



PCI DSS FAQs

1. *What is PCI-DSS Compliance?*

The Payment Card Industry Data Security Standard is a set of requirements for managing data security, implemented by the PCI Security Standards Council. This is a set of best practices to help merchants protect against customer cardholder data loss or theft.

2. *Who do I approach for PCI DSS compliance?*

IATA is committed to the industry objective of supporting Travel Agent achievement of PCI DSS compliance in a timely manner, and welcomes all possible solution providers who can assist Travel Agents with this important cause.

As part of this commitment, IATA has signed an agreement with Trustwave, a Qualified Security Assessor (QSA) by the PCI Security Standards Council, to obtain PCI DSS certification. Visit <https://pci.trustwave.com/iata> for more information and to sign up.

IATA will also accept evidence of PCI DSS compliance from any other certified [PCI Security Standards Council partner](#). To this end, IATA is pleased to see other industry partners such as [Travelport](#) facilitating PCI DSS certification.

3. *What if my acquirer did not ask for any documentation?*

Even if your acquirer did not request any evidence of compliance it is the responsibility of each legal entity processing credit card transactions to be PCI DSS compliant.



4. *What if I do not have an acquirer?*

In that case, you are solely accountable for the PCI DSS compliance of the BSP card transactions you are making on account of the airline whose ticket you are selling. We suggest you contact your GDS provider who can provide guidance, and review which of your systems card details are transmitted or stored. Starting from this, you will know which of your systems must undergo a PCI DSS evaluation.

5. *Where can I find more information directly from the main card payment brands?*

You can see below the contact details for the card payment brand:

- [American Express](#)
- [Discover](#)
- [JCB International](#)
- [MasterCard](#)
- [Visa Inc](#)

6. *Why are there multiple PCI DSS Self-assessment Questionnaires (SAQs)?*

Every self-assessment questionnaire applies to a specific environment; hence, it is essential for all merchants and service providers to choose the right SAQ, when they are going through the self-assessment process.

To make this process easier, TrustKeeper PCI Manager simplifies the process for you by presenting a pathway that's customized to your business. Trustwave's intelligent PCI Wizard guides you to the appropriate self-assessment questionnaire and walks you step-by-step through the process of certifying PCI DSS compliance, even prefilling some of the questions for you.



7. Are compliance certificates recognized for PCI DSS validation?

The answer to this question is no. Any sort of documentation which is not under the authority and validation of PCI DSS, will not be accepted for indicating the company's compliance with PCI DSS.

8. What do I need to provide to IATA to show my agency compliance for PCI DSS?

Please refer to question No.13.

9. What is an attestation of compliance?

The Attestation of Compliance is the document used to indicate that the appropriate Report on Compliance or Self-assessment Questionnaire has been performed, and to attest to your organization's compliance status with PCI DSS.

Each PCI DSS SAQ consists of the following components:

1. Questions correlating to the PCI DSS requirements, as appropriate for different environments:
2. Attestation of Compliance: The Attestation includes your declaration of eligibility for completing the applicable SAQ and the subsequent results of a PCI DSS self-assessment.

10. Where can I find more information related to PCI?

<https://www.pcisecuritystandards.org>

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

<https://www.pcisecuritystandards.org/merchants/>



11. Can a QSA that is not listed in a specific country but listed in another country conduct a certification process in the non-listed country?

Overall speaking, yes. Nevertheless it should be noted that under the QSA program guide, section 6.3.1, there are qualified regions in which QSA can or cannot perform. As noted “QSA Companies are authorized to perform PCI DSS Assessments and QSA-related duties only in the geographic region(s) or country(s) for which they have paid the regional or country fees, and as indicated on the QSA List.”

12. How can IATA help reduce ‘price abuse’ in specific markets from QSAs?

It is not within IATA’s purview to mediate in any commercial quotation.

13. What are the PCI merchant levels?

All merchants will fall into one of the four merchant levels based on Visa transaction volume over a 12-month period. Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) from a merchant Doing Business As (‘DBA’). In cases where a merchant corporation has more than one DBA, Visa acquirers must consider the aggregate volume of transactions stored, processed or transmitted by the corporate entity to determine the validation level. If data is not aggregated, such that the corporate entity does not store, process or transmit cardholder data on behalf of multiple DBAs, acquirers will continue to consider the DBA’s individual transaction volume to determine the validation level.

Listed below are the Merchants levels criteria for VISA and MasterCard. Although there are technically three (3) other major payment brands (AMEX, Discover, and JCB), compliance with the two (2) noted brands generally covers the others:

Merchant Level	Description
1	Any merchant — regardless of acceptance channel — processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant — regardless of acceptance channel — processing 1M to 6M Visa transactions per year.
3	Any merchant processing 20,000 to 1M Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants — regardless of acceptance channel — processing up to 1M Visa transactions per year.

It is reasonable for the Travel Agency to read all references to the ‘merchant’ as applying to his own activity in conducting card sales, because for the card industry the ‘merchant’ is the one conducting the card transaction.

14. *I only process a small number of credit/debit card transactions, do I need to be PCI Compliant?*

Yes, any business that processes, transmits or stores credit or debit card data must be PCI Compliant. Requirements vary by transaction numbers, you can find out more details [here](#).

15. What are the compliance validation requirements?

Level	Validation Action	Validated By
1	Annual On-site PCI Data Security Assessment and Quarterly Network Scan	Qualified Security Assessor or Internal Audit if signed by Officer of the company Approved Scanning Vendor
2 (*)	Annual PCI Self-Assessment Questionnaire (SAQ) and Quarterly Network Scan	Merchant Approved Scanning Vendor
3	Annual PCI Self-Assessment Questionnaire (SAQ) and Quarterly Network Scan	Merchant Approved Scanning Vendor
4	Annual PCI Self-Assessment Questionnaire (SAQ) and Quarterly Network Scan (if applicable)	Merchant Approved Scanning Vendor

Note.- (*) For Level 2 merchants under Mastercard SDP program there is a notation as follows: "Effective 30 June 2012, Level 2 merchants that choose to complete an annual self-assessment questionnaire must ensure that staff engaged in the self-assessment attend PCI SSC ISA Training and pass the associated accreditation program annually in order to continue the option of self-assessment for compliance validation. Alternatively, Level 2 merchants may, at their own discretion, complete an annual onsite assessment conducted by a PCI SSC approved Qualified Security Assessor (QSA) rather than complete an annual self-assessment questionnaire.

Source: PCI Security Standards Council



16. How I select the SAQ and Attestation that best apply to my Agency?

The PCI DSS SAQ Instructions and Guidelines document (available from the [PCI SSC Documents Library](#)) provides information about the different SAQs and the types of environments that each SAQ is intended for. Merchants should also consult with their acquirer (merchant bank) or payment brand to determine if they are eligible or required to submit an SAQ, and if so, which SAQ is appropriate for their environment.

17. Are all credit card transactions taken into account to determine the merchant level?

As a matter of fact, organizations that participate in data preparation, manufacturing, personalizing, and/or embossing for plastic cards are considered Service Providers for purposes of PCI DSS and should adhere to PCI DSS.

It should be noted that UATP is not subject to PCI DSS requirement, and that UATP transactions will not be counted in calculating the Agent's compliance requirements.

That being said, merchant levels are usually set up as per the VISA and MasterCard transactions, and, though there are technically three other major payment brands (AMEX, Discover, and JCB), compliance with the two noted brands generally covers the others.

18. Who is the merchant officer?

The merchant executive officer should be an individual with responsibility/oversight for the overall data security.



19. Do we need to fill in a SAQ per individual IATA number or can we do it jointly per Head office and including all branches?

You can do it jointly for all those point of sales for which the head office has full financial responsibility. In this case, you are only required to validate once annually for all locations and submit quarterly passing network scans by a PCI SSC Approved Scanning Vendor (ASV) for each location, if applicable.

20. What if I do not make use of credit/debit cards, do I have to be PCI DSS Compliant?

If an agency does not process credit card transactions, the Travel Agency must submit a declaration signed by the authorized signatory of the Travel Agency. Such Travel Agency will not be required to provide compliance evidence, however this information will be kept on file and once New Gen ISS resolutions are effective in a country, Travel Agency Credit Card form of payment will be switched off.

21. If there is a blanket GDS compliance- can they not have those certifications as supporting documents?

As part of the distribution chain, Travel Agency must capture payment card data and store or transmit such data in a PCI DSS compliant way to intermediaries such as GDSs which must then also store the card data in an equally secure way in accordance with PCI guidelines.

It is incumbent of each and every participant (e.g. Travel Agency, GDSs, etc.) to protect customers' payment card data regardless of their size.

In light of the above, it is within the purview of the Travel Agency to check with his GDS providers their PCI status as part of his evaluation of the card acceptance.



22. *If I only accept credit cards over the phone, does PCI DSS still apply to me?*

Yes. All businesses that store, process or transmit payment cardholder payment data must be PCI DSS compliant for every sales channel through which they engage in card transactions.

23. *Do Travel Agencies using third-party processors have to be PCI DSS compliant?*

Yes. Merely using a third-party company does not exclude a Travel Agency from PCI DSS compliance. It may cut down on their risk exposure and consequently reduce the effort to validate compliance. However, it does not mean they can ignore the PCI DSS.

It should be noted that it is incumbent on the Travel Agency to verify the PCI status of each provider to whom it delegates card payment related tasks.

24. *My travel agency doesn't store credit card data so PCI compliance doesn't apply to us, right?*

If you accept credit or debit cards as a form of payment, then PCI compliance applies to you. The storage of card data is risky, so if you don't store card data, then becoming secure and compliant may be easier.

It is not only the storage of data that is vulnerable to hackers, but that they may also go after sensitive card payment data when in transit through systems, hence securing data storage or ensuring there is no storage is good but not enough.

25. *We already have a PCI DSS Compliant certificate issued by a third party. Is this enough to cover our BSP or do we need to complete more forms?*

Because most large merchants have complex IT environments, many hire a QSA to glean their specialized value for on-site security assessments required by PCI DSS.



The QSA also makes it easier to develop and get approval for a compensating control. However, for Level 3 and Level 4, PCI DSS provides the option of doing an internal assessment with an officer sign-off if your acquirer and/or merchant bank agrees. Mid-sized and smaller merchants may use the Self-Assessment Questionnaire found on the PCI SSC Web site to assess themselves.

TRUSTKEEPER WIZARD TOOL

26. *Who is Trustwave?*

Trustwave® helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. IATA has partnered with Trustwave to offer a preferential rate to access our award-winning TrustKeeper PCI Manager tool to validate compliance and secure your payment environment.

27. *How do I sign up?*

Please visit <https://pci.trustwave.com/IATA> to review the offerings and register your account. You will need to have your 8-digit IATA Numerical Code in order to register.

Please refrain from entering the VAT number unless you have not been assigned with an IATA numeric code yet (i.e. new applicants).

28. *How do I decide between the security or compliance package?*

The Compliance offering allows you to validate PCI compliance with tools to help meet minimum PCI requirements. The Security offering provides optional tools that will help secure your business environment as well as fact track your compliance process.

29. *Are the costs in USD?*

Prices are shown by default in USD, but can be changed to multiple currencies.

30. *What happens if I do not become compliant*

Understanding that PCI compliance is an ongoing process, there is no limit to how many times you can submit an SAQ or run a vulnerability scan. IATA requires agents become compliant as of 1 March 2018. The TrustKeeper PCI Manager subscription cost is for 1 year of service; there are no refunds for agents who do not become compliant

31. *What languages is the IATA PCI Program available in?*

TrustKeeper PCI Manager for IATA Agents is available in English, English (UK), Spanish, French, French (Canada), German, Polish, Swedish, Chinese (Traditional), Japanese, Portuguese, Chinese (Simplified), Dutch, Norwegian, Danish, Finish and Icelandic.

Support via email and phone is only available in English.



32. *I already have a Trustwave account, how do I report to IATA?*

Contact Trustwave Support with both the merchant ID number for your existing account and your IATA Numerical Code and Trustwave will let you know what options are available to make the process as easy as possible.

33. *How will IATA know when I am compliant?*

If you sign up for an account at <https://pci.trustwave.com/IATA>, once you are compliant this will report directly to IATA.

34. *How do I get help with registration/SAQs/scans?*

Contact Trustwave Support info@trustwave.com