Visa Europe

Third Party Agent Registration and PCI DSS Compliance Validation Guide

August 2016

Version 1.4

Contents

1 Introduction

Third Party Agents play an increasing role in the payment system, bringing innovations and opportunities to card payments.

However, just like other entities that store, process or transmit card or account data, criminals are increasingly targeting Third Party Agents (also known as service providers). It is therefore essential that all entities including Third Party Agents take steps to secure their systems to limit their exposure to card or account data compromises and implement appropriate business practices to protect against financial, legal and reputational risk.

The Payment Card Industry Security Standards Council (PCI SSC) was founded by Visa, MasterCard, JCB, Discover and American Express to develop security standards for the card industry. You can find more information on the PCI SSC website. Payment Card Industry Data Security Standard (PCI DSS) is a security standard owned and managed by the PCI SSC.

The PCI DSS standard includes 12 requirements for any business that stores, processes or transmits payment card or account data. These requirements specify the framework for a secure payments environment.

This guide explains how Third Party Agents can register and validate their Payment Card (PCI DSS compliance with Visa Europe.

By registering with Visa Europe and being added to one or both of the Visa Europe Third Party Agent lists, agents can demonstrate to their existing and potential customers that they take the risks seriously.

1.1 Definitions of Agents

Visa Europe defines two separate categories of Third Party Agents, depending on who they provide services to:

Merchant Agents: Agents that directly or indirectly store, process or transmit card or account data on behalf of a Merchant. Merchant Agents usually have a contract in place with the Merchant to provide these services.

Member Agents: Agents who provide payment related services, to or on behalf of a Visa Europe Member, which includes directly or indirectly storing, processing or transmitting card or account data. Member Agents must have a contract in place with the Member to provide these services.

To reflect the two different Agent types, there are two separate registration processes and Visa Europe listings for PCI DSS validated Agents (see Section 2.0 for further information).

2 Registration Process

There are separate registration processes for Merchant Agents and Member Agents.

Depending on the Agent it is possible that registration under both programmes may be required. This is dependent on the services being offered and to whom.

2.1 Merchant Agent Registration

To register with Visa Europe, a Merchant Agent needs to submit to visamerchantagents@visa.com:

- A completed Merchant Agent Registration Form (MARF)
- Signed MARF Terms & Conditions (available within the MARF form)
- PCI DSS Validation documentation (see section 3.0 for further information).

Merchant Agents can access further information and the MARF form from http://www.visaeurope.com/receiving-payments/security/third-party-agents.

Merchant Agents are required to resubmit the MARF form any time their contact details, services offered, or PCI DSS compliance status changes.

Note: Visa Europe cannot accept digital/pasted copies of signatures on the documentation, therefore please only submit documentation that has been physically signed and scanned. This includes the Terms & Conditions and PCI DSS documentation.

2.1.1 Merchant Agent Fees

Following changes to the Merchant Agent registration processes and a review, we will no longer charge Merchant Agents to be listed on the Visa Europe Merchant Agent List.

2.2 Member Agent Registration

Where a Third Party Agent provides payment related services to a Visa Europe Member, the agent registration has to be submitted by the Member not the Member Agent.

To start the registration process, Member Agents should contact their contracted Visa Europe Member and request to be registered. Members can access further information, including the Member Agent Registration and Designation (ARD) form from Visa Online. The form is located on Visa Online at **Start > Fraud, Security & Risk > Account Information Security (AIS) > Agent Registration > Visa Europe Agent Registration and Designation Form**. This must be completed by the Member only.

If the Member Agent processes, stores or transmits card or account data they are required to validate their PCI DSS compliance to Visa Europe (See section 3.0). The agent can submit these documents themselves or via their QSA.

At section 4 of the ARD form, Members identify the services being provided by the agent. The list of services is identical to that in the PCI DSS compliance documentation. On receipt of the ARD from the Member, Visa Europe checks to ensure all services identified by the Member in this section were within the scope of the agent's PCI DSS audit and are compliant.

Any other Visa Europe compliance requirements related to the services provided by the agent will also be checked and validated as being in place for the agent before the registration process can be completed.

Any errors or documents not included in the submission may result in delays to the Member Agent's registration and a delay in being listed on the Member Agent Weblisting.

Note: Visa Europe lists only Level 1 Member Agents (see Table 1) on the Visa Europe Member Agent Weblisting (See Section 3.1) Member Agents cannot be listed until they have been registered by their contracted Visa Europe Members.

3 PCI DSS Validation

Although the process for registering Merchant and Member Agents is different, PCI DSS validation is the same for all third party agents that store, process or transmit card or account data.

Third Party Agents fall into one of the two levels as outlined below. Whether registering as a Merchant or Member Agent or both, the appropriate PCI DSS validation documentation as indicated must be provided as part of the registration process:

Table 1 - Third Party Agent PCI DSS Validation Requirements and Levels

Level	Service provider	Validation Requirements
1	Visa System Processors [1] or any service provider that stores, processes and/or transmits over 300,000 transactions per year	▪ Annual Report on Compliance (ROC) by QSA ▪ Attestation of Compliance (AOC) Form
2	Any service provider that stores, processes and/or transmits less than 300,000 transactions per year	▪ Annual Self-Assessment Questionnaire (SAQ) ▪ Attestation of Compliance (AOC) Form ▪ A passing ASV Executive Summary dated within the last 90 days

[1] A Visa System Processor (VSP) is a member or non-member that has a direct connection to the Visa Europe Authorisation Service.

3.1 Weblisting, Registration Renewals and PCI DSS Revalidation

Once a third party agent registration has been approved, the agent will be listed on the Visa Europe website at: http://www.visaeurope.com/receiving-payments/security/third-party-agents. There are separate lists for Member Agents and Merchant Agents.

To remain listed, the following annual renewal process need to be adhered to depending on the type of agent registered.

Merchant Agent

Merchant Agents must submit all correct PCI DSS validation documents (as referenced in Table 1) to Visa Europe annually .

In addition, the Merchant Agent is required to provide a new MARF form and re-signed Terms and Conditions annually with the PCI DSS revalidation.

Merchant Agents that have confirmed they are out of scope of PCI DSS should resubmit their MARF form and re-signed Terms & Conditions only, by the anniversary of the date they were first listed.

All documents and communication should be sent to visamerchantagents@visa.com

Member Agent

To remain listed on Visa Europe's Member Agent Weblisting, Member Agents should be registered by their contracted Visa Europe Member(s) and their PCI DSS validation documents should be up to date and submitted annually. A QSA or Visa Europe Member can submit the PCI DSS documentation on behalf of the Member Agent.

Member Agent Registration & Designation Forms should be sent to agentcompliance@visa.com

PCI DSS documentation and related communication should be sent to pcidsseurope@visa.com.

3.2 Monthly publication of the Third Party Agent weblistings

Once a registration has been approved by Visa Europe, the third party agent will be listed on the Visa Europe website. In order to remain listed, the appropriate documents have to be re-submitted (as outlined above) annually.

Depending on the date the registration is completed, the following timescales are applicable for both member and merchant agents to be added to and remain on the weblisting.

- Correct PCI DSS revalidation documents received before the 15th: Will be listed by the first working day of the next month (e.g. completed 14th August, listed 1st of September)
- Correct PCI DSS revalidation documents after the 15th: Will be listed by the first working day of the following month (e.g. completed 16th August, listed 1st of October)
- Any errors or documents not included in the submission of a registration may result in delays to an agent's existing listing being updated.

Third Party Agents that are listed on the Visa Europe website, will remain on the listing for 60 days after their ROC/SAQ has expired. If the required re-validation documents are not re-submitted as outlined above, the agent will be removed from the Visa Europe listing..

3.3 Remaining PCI DSS compliant

Implementing PCI DSS and registering with Visa Europe is intended to protect Third Party Agent's business (and their customers) against real risks.

It is advisable that Third Party Agents put processes in place within their business to ensure that they remain compliant.

Third Party Agents are advised to keep up-to-date with relevant information on www.visaeurope.com including any security alerts, and implement any suggested changes where appropriate.

The PCI DSS is issued by the PCI SSC and reviewed and updated on a regular basis. The following table lists the PCI DSS from 2.0 to the current version 3.2 with the issue date; and the date up to which Visa Europe will accept PCI DSS version documentation (AOC and ROC) for agent registration purposes:

PCI DSS	PCI SSC Version Valid Dates		Visa Europe end date for acceptance of documentation*
Version No	From	To	
2.0	01-Jan-11	31-Dec-14	31-Dec-15
3.0	01-Jan-14	30-Jun-15	30-Jun-16
3.1	15-Apr-15	31-Oct-16	31-Oct-17
3.2	28-Apr-16	Current	Current

* PCI DSS documentation (AOC and ROC) are valid for one year from the date they are signed by the QSA. Therefore, as long as the date of this documentation is within the PCI DSS version's valid dates, VE will accept it up to one year after a version end valid date (e.g we will accept PCI DSS version 3.1 documentation until 30 October 2017 as long as the original documentation is dated prior to 31 October 2016).

4 Visa Europe Member Agent Types

Visa Member Agents are classified into the following registration types:

1. Member Visa System Processor (MVSP) – Member processor directly connected to the Visa System.
2. Visa System Processor (VSP) – Third party processor directly connected to the Visa System. If the agent has a direct connection to the Visa System, the agent must provide us with a completed Exhibit 5A Visa System Letter of Agreement form.
3. Third Party Servicer (TPS) – Third party agent which is not directly connected to Visa.
4. Independent Sales Organisation (ISO) (agent is NOT handling card data) e.g. cardholder solicitation, prepaid ISO, card application processing services, customer service. An Independent Sales Organisation must not perform any of the following functions:

- Clearing and Settlement of Transactions;
- Payment to, or crediting of, Merchant accounts;
- Merchant and Cardholder account underwriting, activation, or charge-offs;
- Risk management, including Transaction monitoring;
- Approval and review of Merchants;
- Approval of Cardholder applications; and
- Establishment of Merchant fees for Transactions

Please note: there no similar classifications for Visa Merchant Agents.

Further details on Agents can be found in Section 1.15 of the Visa Europe Operating Regulations.

5 Visa Europe Contact Details

Merchant Agents

For further information about Merchant Agent registration, Merchant Agents can:

- Contact Visa Europe directly at visamerchantagents@visa.com.

Member Agents

For further information relating to Member Agent registration or PCI DSS revalidation, Member Agents can:

- Refer to Visa Europe website at:

  http://www.visaeurope.com/receiving-payments/security/third-party-agents

- Contact Visa Europe at agentcompliance@visa.com or for PCI DSS validation queries please contact pcidsseurope@visa.com.

6 Glossary of Terms

Account Information Security (AIS)
Mandated since June 2001, the Account Information Security (AIS) requirements protects Visa card or account data wherever it resides and ensures that Visa Europe Members, Merchants and Agents adhere to accepted information security standards.

In 2006, the AIS requirements were incorporated and adopted into an industry standard known as the Payment Card Industry Data Security Standard (PCI DSS).

Acquirer
A Merchant bank that enters into an agreement with a Merchant for the display of any of the Visa Licensed Marks and the acceptance of Visa Products and Services, or that pays currency to a Cardholder.

Approved Scanning Vendor (ASV)
ASVs provide commercial software tools to perform vulnerability scans for systems. You can find further information and download a list of qualified assessors by visiting the PCI Security Standards Council website.

Attestation of Compliance (AOC)
A PCI DSS document that must be completed for all service providers validating PCI DSS compliance. Visit the PCI Security Standards Council website to download the relevant documentation.

Card Verification Value (CVV2)
The three digit security code on the back of a payment card. When accepting card payments through a website, collecting the CVV2 number is essential. In the ecommerce world, it is an important indicator as to the potential for fraud for a transaction.

Member Agent Registration and Designation form (ARD)
Visa Europe form required to be completed by Members registering Agents who provide payment related services to them.

Merchant Agent Registration Form (MARF)
Visa Europe form required to be completed by Agents that directly or indirectly store, process or transmit Visa account information on behalf of a Merchant.

Payment Card Industry Data Security Standard (PCI DSS)
A security standard owned and managed by the PCI Security Standards Council (PCI SSC).

The PCI DSS standard includes 12 requirements for any business that stores, processes or transmits payment card or account data. These requirements specify the framework for a secure payments environment.

PCI Security Standards Council (PCI SSC)
The PCI SSC was founded by Visa, MasterCard, JCB, Discover and American Express. You can find more information on the PCI Security Standards Council website.

Payment Facilitator
Defined as "A third party that contracts with an Acquirer for the purpose of depositing Transactions, receiving Settlement or any other payment service related to a Transaction, on behalf of a Sponsored Merchant, and that is classified as a Payment Facilitator by Visa Europe". There are specific rules regarding Payment Facilitators which can be find in the Visa Europe Operating Regulations.

Qualified Security Assessor (QSA)
Independent experts who help with PCI assessments. QSA companies have trained personnel and processes to assess and prove compliance with the PCI DSS. For further information and to download a list of QSAs, visit PCI Security Standards Council website.

Report on Compliance (ROC)
A PCI DSS document containing details documenting a business' compliance status with the PCI DSS. This is completed by a Qualified Security Assessor (QSA) when an audit is conducted.

Self-Assessment Questionnaire (SAQ)
A PCI DSS document, which is a validation tool for Merchants, and Service Providers who are not required to do on-site assessments for PCI DSS compliance. For further information and download this form visit PCI Security Standards Council website.

A Appendix 1 Frequently Asked Questions (FAQ)

A.1 General FAQ

What is the difference between an Agent, Visa System Processor, Third Party Servicer, and Service Provider and Common Point of Service (CPS)?

A*gent:* An Agent is a Visa System Processor or a Third Party as defined below.

Visa System Processor: A Member or non-Member that is directly connected to the Visa Europe Authorisation Service and provides authorisation, clearing, settlement and/or payment-related processing services for Merchants or other Members.

Third Party Servicer: A non-Member that is not directly connected to Visa System and provides payment-related services, directly or indirectly, to a Member or Merchant such as but not limited to:

- Conducting cardholder or merchant solicitation, card application processing services transaction solicitation and/or customer service
- ATM/POS deployment and/or operational support
- Storing, processing and/or transmitting cardholder and/or transaction data and/or Visa account numbers
- Soliciting other entities to sell, distribute, activate and/or load prepaid cards on behalf of an issuer and for whom prepaid card sales and/or activation is a primary function of its business
- Verified by Visa Processors – organisations hosting the Access Control Server or Enrolment server on behalf of an issuer
- Dynamic Currency Conversion (DCC) Provider

Service Provider or Common Point of Service (CPS): A service provider or common point of service are terms used for an agent that stores, processes or transmits Visa card or transaction data and must be compliant with PCI DSS.

How can I identify if the agent is a Payment Facilitator?

To help you answer this question, please review the following statements. Visa Europe considers the agent a Payment Facilitator if the answer is 'Yes' to any:

- The agent provides payment services to merchants who do not have a merchant agreement in place with an Acquirer.
- The agent settles funds with the merchant (this includes if the agent outsources the settlement to another party).
- The agent approves the onboarding of new merchants and complete their risk assessment for the provision of a merchant account, merchant ID and/or merchant agreement (for acquiring services).

Please note that even if you have answered 'No' to all the above questions, Visa Europe may still consider the Agent a Payment Facilitator, depending on the services and payment model utilised.

How are the Merchant and Member Agent Registration requirements communicated to Third Party Agents?
The registration requirements are communicated to Visa Europe Members, Visa System processors and third party agents through direct communications and Visa Europe's website (located at http://www.visaeurope.com/receiving-payments/security/third-party-agents)

Am I required to be PCI DSS compliant?
If you store, process or transmit card or account data, you must validate PCI DSS compliance with Visa Europe every 12 months.

Every case is different but if you are unsure you should seek the advice of a Qualified Security Assessor (QSA). As a general rule (however not limited to), agents offering the following services need to be PCI DSS compliant:

- Clearing and settlement providers
- Payment gateways
- Digital agencies that touch cardholder data
- Payment service providers
- Hosting providers
- Internet payment service providers
- Fraud screening services
- Loyalty programmes
- Shopping cart solutions providers where they touch cardholder data (excluding shopping cart software manufacturers)
- Merchant payment processing solutions
- Co-Location (only requirements 9 & 12 audited as just provide power and physical location)
- Act as a Payment Facilitator

This list is not intended to be comprehensive.

What information will I need to provide to register?
Both the Merchant and Member Registration processes will require contact and company information. If you store, process or transmit card or account data you will need to sumit evidence that you comply with the Payment Card Industry Data Security Standard (PCI DSS).

Member Agents may also need to provide other Visa Europe required certificates, depending on the services they are providing.

How often do I need to update my PCI DSS validation documents with Visa Europe?
Any documentation related to your PCI DSS validation or status needs to be updated on an annual basis.

What if I cannot identify the specific card brand for a given card transaction volume? How can I calculate what Level I should validate my compliance against?
In instances where Third Party Agents have been unable to identify the card brand relating to their volumes, Visa will consider those transactions as Visa transactions.

What sort of PCI DSS information is Visa Europe looking for?
This will depend on how many transactions are stored, processed, or transmitted annually by the Third Party Agent (see Section 3 – PCI DSS validation). Visa Europe will review the registration to ensure:

- Where appropriate, you have provided an up-to-date validation of your PCI DSS compliance from a QSA, which details the scope of the assessment undertaken
- That you have provided a passed scan from an Approved Scanning Vendor (ASV) that is less than three months old. This will state that an approved commercial software provider has scanned your environment for vulnerabilities.
- If self-assessing your environment, that you have provided the appropriate Self-Assessment Questionnaire (SAQ)
- That you have provided a summary of services that have been PCI DSS validated and that we match against any other validation documents supplied. Please be as thorough and accurate as possible, as merchants will rely on this to choose services based on your description.

Apart from PCI DSS non-compliance, why could my registration not be accepted?
Visa Europe reserves the right to refuse registration of a Third Party Agent where there is a reasonable suspicion that the agent has been engaged in any activities which infringe any applicable laws, or which could have the potential of bringing the reputation of the Visa Brand into disrepute, or is a potential threat to the integrity and security of the Visa System.

Registrations where insufficient or incomplete information has been provided or where documents are not up-to-date will also not be accepted until correct information has been provided.

A.2 Merchant Agent FAQ

How often do I need to update my information with Visa Europe as an "out of scope" agent?
Those Merchant Agents who are not in scope for PCI DSS should resubmit their out of scope registration on an annual basis to confirm their information is still correct.

If no update has been received within 12 months and 60 days from when first listed, the Merchant Agent will be de-listed automatically from the Merchant Agent Web Listing.

I am a web hosting company. Do I need to register?
Yes, you should register your services on this website. If you provide payment related services, these include direct access or potential access (e.g. hosting providers who provide services to e-commerce merchants) to card data; you are considered a Merchant Agent.

My organisation has multiple brand names or products but share one PCI DSS assessed card data infrastructure. Do I need to register multiple times for each product or trading name?
During the registration process you have the ability to indicate several TRADING AS names, which will appear as such on the appropriate Visa Europe Web Listing, under the category "Name and Website." However if you have more than one environment (separate PCI DSS audits) or more than one legal company, you should submit a separate Merchant Agent registration for each environment.

My organisation has multiple PCI DSS assessed card data infrastructures. Do I need to register multiple times for each PCI DSS assessed infrastructure?
The registration process does not allow one Merchant Agent to register multiple PCI DSS assessments for different card data environments as one Merchant Agent listing. A new Merchant Agent registration for each assessment has to be submitted separately.

What happens if I do not renew my registration annually?
If after 60 days, the updated information, PCI DSS validation documentation has not been submitted, the Agent will be de-listed from the Visa Europe website.

It is important to keep your contact details up to date with Visa Europe.

What information can I show on my website or corporate materials to promote my listing?
As a registered agent appearing on the appropriate Visa Europe web listing, you can reference your listing on your website [and other corporate materials] only in the following manner:

'[Agent Name] are registered with Visa Europe as an Agent and are listed on http://www.visaeurope.com/receiving-payments/security/third-party-agents.'

Such consent is only valid whilst you remain a registered Agent listed on the Visa Europe Web Listing. Any reference to Visa Europe must be removed if you cease to be a registered Agent. You may not use any of the Visa logos or trademarks in any way and you may not use any other wording other than as specified above.

Visa Europe reserves the right to revoke or amend this consent at its sole discretion at anytime. Any changes to this consent shall be enacted by updating this guide on the Visa Europe website

What information will show on the public listing?
Once listed, the following information will be shown on the public listing

- Agent Name - the name submitted in the Trading Name on the registration and PCI DSS documentation.
- Website – The website confirmed on the registration.
- Services - the services confirmed in the Attestation of Compliance or entered as free text by "out of scope" agents
- PCI DSS Methodology - the methodology used to produce the assessment
- Agent Country – Confirmed in your Merchant Agent registration.

I am a registered Member Agent but I also provide payment related services directly to Merchants. Do I need to be registered as a Merchant Agent also?
Yes, you should be registered as both a Merchant Agent and Member Agent.

A.3 Member Agent FAQ

These FAQs should be used as a guide to answer or address most high level Agent registration questions and scenarios. Please refer to your Visa Europe acquiring and issuing institutions ('Visa Europe Members') for answers to questions that are specific to the Visa Europe Members' requirements.

I am a registered Merchant Agent but I also provide payment related services to Members. Do I need to be registered as a Member Agent and validate my PCI DSS compliance as a Member Agent also?
Yes, you should be registered as both a Merchant Agent and Member Agent.

I provide services to several Visa Europe Members. Do I have to be registered by each Member?
Yes, all the Visa Europe Members, that you provide your services to, must register you as their Member Agent.

What information will show on the public listing?
Once listed, the following information taken from the Attestation of Compliance (AOC) will be shown on the public listing

- Agent Name
- Validation Date
- Website
- QSA
- Services covered by review

A.4 Does PCI DSS apply to all cards?

We are often asked whether PCI DSS apply to all cards issued by Visa Europe Members.

Generally merchants, Members and their agents that store, process or transmit cardholder data originating from any card bearing the Visa brand marks (e.g. Visa, vPay, Electron including credit, debit and pre-paid products are required to comply with PCI DSS. There are a few exceptions detailed in two PCI SSC FAQs:

1. Does PCI DSS apply to one-time or single-use PANs?
2. If a merchant or service provider has internal corporate credit cards used by employees for company purchases like travel or office supplies, are these corporate cards considered 'in scope' for PCI DSS?

Both these FAQs recommend consulting the individual card brands to determine their requirements. The Visa Europe requirements are as follows:

1. **Single-use virtual cards** which are typically used in the travel sector to guarantee and provide payment to travel-sector merchants do not need to be protected by PCI DSS in the merchant and acquirer environments. However issuers and issuer processers that support the issuance of these single-use virtual cards are still required to comply with PCI DSS.
2. **Corporate cards** and **purchasing cards** do not need to be protected by PCI DSS by the entity to which the cards are issued unless this is explicitly requested by the card issuer. This does not affect the requirement for all members, merchants and their agents to comply with PCI DSS in respect of these card types.

Additionally **Closed-loop cards** that use the Visa system and carry a Visa BIN but which do not bear a Visa brand mark do not need to be protected by PCI DSS unless this is a separate requirement imposed by the operator of the closed loop system.