Managing Third-Party Vendor Security From The Business Perspective

Kara Gunderson, Director Payment Card Operations, CITGO Petroleum
Greg Luna, Sr. Corporate Legal Counsel, CITGO Petroleum
Todd McClelland, Partner, McDermott, Will & Emery, LLP

PCI Security Standards Council®

Kara Gunderson

Director, Payment Card Operations
CITGO Petroleum Corporation

PCI Security Standards Council®

Greg Luna

Sr. Corporate Legal Counsel
CITGO Petroleum Corporation

PCI Security Standards Council®

Todd McClelland

Partner and Legal Counsel
Global Head of Privacy & Cybersecurity
McDermott, Will & Emery, LLP

PCI Security Standards Council®

Managing Third-Party Vendor Security From The Business Perspective

Presentation Overview

- As recent security incidents demonstrate, Service Providers can cause significant cyber risks.
- What should a company do to mitigate and manage this risk?
- We will address this issue by focusing on business aspects of security through the contracting process with Service Providers.
- We will discuss best practices to explore the security posture of a prospective Service Provider, including suggestions for additional cyber-related contract provisions and other considerations.

Service Provider Contractual Security Requirements

Start with a PCI DSS Scope Assessment

- Legal and cyber risk issues should be addressed
- PCI DSS may still be a helpful standard to incorporate

- Consider starting with a “security requirements” template
- Address PCI DSS v4.0 contracting requirements
- Legal and other cyber risk issues should be considered

Security Incident Notification & Response Time

Include Specific Notification Periods in Contract Language

Service Providers should facilitate and enable your breach notification compliance:

- The Payment Brands have varying triggers and timelines for notification.
- All fifty U.S. States, the US Federal Government (e.g., TSA, HIPAA, GLBA) and other jurisdictions (e.g., EU's GDPR) have different breach notification obligations.
- Other parties in the payments space (e.g., processors/acquirors) may have additional notification requirements.

Security Incident Notification & Response Time

Other Issues to Consider Addressing Contractually

- Notification Trigger
- Timing
- Cooperation
- Notification Publicity
- PFI / Forensics
- Information Sharing
- Affected Individuals
- Service Providers
- Risk Allocation

Service Provider Subcontractors

4th Party Risk Should be Contractually Managed with Service Providers

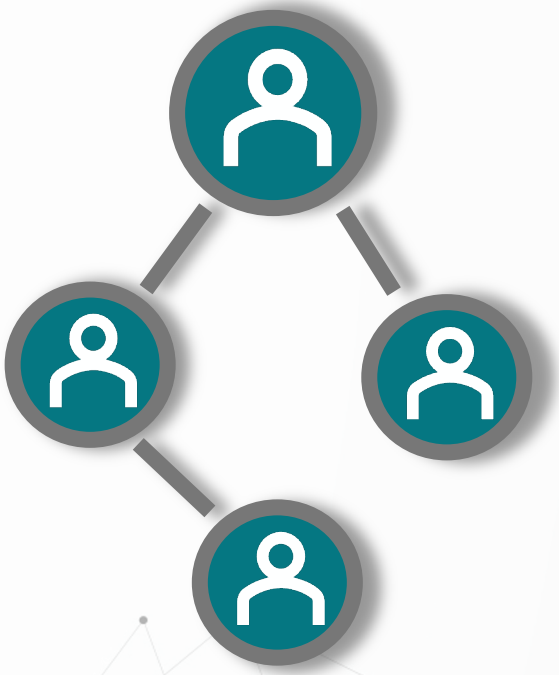
The vendors of a Merchant's Service Providers (i.e., "4th Parties") can, per the scope clarifications in PCI DSS v4.0, be in scope for a Merchant's PCI DSS compliance.

- Same scoping assessment applies.

Agreements should require Service Providers to pass through contractual security requirements to 4th Parties (and their vendors, and so on) as required to comply with PCI DSS.

- Consider passing through your Service Provider's security incident notification and other requirements.

Legal obligations may require the same.



Monitoring Data Use & Access

Identity and Access Management

Roughly a third of PCI DSS focuses on the pillars of Identity and Access Management (i.e., Governance, Authentication, Authorization, and Audit)

Merchants should work with Service Providers to determine how a Service Provider's systems and users will connect to the CDE while complying with PCI DSS and other legal requirements

IAM obligations must be balanced and reconciled against applicable privacy and cybersecurity laws.

Monitoring, for example, is a hot issue for many privacy regulators

Data Privacy Requirements

Add Data Privacy Obligations to Service Provider Contracts

Data privacy laws are rapidly expanding and evolving around the world. These laws often embed data security obligations, even in such seemingly benign requirements to have “reasonable” security.

- Regulators have taken undefined requirements and enforced rather stringent security obligations.

Merchants should contemplate data privacy compliance obligations withing their PCI DSS compliance program and their engagement with Service Providers.

PCI DSS and many laws (e.g., GDPR, HIPAA) require certain contractual language to be added in Merchant/Service Provider contracts.

Consider privacy issues with consumer information left behind for requests for transaction and/or chargeback information

Vendor Pen Testing & Test Timing

Add Contractual Rights to Pen Test in Service Provider Contracts

Pen Testing is a PCI DSS requirement

- including Service Provider in-scope systems and environments

Merchants and Service Providers should consider addressing pen testing in their contracts in reasonable detail

Things to consider	Who does the testing
	Testing limitations, protocols and parameters
	Coordination and timing
	Disclosure and use of results
	4th Party testing
	Frequency of Testing

Third-Party Assessments Certifications

Will Your Service Provider be Included in Your Assessment or Their Assessment?

As a part of PCI DSS scoping, Merchants and Service Providers should discuss and agree whether the Service Provider will be incorporated into the Merchant's assessment or will procure and issue their own assessment attestation.

Additional third-party certifications and assessments may be helpful for legal, insurance and other risk management purposes. Common examples include:

- SSAE 18 SOC 1 & 2
- ISO 27001
- HiTrust

Liability

The Limitation of Liability is a Key Contractual Component Between Contracting Parties

Liability for noncompliance with PCI DSS and other consequences of a data breach can be costly.

Merchants and Service Providers will want to address which party bears this risk.

It is common for Merchant / Service Provider contracts to have terms that address direct, indirect, consequential and similar damages and liability. These contracts may also include indemnification, insurance and related risk terms.

All parties in the payments space are still learning how best to manage these risks

How data breaches and other PCI-related damages or claims are handled under these liability limitations is evolving

Other Contractual Considerations

Confidentiality

Exit Strategy

- Merchants should consider adding contract language to address termination and an exit strategy. This strategy should address, for example, how the Merchant will move to another Service Provider when the contract terminates or expires.
- Consider a realistic wind down period.
- Make sure your exit strategy won't affect your PCI DSS or legal compliance.
- Negotiate pricing for any necessary extension to your transition period.

Negotiate Contractual Obligations Before There is Trouble

Service Provider Contractual Security Requirements

1. Start with a PCI DSS scope assessment. Whether in or out of scope, PCI DSS is a useful standard.
2. Contractually address the Service Provider's incident notification and other obligations.
3. Address a Service Provider's "4th Parties" and flow-through obligations.
4. Identity and access management are core PCI DSS requirements to address with your Service Provider.
5. If personal information is involved, make sure to address your privacy compliance obligations.
6. There are many aspects of pen testing to agree to up front.
7. Determine how your Service Provider will be assessed for PCI DSS and other common security certifications and assessments.
8. Merchant and Service Providers should contractually allocate cyber and PCI DSS liability.
9. Contracts should include appropriate confidentiality obligations.
10. The contract is your "prenup." Contractually address your exit strategy.

R

E

C

A

P

Managing Third-Party Vendor Security From The Business Perspective

Kara Gunderson, Director Payment Card Operations, CITGO Petroleum
Greg Luna, Sr. Corporate Legal Counsel, CITGO Petroleum
Todd McClelland, Partner, McDermott, Will & Emery, LLP

PCI Security Standards Council®