

## Visa Europe Account Information Security (AIS)

### Service provider compliance validation requirements

Updated 1 September 2009

#### Service Provider Levels and Validation Requirements

Effective 1 April 2009 in Europe, service providers that store, process or transmit Visa cardholder data on behalf of Visa Europe acquirers, issuers, merchants or other service providers will fall into one of two service provider levels.

Level	Service provider	Validation Requirements	Result
1	Visa System Processors <sup>1</sup> or any service provider that stores, processes and/or transmits over 300,000 transactions per year	<ul style="list-style-type: none"> <li>Annual Report on Compliance (ROC) by QSA</li> <li>Quarterly network scan by Approved Scanning Vendor (ASV)</li> <li>Attestation of Compliance (AOC) Form</li> </ul>	Included on Visa Europe's <i>List of PCI DSS validated service providers</i>
2	Any service provider that stores, processes and/or transmits less than 300,000 transactions per year <sup>2</sup>	<ul style="list-style-type: none"> <li>Annual Self-Assessment Questionnaire (SAQ)</li> <li>Quarterly network scan by Approved Scanning Vendor (ASV)</li> <li>Attestation of Compliance (AOC) Form</li> </ul>	Not included on Visa Europe's <i>List of PCI DSS validated service providers</i> Confirmation email of Receipt provided

<sup>1</sup> A Visa System Processor (VSP) is a member or non-member that has a direct connection to the Visa Europe Authorisation Service

<sup>2</sup> Service providers may choose to validate as a level 1 service provider if they wish to appear on Visa Europe's *List of PCI DSS validated service providers*



## Validation Documentation Submission

Visa Europe requires the following to be submitted to Visa Europe at [agentcompliance@visa.com](mailto:agentcompliance@visa.com) in order for a service provider to be included on Visa Europe's *List of PCI DSS validated service providers*:

1. **Attestation of Compliance (AOC)** - Level 1 service providers should submit an *Attestation of Compliance for Onsite Assessments (AOC) – Service providers* version 1.2 dated October 2008 signed by the service provider and the QSA to demonstrate PCI DSS compliance to [agentcompliance@visa.com](mailto:agentcompliance@visa.com). The AOC must refer to the correct version and date of the final Report on Compliance (ROC) and must be signed by both the QSA and the service provider.
2. **Report on Compliance (ROC)**<sup>3</sup> - The ROC should be submitted in the following circumstances:
  - The service provider has never appeared on Visa Europe's *List of PCI DSS validated service providers*
  - The service provider has appeared previously on Visa Europe's *List of PCI DSS validated service providers* but was removed due to missing the annual validation deadline
  - The service provider is a Visa System Processor<sup>4</sup>
  - Visa Europe has requested the ROC to be sent
3. **Agent Registration** - All service providers must also be properly registered with Visa Europe as an agent by a Visa Europe Member prior to being listed on Visa Europe's *List of PCI DSS validated service providers*. The process for registering an agent is described in Visa Europe Member Letters VE 37/07 and 21/08. Service providers based outside of Europe can be listed on Visa Europe's List of PCI DSS compliant service providers if they are registered by a Visa Europe member. It is the responsibility of the service provider to request that the Visa Europe member that they provide services to either directly or through a merchant registers them correctly.
4. **Services included in the PCI DSS audit** - Along with the AOC, the services that were included in the scope of the PCI DSS assessment should also be sent to Visa Europe by the Qualified Security Assessor (via email to [agentcompliance@visa.com](mailto:agentcompliance@visa.com)) and must match the scope in the ROC's Executive Summary. Any Visa card or payment related services that were not included in the scope should also be listed with an explanation of why they were out of scope and when they will be included. This will be used to create the list of 'Services covered by the review' in Visa Europe's *List of PCI DSS validated service providers*. The QSA should select from the following services:

---

<sup>3</sup> Visa Europe will not necessarily review the contents of the SAQ or ROC as Members who use the service providers are responsible for reviewing the accuracy of the validation documentation. Visa Europe reserves the right to require submission of a service provider's complete ROC. All materials should be sent securely via Entrust or PGP encryption to [agentcompliance@visa.com](mailto:agentcompliance@visa.com). If Entrust or PGP is not available, please contact Visa at [agentcompliance@visa.com](mailto:agentcompliance@visa.com) to discuss an alternative submission method.

<sup>4</sup> A Visa System Processor (VSP) is a member or non-member that has a direct connection to the Visa Europe Authorisation Service

- Payment Processing – POS, Internet, MOTO, ATM
  - Payment Gateway/Switch
  - Dynamic Currency Conversion provider
  - Hosting provider – Please specify Hardware, Web
  - Network provider/transmitter
  - Clearing & settlement
  - Loyalty programmes
  - Issuer Processing – Please specify Authorisation, Prepaid card processing, Data Preparation
  - 3-D Secure ACS hosting provider
  - Other - please specify
5. **Self-Assessment Questionnaire (SAQ) for Level 2 service providers** – They will not be listed on Visa Europe's *List of PCI DSS validated service providers*. They should submit version D of the Self-Assessment Questionnaire (SAQ) version 1.2 dated October 2008 which also includes an Attestation of Compliance (AOC) to [agentcompliance@visa.com](mailto:agentcompliance@visa.com)

Visa Europe will not necessarily review the contents of the SAQ or ROC as Members who use the service providers are responsible for reviewing the accuracy of the validation documentation. Visa Europe reserves the right to require submission of a service provider's complete ROC. All materials should be sent securely via Entrust to [agentcompliance@visa.com](mailto:agentcompliance@visa.com). If Entrust is not available, please contact Visa at [agentcompliance@visa.com](mailto:agentcompliance@visa.com) to discuss an alternative submission method.

#### **More information on Visa Europe's List of PCI DSS compliant service providers**

- **Validation Date** - This date is the last day of the month that Visa Europe received and accepted the AOC and ROC if relevant. The annual revalidation date is 12 months from the 'Validation date'.
- **Annual revalidation** - Visa Europe's *List of PCI DSS validated service providers* will denote service providers that are 1 to 60 days delinquent in their annual re-validation in **orange** and those that are 61 to 90 days late in **red**. Once the service provider has revalidated their compliance and submitted the appropriate documentation their listing will return to black with their new validation date. A service provider that does not revalidate PCI DSS compliance within 90 days of its annual due date will be removed from the list.
- **Level 2 service providers** - Level 2 service providers will not be listed on Visa Europe's List of PCI DSS compliant service providers. Only Level 2 service providers that opt to undergo a Level 1 onsite security assessment will be listed. Service providers who validate PCI DSS compliance with an annual SAQ and quarterly network scan prior to 1 April 2009 will remain on Visa Europe's list until their next annual revalidation date.
- **Registration** - All service providers must also be properly registered with Visa as an agent by a Visa Europe Member prior to being listed on Visa Europe's *List of PCI DSS validated service providers* as described in Visa Europe Member Letters VE 37/07 and 21/08. Service providers based outside of Europe can be listed on Visa Europe's *List of PCI DSS validated service providers* if they are registered by a Visa Europe Member.

