidelines to PCI DSS Compliance

Summary:

As adopted by the PaConf/39, PCI DSS compliance will be a mandatory condition to obtain and retain accreditation as an IATA Accredited Agent in all its Accredited locations under the Passenger Sales Agency Rules in Resolution 818g.

In case of a non – compliance with PCI DSS security standards, 2 instances of irregularity will be recorded for the agency.

The following Guidelines were prepared to assist ECTAA Members and their Members to comply with the PCI DSS.

Introduction- General Information

PCI Data Security Standard were elaborated for merchants and processors handling sensitive payment card information. The PCI DSS security standards provide common data security standards to protect confidential payment card information against theft. All entities that store, process and transmit payment card data are required to adhere to PCI security standards.

The Payment Card Industry (PCI) Security Standards Council is responsible for managing the security standards for the payment card industry. There are 5 main payment card brands, which took part in the creation of this Council: American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.

The PCI DSS standards are in force since 2005 and are part of Resolution 818g since 2011. PaConf/39 added a provision to Resolution 818 §2.1.18 introducing a sanction in case of non-compliance.

The compliance procedure will vary according to the type of payment system adopted by the agent, the number of credit card transactions, as well as on the manner the credit card data is processed and stored.

There are two main PCI DSS Compliance Reports, attesting that the compliance procedure has been successfully accomplished:

- PCI DSS Attestation of Compliance (AOC)

- Self-assessment questionnaire (different types according to the type of business).

General Tips and Strategies for PCI DSS Compliance

The following tips and strategies are valid for all types of companies willing to be PCI DSS compliant. Their main goal is to eliminate storage of cardholder data which is not needed and isolate the data which is needed.

1. Sensitive Authentication Data (includes the full track contents of the magnetic stripe or equivalent data on a chip, card verification codes and values, PINs, and PIN blocks). This data should not be stored.
2. Software check
3. Cardholder data storage – 2 cases:
   a) When cardholder is needed
   b) When cardholder data is not needed

   Take inventory of all the reasons and places where the data is stored. If the data doesn't serve a legitimate business purpose, consider eliminating it.

   You can limit the scope of a PCI DSS assessment by consolidating data storage in a defined environment and isolating the data through the use of proper network segmentation. For example, if your employees browse the Internet and receive e-mail on the same machine or network segment as cardholder data, consider segmenting (isolating) the cardholder data onto its own machine or network segment (for example, via routers or firewalls). If you can isolate the cardholder data effectively, you may be able to focus your PCI DSS efforts on just the isolated part rather than including all your machines.

   To know more about this procedure, please consult Guidance for PCI DSS Scoping and Network Segmentation
4. Compensating controls

   Compensating controls may be considered for most PCI DSS requirements when an organization cannot meet the technical specification of a requirement, but has sufficiently mitigated the associated risk through alternative controls.

   If an organization does not have the exact control specified in PCI DSS but has other controls in place that satisfy the PCI DSS definition of compensating controls (see "Compensating Controls" in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms), the organization should do the following:

   a) Follow the procedures for compensating controls as outlined in PCI DSS Appendix B of the selected SAQ (Self-assessment questionnaire).

   b) For all requirements that were met with the assistance of a compensating control, respond to the SAQ question by checking the "YES with CCW" column.

   c) Document each compensating control by completing a Compensating Controls Worksheet in Appendix B of the SAQ. A Compensating Controls Worksheet must be completed for each requirement that is met with a compensating control.

d) Submit all completed Compensating Controls Worksheets, along with your completed SAQ and/or Attestation of Compliance, according to instructions from your acquirer or payment brand.

5. Professional Assistance and Training

PCI DSS Compliance Procedure

Step 1: **Contact with the merchant bank**

The travel agent should contact its merchant bank or the applicable payment brand:

a) American Express

b) Discover

c) JCB International

d) MasterCard

e) Visa Inc

Each of these operators has determined procedures to follow and different thresholds (number of transactions) according to which the travel agent will be able to determine whether it should conduct the PCI Data Security Standard assessment by a Qualified Security Assessor or a self-assessment procedure will be sufficient.

Step 2: **PCI Data Security Standard assessment**

If it is confirmed that a PCI Data Security Standard assessment must be done, the procedure must be conducted by an external Qualified Security Assessor.

The main tasks are:

- Verify all technical information given by merchant or service provider.
- Use independent judgment to confirm the standard has been met.
- Provide support and guidance during the compliance process.
- Be onsite for the duration of the assessment as required.
- Adhere to the PCI Data Security Standard Assessment Procedures.
- Validate the scope of the assessment.
- Evaluate compensating controls.
- Produce the final Report on Compliance.

The list of Qualified Data Assessors may be found HERE

Step 3: Self-assessment Questionnaires (SAQ)

If it is confirmed that a self-assessment is sufficient, the agent must determine which questionnaire is the most suitable.

General Guidelines and Instructions on SAQ are available HERE

There are different types of questionnaires, according to the type of transactions processed by the agent:

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order), that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Not applicable to face-to-face channels. SAQ A is available HERE
A – EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of cardholder data on merchant's systems or premises. Applicable only to e-commerce channels. SAQ A-EP is available HERE
B	Merchants using only: - Imprint machines with no electronic cardholder data storage, and/or - Standalone, dial-out terminals with no electronic cardholder data storage. Not applicable to e-commerce channels. SAQ B is available HERE
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor with no electronic cardholder data storage. Not applicable to e-commerce channels. SAQ B-IP is available HERE
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based, virtual payment terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels. SAQ C- VT is available HERE
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. Not applicable to e-commerce channels.

	SAQ C is available HERE
P2PE	Merchants using only hardware payment terminals included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce merchants. SAQ P2PE is available HERE
D	SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types. SAQ D for Merchants is available HERE SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete an SAQ. SAQ D for Service Providers is available HERE

Step 4: Reporting

Reports are the official mean through which merchants and other entities, document their compliance status with the PCI DSS Security Standard to their individual card payment brand or their corresponding financial institution. These reports must be presented to IATA as an evidence of PCI DSS compliance. Depending on the number of card transactions handled those can be:

- PCI DSS Attestation of Compliance (AOC) completed by a Qualified Security Assessor (QSA).

  Template for Report on Compliance is available HERE

- Self-assessment questionnaire signed by an authorized officer.
- The results of quarterly vulnerability scans if applicable.

Next steps:

- Resolution 818 g §2.1.18 stipulates that agencies have to comply by the 1st June 2017. This provision was adopted by PaConf/39 in September 2016.
- Travel agents should be strongly encouraged to comply with provisions of the Resolution as a matter of priority.
- ECTAA will maintain close contacts with IATA to further assist the industry. ECTAA will further seek clarifications on the number of notices of irregularity sent to travel agents in case of non-compliance. Indeed, the resolution refers to one notice of irregularity, instead of two as mentioned in the communication issued by IATA.
- Lastly ECTAA will further seek confirmation from IATA, that all airlines participating to the BSP, will be PCI DSS compliant.

Best regards,

Ewa Grabiak

Legal Advisor