

THIRD PARTY AGENT REGISTRATION PROGRAM

Frequently Asked Questions

General

Q. What is the Agent Registration Program?

A. The Agent Registration Program is a Visa-mandated program established to ensure that Visa members are in compliance with Visa Inc. Operating Regulations (“Visa rules”) and policies regarding their use of Third Party Agents (TPAs). Agent registration is required for all entities providing solicitation activities, managed services and/or storing, processing or transmitting Visa account numbers for Visa members (or on behalf of their merchants). Visa members are required to perform due diligence reviews to ensure that they understand the TPAs’ business models, financial conditions, background and Payment Card Industry Data Security Standard (PCI DSS) compliance status.

Q. What is a Third Party Agent (TPA)?

A. A TPA is an entity, not connected to VisaNet that provides payment-related services, directly or indirectly, to a Visa member and/or stores, processes or transmits Visa account numbers.

Q. What are the different types of TPAs?

A. A TPA can be any of the following:

Independent Sales Organizations (ISO)

- Merchant or cardholder solicitation activities and / or customer service
- Prepaid program solicitation activities and / or customer service
- Deploying and / or servicing ATMs
- High Risk Merchant solicitation, sales, customer service, merchant transaction solicitation and/or customer training for the following Merchant Category Codes (MCC): 5962, 5966, 5967, 7995, 5912, 5122.

Encryption Support Organizations (ESO)

- Deploys ATM, POS or kiosk PIN acceptance devices that process and accept cardholder PINs
- Manages encryption keys

Third-Party Servicers (TPS)

- Storing, processing or transmitting Visa account numbers on behalf of Visa members

Merchant Servicers (MS)

- Storing, processing or transmitting Visa account numbers on behalf of Visa members’ acquired merchants



Corporate Franchise Servicers (CFS)

- A CFS owns or operates a centralized or hosted network environment used by franchisees that can affect the franchisee's cardholder data environment if accessed by unauthorized parties. In some cases CFS entities also provide card payment processing services to franchisees through these network environments.

Payment Service Providers (PSP)

- Contracting with Visa member to provide payment services to sponsored merchants

High Risk IPSPs (HRIPSP)

- Providing services to High Risk Internet Merchants (MCCs 5962, 5966, 5967, 7995, 5912, 5122) and stores, processes or transmits cardholder data and has a direct contract with the member

Distribution Channel Vendors (DCV)

- Packaging, storing and shipping of non-personalized Visa products (e.g. warehouses, wholesalers, logistics companies)
For more information please contact mgorski@visa.com.

Instant Card Personalization Issuance Agent (ICPIA)

- Performs instant card personalization and issuance for the issuer that is generally a retailer or kiosk location
For more information please contact mgorski@visa.com.

Dynamic Currency Conversion (DCC)

- Providing currency conversion services to sponsored merchants at checkout.
For more information please contact DCCcompliance@visa.com.

Note that a TPA can do one or more of these functions and must be registered for each function that they participate in by each issuer/acquirer they are operating on behalf of.

Q. Which TPA types are required to validate PCI DSS compliance?

- A. All entities that provide managed services and/or process, store or transmit Visa cardholder data on behalf of Visa members, merchants or other service providers are required to validate PCI DSS compliance with Visa. The following are TPA types that are required to comply with this requirement:
- Third Party Servicer (TPS)
 - Merchant Servicer (MS)
 - Corporate Franchise Servicer (CFS)
 - Payment Service Provider (PSP)
 - High Risk Internet Service Provider (HRIPSP)

Q. What are PSPs?

- A. A PSP is a TPA that contracts with an Acquirer to provide payment services to a Sponsored Merchant. The new term "PSP" replaces the old terminology "IPSP" which now includes all commerce type aggregation, including face-to-face in addition to ecommerce merchant aggregation.

Effective 1 July 2011, any entity acting as a PSP must register with Visa and comply with the new operating regulations.

For more information, please visit www.visa.com/third-party-agent.

Q. How are Third Party Agent levels defined?

- A. Third Party Agents are separated into two levels based on the volume of Visa accounts and transactions the service provider stores, processes, or transmits annually.

Service Provider Level	Description
Level 1	All Third Party Agents that store, process, or transmit more than 300,000 Visa accounts and transactions annually
Level 2	All Third Party Agents that store, process, or transmit fewer than 300,000 Visa accounts and transactions annually

TPA Registration

Q. Who registers TPAs?

- A. Visa members must register all their TPAs including any TPAs their merchants are utilizing. Ultimately, a Visa member is liable for its TPAs and therefore must perform their own due diligence and weigh the operational and financial risks of utilizing these entities.

Q. How does a member register a TPA?

- A. Registration must be received by Visa via the Visa Membership Management (VMM) application. This online tool serves as the central location where issuers and acquirers can register third-party agents and manage their relationships with these entities.

Q. Is registration required for all TPAs?

- A. Yes. If a Visa member has a relationship with a TPA, directly or indirectly, they must register the TPA. The fine for an unregistered agent starts at \$10,000 per TPA.

Q. Is registration required for Point-of-Sale (POS) software providers?

- A. POS software providers that **only** provide the payment application and do not store, process and/or transmit Visa account numbers are not required to register. The Payment Application Data Security Standard (PA-DSS) is available to ensure the secure development of these applications. Details on payment applications are available at www.visa.com/pabp.

Q. Prior to registering a TPA, what kind of due diligence must a Visa member perform?

- A. The Visa member should look into a TPA's basic background, financial and operational reviews. Additionally, any TPA that stores, processes or transmits Visa account numbers must be PCI DSS compliant or in the process of validating compliance with a reasonable target completion date. However, Visa members are encouraged to increase the scope of review based on the TPA business type, services performed, relative program risk, Visa account data held or processed and the individual Visa member's internal risk appetite and requirements. You may refer to the Third Party Agent Due Diligence Risk Standards posted on www.visa.com/third-party-agent.

Q. What are the TPA registration fees for Visa members?

A. There are two fees that Visa members are assessed:

- 5,000 USD for initial registration
- 2,500 USD annually

The first Visa member to register a MS, a TPS or an ESO is billed an initial registration fee and is then billed annually after the first year of registration. Additional Visa members who register these TPAs are not billed. For HRIPSPs, PSPs, ISOs, ICPIAs, DCVs and DCCs fees are billed to each Visa member that registers these TPA types.

There is currently no fee to register CFSs.

Q. What does a TPA have to do to register?

A. To start the registration process, TPAs have three avenues they can go through:

1. If the TPA has a contracted Visa member, they can contact them to initiate the registration process.
2. If the TPA has a contract with a Visa member's merchant, the TPA can directly contact the merchant's Visa member (usually identified by asking the merchant for their acquiring / merchant bank contact information).
3. Visa can also facilitate the registration by contacting the merchant's Visa member on behalf of the TPA.

If the TPA chooses to have Visa facilitate the registration, the following specific information is required and must be provided via e-mail to agentregistration@visa.com in the following format:

- 1) What services performed by the TPA require PCI DSS compliance?
- 2) What is the TPA's PCI DSS status?
 - a) Compliant / in process
 - b) Validating with an Attestation of Compliance (AOC) or an SAQ-D?
 - c) If submitting an AOC, who is the Qualified Security Assessor (QSA)?
 - d) When will the AOC or SAQ-D be submitted to Visa?
- 3) Does the TPA have contracts with Visa members (Financial Institutions) or merchants?
 - a) If the TPA has contracts with Visa members, which members are they? Who is the TPA's Visa member contact?
 - b) If the TPA has contracts with merchants, which merchants are they? Who is the TPA's merchant contact? What is the Merchant ID? Also, please list the acquiring bank for each merchant.
- 4) Provide the following TPA contact information: company name, company address; your name, e-mail address, phone number, and title; company website url.

Q. How do Visa members and TPAs obtain agent registration information?

A. Visa members and TPAs may obtain agent registration requirement information through industry conferences, direct communication, Visa Business News, the TPA Guide and through Visa's Third Party Agent website (www.visa.com/third-party-agent).

Payment Card Industry Data Security Standard (PCI DSS)

Q. What is the PCI DSS?

A. In 2006, CISP requirements were incorporated and adopted into an industry standard known as the Payment Card Industry Data Security Standard (PCI DSS). This standard is now owned and managed by the PCI Security Standards Council (PCI SSC).

Q. What is the Cardholder Information Security Program (CISP) / Account Information Security (AIS)?

A. Mandated since June 2001 and instituted by Visa Inc., the Cardholder Information Security Program (CISP) / Account Information Security (AIS) protects Visa cardholder data wherever it resides and ensures that Visa members, merchants and agents adhere to accepted information security standards.

Q. What types of TPAs are required to be PCI DSS compliant?

A. Any TPA that provides managed services and/or stores, processes or transmits Visa account numbers must validate PCI DSS compliance with Visa every 12 months.

The following are the TPA types required to be PCI DSS compliant:

- Third Party Servicer (TPS)
- Merchant Servicer (MS)
- Corporate Franchise Servicer (CFS)
- Payment Service Provider (PSP)
- High Risk Internet Service Provider (HRIPSP)

The fine for non-compliance starts at 50,000 USD per TPA.

Q. How about agents that handle PIN?

A. If an agent deploys ATM, POS or kiosk PIN acceptance devices that process and accept cardholder PINs and/or manage encryption keys, the member must ensure that a QSA has conducted an on-site review of the agent's PIN security controls to validate compliance with the PCI PIN Security Requirements and the PCI Security Standards Council Payment Transaction Security (PTS) manuals. (For the Latin America and Caribbean market the onsite review must be conducted by Visa (or a Visa-designated field reviewer). These manuals contain the physical and logical security requirements for all payment security devices. Members must also establish policies and procedures that include an annual review of the agent's processes and controls to ensure that the agent remains compliant with applicable PCI PIN security requirements and PCI PTS manuals.

Q. Can a Visa member register a TPA before the TPA validates PCI DSS compliance?

A. Yes. If the Visa member registers a TPA prior to the TPA validating compliance, the TPA must be contracted with an approved Qualified Security Assessor (QSA), or commit to completing a Self Assessment Questionnaire (SAQ) and have an expected date of compliance. A list of QSAs may be found on www.pcisecuritystandards.org.



Q. If validating with an AOC, how do I submit my PCI DSS documents to Visa?

A. On behalf of the TPA, the TPA's QSA will submit an executed Attestation of Compliance (AOC) Form to Visa via e-mail to pciocs@visa.com. Once the AOC is validated, Visa will send an email either confirming that all of the requirements have been met or asking for additional information.

Q. How do I submit my PCI DSS documents to Visa if validating with an SAQ-D?

A. SAQ-Ds are only accepted in conjunction with an agent registration and Visa will only accept SAQ-Ds sent via pciocs@visa.com for revalidating agents. First time submissions should be sent to the TPA's financial institution so the document may be attached to the VMM case.

Q. How often does a TPA need to validate PCI DSS compliance with Visa?

A. Visa Third Party Agents that store, process or transmit Visa accounts must perform the compliance review on an annual basis. If Visa does not receive the renewal documents:

Within 1 - 60 days upon expiry of the compliance documents, the third party agent will be highlighted in **Yellow** on the Visa Global Registry of Service Providers - PCI DSS Validated Entities.

Within 61 - 90 days upon expiry of the compliance documents, the third party agent will be highlighted in **Red** on the Registry.

After 90 days, the third party agent will be removed from the Registry.

Q. How does a TPA get listed on the Visa Global Registry of Service Providers - PCI DSS Validated Entities?

A. In order to appear on the Visa Global Registry of Service Providers - PCI DSS Validated Entities the TPA must be both a registered agent (MS, TPS, PSP, HRIPSP or CFS) and PCI DSS compliant as a level 1 third party agent.

Q. How about getting listed on the Visa Global Registry of ISOs and ESOs?

A. An ISO or ESO is added to the Global Registry in the month of, or the month following the first registration.

Q. What is a Visa member's liability for a TPA?

A. Visa members are responsible for ensuring that their TPAs are PCI DSS compliant. Visa members may be subject to fines and penalties for any TPA found to be out of compliance with the PCI DSS or with the Visa International Operating Regulations.

Q. How does a TPA validate that it is PCI DSS compliant?

A. There are different validations requirements for each TPA level:

Level	Validation Action	Validated By
1	Annual On-Site PCI Data Security Assessment	Qualified Security Assessor (QSA)
	Quarterly Network Scan	Approved Scanning Vendor (ASV)
2	Annual PCI Self-Assessment Questionnaire	Service Provider
	Quarterly Network Scan	Approved Scanning Vendor (ASV)

Details are available at www.visa.com/third-party-agents.

Other

Q. How long does it take for validation requests to be processed?

A. Visa will review requests sent to pciocs@visa.com within two weeks. To ensure existing entries on the Registry are updated prior to expiring, please send required documentation by the 15th of the month prior to the Validation Date published on the Registry.

Q. Do I need to notify Visa of any changes and updates regarding our entity?

A. In order to keep the TPA profiles current and accurate, registered TPAs are required to notify *their financial institution(s)* of any changes to any information such as changes in:

- Legal Name / Business Aliases (DBAs, Alternate Names)
- Address
- Company Point of Contact
- Types of services offered
- Number of Visa transactions or accounts processed annually
- Compliance status (where applicable)
- Mergers
- Financial solvency

The financial institutions will update TPA information thru the Visa Membership Management tool (VMM).

Q. Who should I contact regarding TPA registration questions?

A. Please contact the TPA registration representative according to location.

Location	Email
North America	agentregistration@visa.com
Latin America and the Caribbean	agentregistrationLAC@visa.com
Asia Pacific / Central Europe, Middle East and Africa	agents@visa.com



Q. Who should I contact regarding PCI DSS compliance validation requirements?

A. Please contact the representative based on your location.

Location	Email
North America / Latin America and the Caribbean	pciocs@visa.com
Asia Pacific / Central Europe, Middle East and Africa	vpssais@visa.com