



Registry of Service Providers Program Guide



[Contents](#)

[Introduction](#)

[Registration
Requirements](#)

[Registration
Process](#)

[Post-
Registration](#)

[Reference](#)

[Glossary](#)



Contents

1	Introduction	2
1.1	What is the Registry of Service Providers?	2
1.2	Who can register?	3
1.3	Why register with Visa?	3
1.4	Implications for Visa Clients	4
2	Registration Requirements	5
2.1	Which security standards do you need to comply with?	5
2.2	Compliance with PCI DSS	7
2.3	Compliance with PIN Security Standards	8
2.4	Compliance with 3-D Secure Access Control Server Security Standards	8
3	Registration Process	9
3.1	Registration Form	9
3.2	Supporting Documents	10
3.3	Registration Fee	11
4	Post-Registration	12
4.1	Annual Renewal	12
4.2	Changes and Updates	14
5	Reference	15
	Glossary	16

[Contents](#)

[Introduction](#)

[Registration Requirements](#)

[Registration Process](#)

[Post-Registration](#)

[Reference](#)

[Glossary](#)



1 Introduction

1.1 What is the Registry of Service Providers?

The Registry of Service Providers (Registry) is a listing of service providers that provide payment related services to Visa clients and merchants.

The Registry can be viewed on the Visa Asia Pacific website at www.visa-asia.com/spregistry.

The Registry includes the following information on each service provider:-

- ➔ Legal and Doing Business As name(s)
- ➔ Company website, address and contact details
- ➔ Type of services offered
- ➔ Visa programs enrolled in

This Registry serves as a source of reference for Visa clients and merchants when selecting service providers for outsourcing their services.

Contents

Introduction

Registration
Requirements

Registration
Process

Post-
Registration

Reference

Glossary

1.2 Who can register?

Any company that provides payment related services to Visa clients, merchants or other service providers may register for the program.

Please refer to Section 2 for details on the registration requirements.

1.3 Why register with Visa?

Marketing opportunity

The Registry provides listed service providers with access to a new communication channel to promote their payment card related services to potential clients worldwide.

Competitive edge

The Registry serves as a platform where service providers can broadcast their PCI DSS compliance status and differentiate themselves from other service providers.

Simplified reporting

Under the Visa Account Information Security (AIS) program, all Visa clients are required to submit annual PCI DSS attestation to Visa for each of the service providers they have engaged.

Service providers in turn are required to submit their compliance reports to every acquirer or issuer that they provide services to.

Under the Registry of Service Providers program, service providers have the opportunity to report their annual PCI DSS compliance status to Visa directly.

1.4 Implications for Visa Clients

Visa issuers and acquirers remain responsible to perform due diligence prior to engaging any service provider and execute a written contract with each service provider that performs cardholder or merchant solicitations and/or stores, processes, or transmit cardholder or transaction data on behalf of the Visa client.

If the service provider is contracted by the acquirers' merchant, the acquirer remains responsible to conduct the appropriate due diligence and ensure that the merchant and their agents comply with the relevant Visa and industry requirements.

Visa clients must also ensure that their service providers that handle cardholder data are PCI DSS compliant and adhere to all Visa operating rules.

If their service providers have directly registered with Visa under this program, Visa will collect the annual PCI DSS attestations directly from the service providers.

For service providers that have not registered directly with Visa, Visa clients will have to submit to Visa the required attestation documents on their behalf.

[Contents](#)

[Introduction](#)

[Registration Requirements](#)

[Registration Process](#)

[Post-Registration](#)

[Reference](#)

[Glossary](#)

2 Registration Requirements

2.1 Which security standards do you need to comply with?

Service providers that store, process and/or transmit:-

- Visa Account Number¹,
- CVV, CVV2, iCVV¹ and/or
- Other cardholder data¹,

must be compliant with Payment Card Industry Data Security Standards (PCI DSS). Please refer to Section 2.2 for details on the requirements.

In addition, service providers that also store, process and/or transmit cryptographic keys and/or personal identification number (PIN) have to comply with the PIN security standards. Please refer to Section 2.3 for the requirement details.

Service providers that provide services relating to 3-D Secure Access Control Server (Verified by Visa), please refer to Section 2.4.

¹Please refer to the Glossary for the definition of these terms.

Service providers that are enrolled in Visa's Approved Card Vendor program in Asia Pacific are automatically included in the Registry of Service Providers unless otherwise advised.

Service providers that do not fall in any of the above categories are required to be registered by a Visa client in Asia Pacific under the Agent Registration program. Please contact the Visa client that you are working with to confirm this.

For service providers that do not have a direct business relationship with a Visa client, at least one reference from a current customer is required confirming the nature of the relationship, services provided and the length of the business relationship.



2.2 Compliance with PCI DSS

Service providers that store, process and/or transmit Visa cardholder account or transaction information are required to be in compliance with PCI DSS as follows:-

	More than 300,000 Visa transactions* per year	Less than 300,000 Visa transactions* per year
PCI DSS onsite review	Mandated	Recommended
Quarterly network scan	Mandated	Mandated
Self assessment questionnaire (SAQ)	Optional	Mandated

* includes all transactions, regardless of the type / channel

PCI DSS onsite security reviews must be performed by a Qualified Security Assessor (QSA) approved by the PCI Security Standards Council (PCI SSC).

The quarterly network scans must be performed by an Approved Scanning Vendor (ASV) listed by the PCI SSC.

For detailed information on the PCIDSS, the list of QSAs and ASVs, please go to www.pcisecuritystandards.org.

Please note that only service providers that have been attested to be in full compliance with PCI DSS via an onsite review by a QSA will be listed on the Registry.

Service providers that have only completed a self-assessment via the questionnaire and network scans are encouraged to register with Visa. However, they will not appear on the Registry.

Service providers that are directly connected to Visa via the VisaNet Extended Access Servers (VEAS) have to comply with additional requirements. For more information, please contact your local Visa office.

2.3 Compliance with PIN Security Standards

Service providers that store, process and/or transmit Personal Identification Numbers are required to be in compliance with the PIN security standards. These service providers are inspected by Visa under the PIN Security Program.

For more information on the PIN security standards, please visit www.visa.com/pinsecurity or email appinsec@visa.com.

2.4 Compliance with 3-D Secure Access Control Server Security Standards

Service providers that provide services relating to 3-D Secure Access Control Server (ACS) under the Verified by Visa program are required to have undergone an inspection by Visa before providing such services.

To find more about the 3-D Secure ACS security requirements, please visit www.visa.com/3-dsecure.

3 Registration Process

3.1 Registration Form

The registration form can be downloaded from www.visa-asia.com/spregistry. You will need Adobe Reader version 7.0 or above to view and complete the form. Should you not have Adobe Reader, you may download and install it free of charge from www.adobe.com.

Once completed, there are three ways to submit the form:

1. Insert the digital image of the signature of the authorized signatory, click on the “Submit via Email” button if you are using Microsoft Outlook, attach the supporting documents and send the email.
2. Insert the digital image of the signature of the authorized signatory, save the registration form and submit it together with any supporting documents to apsregistry@visa.com.
3. Print the form, sign and scan it before sending it to apsregistry@visa.com together with the supporting documents.

Registration is only accepted for legal entities. Should a service provider operate in multiple locations as a separate legal entity, it is required to submit a registration form and supporting documents for each one of its legal entities.

A legal entity is the company that is registered with the respective country’s equivalent of the Registrar of Companies.

3.2 Supporting Documents

PCI DSS Compliant Service Providers

Service providers that have completed a PCI DSS onsite review must submit the following documents together with the registration form:

1. Attestation of Compliance Form signed by a QSA and the service provider.
2. Executive Summary and the Description of Scope of Work and Approach Taken sections of the Report on Compliance (“ROC”) issued by a QSA. The full ROC is not required. However, Visa reserves the rights to request the ROC as and when necessary.

Service providers that only completed a PCI DSS self-assessment are required to submit:

1. Self-Assessment Questionnaire (SAQ) Version D. Visa will not review the contents of the SAQ as issuers and acquirers are responsible for reviewing the accuracy of the SAQ.

3.3 Registration Fee

To participate on the Registry service providers pay US\$5,000 annual registration fee.

Service providers that are directly connected to Visa via the VisaNet Extended Access Servers and card vendors under the Approved Card Vendor program are under separate program fees.

Once registration is approved, Visa notifies the service provider and sends the invoice for the registration fee.



[Contents](#)

[Introduction](#)

[Registration Requirements](#)

[Registration Process](#)

[Post-Registration](#)

[Reference](#)

[Glossary](#)

4 Post-Registration

4.1 Annual Renewal

Service providers that are required to be in compliance with PCI DSS must perform the compliance review on an annual basis.

Two months prior to the expiry of the Attestation of Compliance, Visa will notify the service provider to submit the new compliance documents together with the annual registration fee of US\$5,000.

As indicated earlier, service providers that are connected to Visa via the VisaNet Extended Access Servers and card vendors under the Visa Approved Card Vendor program are not required to pay the annual registration fee.

[Contents](#)[Introduction](#)[Registration Requirements](#)[Registration Process](#)[Post-Registration](#)[Reference](#)[Glossary](#)

For those that are required to be PCI DSS compliant, if Visa did not receive the renewal documents and the registration fee:

- **Within 1 - 60 days** upon expiry of the compliance documents, the service provider will be highlighted in **Yellow** on the Registry.
- **Within 61 - 90 days** upon expiry of the compliance documents, the service provider will be highlighted in **Red** on the Registry.
- **After 90 days**, the service provider will be removed from the Registry.

Please note that Visa reserves the rights to remove any service provider from the Registry at its own discretion.

4.2 Changes and Updates

In order to keep the Registry current and accurate, registered service providers are required to notify Visa of any changes to the following information via the updated Registration form:-

- Company Profile such as Legal Name, Address and Doing Business As Name(s)
- Company Contacts or Contact Information
- Parties that the Company provide services to
- Types of services offered
- Types of data stored, transmitted or processed
- Number of Visa transactions or accounts processed annually
- Compliance status (if applicable)



5 Reference

For further information relating to PIN security requirements, please refer to www.visa.com/pinsecurity.

For further information relating to Verified by Visa program, please refer to www.visa-asia.com/ap/sea/merchants/productstech/vbv_intro.shtml.

For further information relating to the 3-D Secure Access Control Server security requirements, please refer to www.visa.com/3-dsecure.

For further information relating to PCI DSS, please refer to www.pcisecuritystandards.org.

Should you have any questions, please contact us directly at apsregistry@visa.com.

Contents

Introduction

Registration
Requirements

Registration
Process

Post-
Registration

Reference

Glossary

GLOSSARY

Account Number

A primary Cardholder account number that is either:

- Embossed and encoded on a Visa Card
- Encoded on an Electron Card, a Proprietary Card bearing the PLUS Symbol or a card bearing the Visa Electron Symbol

ATM

An Unattended Terminal that has Electronic Capability accepts PINs and disburses currency or checks.

Authorization

A process that approves transactions for specified amounts or provide facilities to respond to requests for authorizations for transactions or cash disbursements.

Cardholder Data

Data encoded in the card magnetic stripe such as cardholder name, card expiry date, CVV, etc.

Card Verification Value (CVV)

A unique check value encoded on the Magnetic Stripe of a Card to validate Card information during the Authorization process. The Card Verification Value is calculated from the data encoded on the Magnetic Stripe using a secure cryptographic process.

[Contents](#)

[Introduction](#)

[Registration Requirements](#)

[Registration Process](#)

[Post-Registration](#)

[Reference](#)

[Glossary](#)

Card Verification Value 2 (CVV2)

A unique check value generated using a secure cryptographic process, as specified in the VisaNet Standards Manual, that may be indent-printed on the back of a Visa Card. Card Verification Value 2 may be used as an additional means of cardholder verification during the referral process.

iCVV (Integrated Circuit Card)

The three-digit CVV value encoded on Chip cards to validate card information during the Authorization process for Chip cards.

Clearing

All of the functions necessary to collect a Clearing Record from an Acquirer in the Transaction Currency and deliver it to the Issuer in the Billing Currency, or to reverse this transaction, or to process a Fee Collection Transaction.

Cryptographic Key

A parameter used in conjunction with a cryptographic algorithm.

Magnetic Stripe

The magnetic stripe on a Card that contains the necessary information to complete a Transaction.

Payment Gateway

A system that provides electronic commerce services to merchants for the Authorization and Clearing of Secure Electronic Transaction Specification-compliant Transactions.

[Contents](#)

[Introduction](#)

[Registration Requirements](#)

[Registration Process](#)

[Post-Registration](#)

[Reference](#)

[Glossary](#)



PIN	A personal identification alpha or numeric code that identifies a cardholder in an Authorization Request originating at a terminal with Authorization-Only or Data Capture-Only Capability.
Prepaid Card	A card purchased for a specified amount, not exceeding US \$100, or local currency equivalent that is in turn used to purchase goods or services such as telephone calls, public transportation, or vending machine services.
Settlement	The reporting and transfer of Settlement Amounts owed by one Client to another, or to Visa, as a result of Clearing.
VisaNet	The systems and services, including the V.I.P. System and BASE II, through which Visa delivers Authorization, Clearing, and Settlement services to Clients.
VisaNet Extended Access Server (VEAS)	Visa equipment and software used to access the VisaNet Systems

[Contents](#)[Introduction](#)[Registration Requirements](#)[Registration Process](#)[Post-Registration](#)[Reference](#)[Glossary](#)



www.visa-asia.com/spregistry

Contents

Introduction

Registration
Requirements

Registration
Process

Post-
Registration

Reference

Glossary

