Visa Introduces Corporate Franchise Servicer as a New Third Party Agent Category

U.S. Canada

A review of recent cardholder data breaches affecting franchise locations indicates that the breaches have originated and spread quickly among locations due to systems owned or managed by corporate franchise organizations including cases where the franchisor / shared network has no direct role in processing cardholder data i.e. inventory control networks, restaurant menu distribution networks, etc. Corporate Franchise Servicer entities operate in a number of merchant segments, including lodging and food service.

Accordingly, Payment Card Industry Data Security Standard (PCI DSS) non-compliance of franchisors or other organizations performing aggregator or gateway functions may potentially expose acquirers to non-compliance penalties and increase potential liability in the event of a data compromise.

In an effort to address the increasing threat of data compromises that affect franchise businesses, **effective immediately**, Visa will extend the Third Party Agent Program to include a new category of agents, called "Corporate Franchise Servicers." Corporate Franchise Servicers (CFS) operates in a number of merchant segments, including food service and lodging.[1]

The inclusion of Corporate Franchise Servicer agents in the Visa Third Party Agent Program will help ensure that Corporate Franchise Servicer agents protect card data by at a minimum complying with the Payment Card Industry Data Security Standards (PCI DSS).

It is important to note, the new CFS category will **not** increase requirements for franchisors already participating in validation programs such as, Visa's Payment Card Industry Compliance Acceleration Program (PCI CAP) or Service Provider Program.

Corporate Franchise Servicers

A Corporate Franchise Servicer is defined as a corporate entity or franchisor that provides or controls a centralized or hosted network environment irrespective of whether Visa cardholder data is being stored, transmitted or processed through it. Although it may or may not host or provide card payment services, more importantly, the insecurity of the shared network can affect an independent location or franchisee and that of its own cardholder data environment if accessed by unauthorized parties.

A Corporate Franchise Servicer will qualify for registration under the Third Party Agent Program if it does any of the following:

- Provides card payment processing services to but does not meet merchant PCI DSS validation criteria.
- Owns or operates: a centralized or hosted network environment, connected physical and logical assets or locations which are used by the corporation, franchisees or other entities.

Note: If PCI DSS-compliant segmentation exists between these assets and the franchisee cardholder data environment, the corporate franchise **may** be excluded from this requirement.

[1] *Additional information on the requirements for registering a Third Party Agent is available at www.visa.com/third-party-agent.*

CFS Agent Registration

Corporate Franchise Servicers must be registered with Visa as a Third Party Agent and validate PCI DSS compliance in accordance with Visa Operating Regulations. Unique registration requirements exist for Corporate Franchise Servicers and are noted below:

A Corporate Franchise Servicer notified of the need to register by Visa or their acquirer must work through their acquirer to complete the registration process. If the Corporate Franchise Servicer does not have an acquirer relationship, the Corporate Franchise Servicer must:

- Directly contact and work with the franchisee's acquirer (usually identified by asking the franchisee for their acquiring / merchant bank contact information) to initiate the registration.
- The acquirer must note that it is registering a Corporate Franchise Servicer by adding the correct designation in the "Notes" section of the Visa Membership Management application.
- Corporate Franchise Servicers will have 60 days from notification by Visa or their acquirer to register, or provide ample documentation that the registration is in process.
- Acquirers that do not complete this process may be subject to non-registration fines as stated in the Visa International Operating Regulations.

PCI DSS Validation Requirements

Corporate Franchise Servicers must validate PCI DSS compliance within 12 months of initial notification from Visa or their acquirer that they are required to be registered. Members must verify that the Corporate Franchise Servicer is actively working towards (or has validated) PCI DSS compliance as a Level 1 service provider.

Noted below are the processes for validation of PCI DSS compliance; all materials must be submitted to the acquirer by the specified deadlines. Visa does not need copies of these materials; however Visa does retain the right to request any and all documentation at any point in time:

- Enter into a contractual agreement with a Qualified Security Assessor (QSA) within 90 days from the date of notification and submit a copy of agreement to the registering acquirer.
- Schedule the initial on-site assessment within 30 days from the QSA agreement submission and submit a copy of the time line to the registering acquirer.
- Complete the review and submit a Report on Compliance (ROC) to the registering acquirer 150 days after the QSA on-site is scheduled.
- The Corporate Franchise Servicer will have 90 days after the initial ROC submission to complete any required remediation. Upon completion, a fully compliant ROC and a copy of the remediation plan must be submitted to the registering acquirer. If remediation is not required, the ROC must immediately be submitted to the registering acquirer.
- Upon successful completion of the review, the "Executive Summary" and signed "Attestation of Compliance" sections of the compliant ROC must be e-mailed to Visa at pcirocs@visa.com.
- Corporate Franchise Servicer involved in a data compromise will be subject to an accelerated remediation and PCI DSS compliance validation timeline.
- Fines for non-registration and non-PCI DSS compliance may be assessed to acquirers per Third Party Agent guidelines.

Responsibility and Liability

If an acquirer has a relationship with a Corporate Franchise Servicer (directly or indirectly), and the Corporate Franchise Servicer is not registered by the acquirer, the acquirer may be assessed an unregistered agent fine as stated in the Visa Operating Regulations. An acquirer's obligation to monitor the practices of its third party agent(s) is a long-standing requirement. The Visa Operating Regulations impose specific monitoring standards and prescribe fines for non-compliance.