Beyond the Contract: Managing Customer/Service Provider Relationships After Contract Execution

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

Disclaimer

The views and opinions expressed in this presentation are solely those of the speakers. Although two of the presenters are lawyers, we are not providing any legal advice. If you have any questions about legal issues raised or discussed, you should seek the assistance of an attorney who is competent in this area. You should not rely on our presentation, discussion or commentary.

PCI Security Standards Council

Challenging Contracts Have Many Origins

Legacy Contracts
Old / Outdated

No Leverage
Only service provider we could get

“Big Customer”
We had to accept their terms to get the deal

“Take It or Leave It” Contract

Timing
No Time to Negotiate

Inherited Contract
From an Acquisition

Someone Else Negotiated It

PCI Security Standards Council

1. Inadequate PCI DSS terms.
2. Terms subject you to PCI DSS.
3. Inadequate or aggressive breach notification & cooperation.
4. You take the security incident risk.
5. Challenging termination terms.
6. Data privacy deficient.

PCI Security Standards Council

PCI DSS Requirement 12.8.2

Written Agreements with Third-Party Service Providers

What Does PCI DSS Require to be Included in Third-Party Service Provider Contracts?

PCI DSS Section 12.8.2

"Written agreements with TPSPs are maintained as follows:

- *Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE.*
- *Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.*

PCI Security Standards Council

What Does PCI DSS Require to be Included in Third-Party Service Provider Contracts?

IMPORTANT!

Applicability Notes in Section 12.8.2 provide flexibility

"The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party.

- *The acknowledgment does not have to include the exact wording provided in this requirement.*

PCI Security Standards Council

Contract Scenarios

Contract Example #1

– Existing Terms Were Sufficient

Review - Existing Terms Were Sufficient

SUFFICIENT TERMS

REVIEW

Legacy contract for outsourcing services.

Initially, PCI DSS services were not in scope.

Over time, services added pulled the service provider in scope.

Specific PCI DSS language not included.

Parties discuss possible contractual changes.

Neither party wanted to reopen contract.

PCI Security Standards Council

Approach - Existing Terms Were Sufficient

SUFFICIENT TERMS

APPROACH

Parties assessed existing terms.

Service provider agreed to comply with and protect all Merchant data following “applicable industry standards.” PCI DSS is an industry standard.

Cybersecurity exhibit controls met PCI DSS requirements. These controls expressly covered all data provided by the Merchant, which would include Cardholder data (“CHD”).

Contract audit rights required cooperation with the assessors/auditors.

Definition of “Confidential Information” included all data provided by the Merchant. Service Provider agreed to protect the confidentiality of all Confidential Information. Also, confidentiality language required “immediate” notification of a confidentiality breach.

PCI Security Standards Council

Lessons Learned - Existing Terms Were Sufficient

SUFFICIENT TERMS

LESSONS LEARNED

PCI DSS allows some flexibility.

PCI DSS does not require an actual standard reference.

Legacy contracts with appropriate language may be sufficient.

Contract acknowledgements are required of service providers.

Other requirements can be handled outside the contract, such as information sharing.

PCI Security Standards Council

Contract Scenarios

Contract Example #2

– Targeted Amendment

Review – Targeted Amendment

TARGETED AMENDMENT

REVIEW

Legacy contract for security services.

Security services affected the merchant's cardholder data environment.

Merchant identified service provider to be in scope.

Service provider believed they were out of scope.

PCI Security Standards Council

Approach – Targeted Amendment

TARGETED AMENDMENT

2

APPROACH

Parties discussed PCI DSS v4.0 scope requirements.

Service provider acknowledged their PCI DSS scope.

Service provider realized they will lose customers without meeting 12.8.2 compliance.

Parties targeted necessary and sufficient amendments for PCI DSS.

Responsibilities discussion and matrix ensued and shared with all customers.

Approach simplified contract negotiations for the service provider.

PCI Security Standards Council

Lessons Learned – Targeted Amendment

TARGETED AMENDMENT

2

LESSONS LEARNED

Unaware service providers in PCI DSS scope.

Knowing “hot issue(s)” lead to informed discussions and creative approaches.

Good-faith, transparent negotiations = quicker resolution.

Expert advisors often resolve PCI DSS resistance and misunderstandings, but not always.

PCI DSS Benefits = possible business and security advantage with the added layer of assessment.

A QSA-issued RoC/AoC may offer legal benefits.

PCI Security Standards Council

Contract Scenarios

Contract Example #3

– Exiting the Relationship

Review – Exiting The Relationship

EXIT RELATIONSHIP

REVIEW

Service provider required to comply with “the then-current version of PCI DSS.”

Service provider claimed out of scope, they had no cardholder data.

Merchant perceived the service provider could affect the security of the cardholder data environment (“CDE”).

Parties could also not agree to security, monitoring and information sharing measures to enable the merchant to meet its PCI DSS requirements.

PCI Security Standards Council

Approach – Exiting The Relationship

EXIT RELATIONSHIP

APPROACH

Parties separately discussed with their respective experts/PCI QSAs.

Each party's expert/QSA agreed with their client's respective position.

Each party reviewed contract rights and remedies.

Contract only allowed termination for material breach.

Merchant could not easily terminate and transition from service provider.

PCI Security Standards Council

Lessons Learned – Exiting The Relationship

EXIT RELATIONSHIP

3

LESSONS LEARNED

If parties disagree, be cooperative and good partners.

QSA “check and verify” the parties’ positions followed by merchant’s Acquirer.

Always consult attorney to create a defensible position against future data breach lawsuits or governmental investigations.

Consider exit strategy for both.

Service providers termination cost implications = wind-down costs and up-front investment recovery.

Both consider termination terms = data return, transition process and costs.

Consult with attorney to review terms, limitations on liability, governing law, and arbitration/mediation.

PCI Security Standards Council

Other Risk Mitigating Measures

Confirm Other PCI DSS Requirements Are Met

Other Risk Mitigating Measures

Confirm Other Service Provider Requirements Are Met

1

List all TPSPs

PCI DSS 12.8.1

- Maintain a list of all TPSPs (Third-Party Service Providers), including a description of the services provided.

Due Diligence

PCI DSS 12.8.3

- Confirm a process is implement to conduct proper due diligence prior to engagement.

Monitoring

PCI DSS 12.8.4

- Confirm a program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.

Responsibility Allocation

PCI DSS 12.8.5

- Maintain a list for each TPSP about the allocation of responsibilities between the TPSP and the merchant.

Get Creative

Work Together On Creative Solutions to Meet Requirements

Other Mitigating Efforts

PCI DSS, cybersecurity, and privacy risk mitigation

2

Reduce Access to CHD/CDE

Obtain Certifications, Assessments, Etc.

Security & Privacy Questionnaire

Reduce Risk, Volume and Data Processed/Retained

Supply Chain Incidents Occur

(e.g., MOVEit)

Ask for Usage and Mitigation

Current News Search Engine Subscription Notifications

IT Vendor Risk Management Solutions Market

(e.g., Security Scorecard, Bitsight)

[Examples only. We are not endorsing these products.]

PCI Security Standards Council

Other Mitigating Efforts

Law School Example: “Every Dog Gets One Bite”

3

Another Data Breach ?

- Obtain security incident information and remediation.
- Interview to obtain details.
- Consider legal counsel involvement to memorialize investigation facts.
- Ramification considerations with multiple security incidents.

PCI Security Standards Council

Other Mitigating Efforts

4

Consider cyber liability and other insurance

- Cyber Liability Insurance
- Confirm Incident Coverage
- Check for Realistic Coverage
- Appropriate Deductible
- Cyber Liability Insurance Contract Inclusion

Be Creative!

Work Cooperatively

Find Ways to Obtain Proper Coverage

Pre-Approved, Endorsed, and Preferred Legal Counsel and Forensics Firm

PCI Security Standards Council

After The Contract Discussion

1. Review and assess contracts.
2. Document allocation of PCI DSS responsibilities.
3. Legal review to assess terms, conditions and termination clauses.
4. Discuss open items with contracted parties.
5. Obtain third-party QSA and Legal assessments of agreements.
6. Seek Acquirer opinion for scope and responsibilities.
7. Would termination and transition be more expensive than sharing costs to reach a compromise?
8. Get Creative! Work together with all parties to find resolutions.

R
E
C
A
P

PCI Security Standards Council

Beyond the Contract: Managing Customer/Service Provider Relationships After Contract Execution

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