

Calling all Payment Call Centers: Registration and PCI Guidance 101

By Susan Kohl, President, ThoughtKey, Inc. (www.ThoughtKeyInc.com)

There are core elements important to the vitality of a company. One of the most important elements impacting a company's reputation and shareholder value is the **Customer**. Due to the importance of servicing customers many companies outsource these operations to experts specializing in call center operations.

Many companies in the payment industry rely heavily on outsourced call centers to provide the highest quality customer service and payment acceptance. Catalog and other MOTO/ecommerce merchants are a prime example. In addition, customers rely heavily on these merchants to protect any personal data provided in the course of business- in particular card transaction (cardholder) data. Imagine how catastrophic it would be to these merchants should a customer's identity be compromised as a result of poor internal controls at a call center.

As a call center, what should you do to protect your customers and your customers' customer? The first step is unfortunately mandatory but does protect you from fines up to \$500k USD being passed down from the card brands. This step is called "Registration".

Registration

The card brands (Visa, Mastercard, STAR, etc.) require "Registration" of all entities providing the following services to the payment industry (referred to as Third-Party Service Providers/Agents (TPAs)):

- ✓ Solicitation of payment activities
- ✓ Call center operations
- ✓ Chargeback, fraud and settlement management services
- ✓ Enabling authorization and/or settlement activities
- ✓ Performing encryption management services
- ✓ Payment program managing, monitoring and/or reporting (such as loyalty programs)

The purpose of Registration is to clearly identify all parties that handle payment transactions and/or cardholder data in any way. A card brand Member must register and sponsor each TPA that provides services to the Member's payment portfolio. A Member must be a financial institution (aka bank) that meets the criteria of the card brand to sponsor TPAs. We will refer to these Members as a "Sponsor Bank" for

TIP: Make sure you obtain written confirmation that your entity has been properly registered with each card brand that you accept as a payment mechanism from customers.

purposes of this article. There are many other types of Members not relevant to this article. TPA’s can select their Sponsor Bank or rely upon the payment processors’ Sponsor Bank to complete the proper Registration.

The table below highlights key information required, at a minimum, from you for the Sponsor Bank to properly complete registration. Each Sponsor Banks Registration program requirements may vary, however some basic information standards are required by all Sponsor Banks as dictated by the card brands operating rules and bank regulations.

Table – Registration Information Required

	You Provide	Sponsor Bank Performs	Result
1.	<p>Memo describing your business activities related to payments and provide a process flow that outlines incoming and outgoing activity (authorization pass through, settlement points, etc.), third party service touchpoints</p> <p>If possible, request a face-to-face meeting with the Sponsor Bank and/or Processor</p> <p><i>(TIP: Sponsor Banks may not request this, however to avoid confusion on what category you should be Registered as and the risk associated with your business it is prudent to provide such documentation)</i></p>	Review to determine Registration category and how to underwrite the risk and identify what third party companies handle cardholder data	The more clear and concise the business overview and operations the less frustrating and misclassification will occur during your registration process.
2.	Application for registration	Information used for underwriting and to prepare the card brand specific forms	In some cases, the TPA may be requested to complete all of the card brand forms rather than a single application. Each Sponsor Bank may differ on their procedures. Inaccurate and/or in complete information may be grounds for denying an application.
3.	Registration and application Fee(s)	Submits fees to card brand and maintain a small portion for the administrative process	Fees along with submission of the required documents to the card brands yields “Registration”, if approved.
4.	List of all principal owners (for	Background checks (criminal, credit,	Ensure the results do not

	You Provide	Sponsor Bank Performs	Result
	non-public entities only) <i>(TIP: Run a federal and state background check on each of the principal owners first and be prepared to address any known issues.)</i>	financial)	violate company policy for items such as federal offenses and related financial crimes.
5.	Financial statements and tax returns (most recent year and 1 -2 previous years)	Financial analysis to determine credit and financial risk	The analysis may yield a required reserve and/or principal owner guarantee to cover risks that may exceed credit and financial ability.
6.	W-9 (Tax ID)	Run a company background check	May be denied Registration if the company Tax ID and business existence cannot be validated
7.	Business License, Declaration of Corporation (non-public entities only)	Validate business existence and purpose of conducting business	May be denied Registration if the company existence and business purpose cannot be validated
8.	Credit check authorization form (non-public entities only) <i>(TIP: Review credit bureau reports for all principal owners first and be prepared to address any known issues.)</i>	Perform a credit check	Derogatory credit information may either pend the Registration process requiring more information from the TPA or a higher requested reserve. The TPA may be denied if bankruptcy or poor credit scores were noted.
9.	PCI compliance status/validation	Review the list of approved service providers and the PCI status at http://usa.visa.com/merchants/risk_management/cisp.html?ep=v_sym_cisp (Global List of PCI DSS Validated Service Providers) If not listed and/or a Report on Compliance (ROC) has not been provided by the TPA, they will request an action plan to achieve PCI DSS.	Entities not PCI validated may be denied Registration unless they can provide evidence that cardholder data is not “handled” (stored, processed and/or transmitted) in the TPA environment.
10	Other information/forms specific to the Sponsor Bank (e.g. business insurance verification)	Varies depending on the information requested; ensure proper liability coverage	Will vary depending on the information requested. If insurance coverage is insufficient to cover the risk

PCI Data Security Standards (PCI DSS)

The PCI DSS applies to any entity that stores, processes, and/or transmits cardholder data. It covers technical and operational system components included in or connected to cardholder data. If your business accepts or processes payment cards, it must comply with the PCI DSS.

The PCI Data Security Standards include the following 12 common sense steps to protect cardholder data.

Table – PCI Data Security Standards

Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored data4. Encrypt transmission of cardholder data and sensitive information across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software6. Develop and maintain secure applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to data by business need-to-know8. Assign a unique ID to each person with computer access
Regularly Monitor and Test Networks	<ol style="list-style-type: none">9. Restrict physical access to cardholder data10. Track and monitor all access to network resources and cardholder data
Maintain an Information Security Policy	<ol style="list-style-type: none">11. Regularly test security systems and processes12. Maintain a policy that addresses information security

PCI is an important component of the Registration process, one not taken lightly by a Sponsor Bank and the card brands. TPAs are not only required by the card brands to be Registered they must also be PCI DSS compliant if they store, process and/or transmit cardholder data. PCI validation requirements vary slightly based on the Service Provider PCI Level as noted in the table below.

Table – Service Provider PCI Levels and Requirements Summary

Service Provider PCI Level	Criteria (varies per card brand)	Requirements
Level 1	All third party processors, all service providers that store, transmit, or process greater than 300,000 transactions annually (evaluated by individual card brand)	<ul style="list-style-type: none"> • Annual Onsite Assessment by a Qualified Security Assessor • Quarterly Network Scan by an Approved Scanning Vendor
Level 2	Includes all service providers that store, transmit, or process less than 300,000 transactions annually (evaluated by individual card brand)	<ul style="list-style-type: none"> • Annual Self-Assessment Questionnaire (SAQ) – Version D • Quarterly Network Scan by an Approved Scanning Vendor

For more information about specific card brand PCI requirements review the following websites.

- ✓ Visa (“CISP”): http://usa.visa.com/merchants/risk_management/cisp_service_providers.html
- ✓ MasterCard (“SDP”): http://www.mastercard.com/us/sdp/serviceproviders/serviceprovider_levels.html
- ✓ American Express: https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=spinfo&ln=en&frm=US
- ✓ Discover (“DISC”): <http://www.discovernetwork.com/fraudsecurity/disc.html>

For additional detail on the PCI requirements review the PCI Security Standards Council website at https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf and contact ThoughtKey for assistance in navigating through your implementation of the PCI requirements and/or registration process.

Susan Kohl is CEO of ThoughtKey, a payment industry boutique consulting firm focused on PCI, regulatory compliance, risk management and expert testimony serving all parties of the payment industry value chain. www.ThoughtKeyInc.com Susan.Kohl@ThoughtKeyInc.com (678)522-2466. Twitter: PCISK