SANS Institute
Information Security Reading Room

Contracting for PCI DSS Compliance

Christian Moldes

Contracting for PCI DSS Compliance

GLEG Gold Certification

Author: Christian J. Moldes

Christian_moldes@hotmail.com

Adviser: Charles Hornat

Accepted: August 14, 2009

Outline

Abstract

PCI DSS Requirement 12.8.2 states that companies should maintain a written agreement with service providers that are responsible for the security of cardholder data the service provider possesses. Many people consider this requirement unnecessary or less important than most of the requirements. However, misunderstanding of this requirement may expose a company to serious liability. This paper intends to identify most of the risks a company may face when dealing with service providers. This paper provides sample clauses that an agreement should have in order to protect a company when dealing with other companies' cardholder data.

The audience for this paper is legal counselors, security officers, compliance directors, IT auditors, and anyone responsible for PCI DSS compliance.

1. Legal Disclaimer

The author of this paper is not a lawyer. This paper contains general information and should not be considered legal advice for any particular situation. Companies and individuals needing legal advice should consult their own counsel.

2. PCI Security Standards Council and PCI DSS

PCI Security Standards Council (PCI SCC) was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. Companies accepting payment card transactions from any of these payment brands have to comply with PCI DSS requirements. Non-compliant companies are exposed to higher transaction fees imposed by their acquirer banks, fines imposed by the payment brands, higher liability if a breach occurs, and even to the risk of losing the authorization to process payment card transactions.

PCI DSS requires documentation to be developed and maintained, preventive and detective security controls to be implemented, and processes to be in place in order to identify and contain any security breach attempts as soon as possible. PCI DSS and its supporting documents are available for download at PCI Security Standards Council website.

3. How security breaches are discovered

One important factor to understand the liability companies are exposed is to understand the implications of a security breach, and more importantly how those breaches are discovered. Verizon Business in its 2009 Breach Report provides valuable insight about this. Many

security breaches are not discovered by the companies themselves, but by third parties.

According to the report, 70% of the breaches are discovered by a third party, 13% discovered by an employee during normal work activities, 11% discovered during troubleshooting of unusual system behavior or performance, 6% during event monitoring or log analysis, and 2% during routine internal audits, 2% due to blackmail or extortion, and 1% by a confession or brag of the perpetrator (Verizon Business RISK Team, 2009, p.38). Values sum more than 100 percent as many breaches may be discovered by a combination of factors.

For companies that accept payment cards as a method of payment, the third parties that would eventually discover the breach are more than likely law enforcement agencies or the payment card brands.

From the statistics above, we can deduce that in 70% of the cases, a company would be notified of a security breach but it wouldn't know the source of the breach until a thorough investigation is completed. Unfortunately, for companies that share cardholder data with third parties, the investigation should not only include the merchant but also all its service providers, who possess the merchant's cardholder data or that they may have an impact on the security of the merchant's cardholder data.

3.1. Breaches Discovered by the Payment Card Brands

Usually, cardholders are the first to detect that a credit card has been compromised which is discovered through unauthorized transactions in their credit card statements. Cardholders report unauthorized transactions to their issuer banks. The bank will investigate the entire transaction flow, which also includes the

chargeback process to the merchant. Chargebacks and any other reports of compromised cards are stored on the payment card companies' databases.

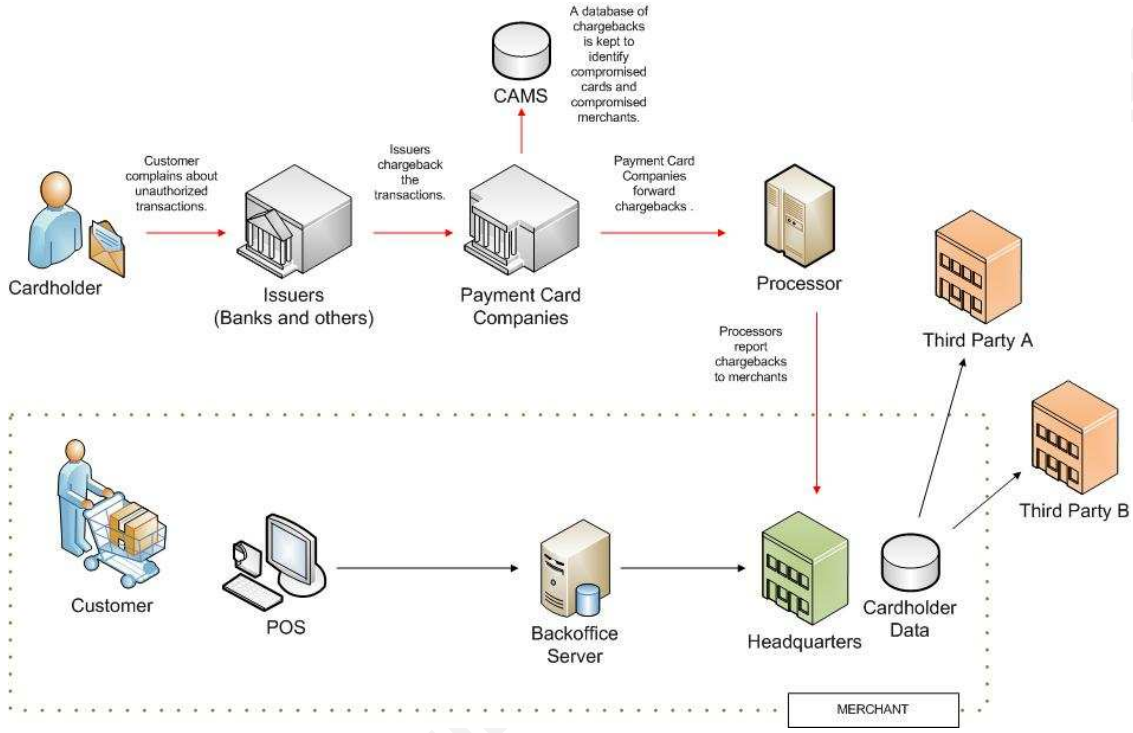

Figure 1. Chargeback's dataflow

Using correlation technology, payment card companies can pinpoint the source of the breach. Compromised cards would have transactions with a common merchant, or even a specific store. As a larger number of cards are compromised, the easier it is to identify the merchant who has been compromised.

3.2. Breaches Discovered by Law Enforcement

Law enforcement has been very successful in detecting compromised companies by taking an active role in combating cyber fraud.

In 2003, the FBI (Federal Bureau of Investigations) mounted a sting operation using an informant to run TheGrifters.net, a carders site. The informant recorded private messages and IRC chats for the FBI (Zetter, 2007). These recording were not only helpful to make a case against criminals but also allowed the FBI to be aware of breaches even though the victims were not even aware.

For almost two years, beginning in 2006, the FBI while involved in a sting operation, was able to run Darkmartket.ws, which posed as a forum where identity thieves, credit card fraudsters, and crackers could exchange tips as well as trade hacker tools and stolen cardholder data. Federal agents used intelligence from the site to develop intelligence reports and mount investigations (Leyden, 2008).

In 2009, an U.S. Secret Service undercover operation came to light after one of its informants, Albert Gonzales, was involved in several intrusion incidents. According to Computerworld, Gonzales helped put away nearly 30 fellow hackers. Months later, Albert Gonzales himself would be indicted as the mastermind behind the largest case of computer crime and identity theft ever prosecuted.

All these covert operations provide law enforcement with key intelligence to detect security breaches and prevent additional compromises. In many cases, such as in the Forever 21's breach, the United States Secret Service and/or the Federal Bureau of Investigation informed companies of the security breaches that were discovered during the undercover operations (Savage, 2008).

3.3. Understanding Where Cardholder Data Could Be Compromised

The paper will focus our analysis on two possible scenarios: 1)

liability from a merchant's and 2) the service provider's perspective.

In the first scenario, a brick-and-mortar retailer accepts payment cards as a method of payment from their point of sale (POS). The transactions are sent to an office or a corporate server(s) for authorization. The authorization servers will then communicate with one or more payment processors, which will then forward the transactions to the payment card brands. Finally, the payment card brands connect with the card issuers, which will authorize or decline the transaction. For some payment card companies such as American Express, Discover and AJB, this dataflow may be slightly different.

For this scenario, the merchant also shares cardholder data with two service providers. The third party service providers could be anything from loyalty programs to an outsourced customer service center. A compromise could occur at any of the following locations depicted below in the diagram, including the third party location(s).

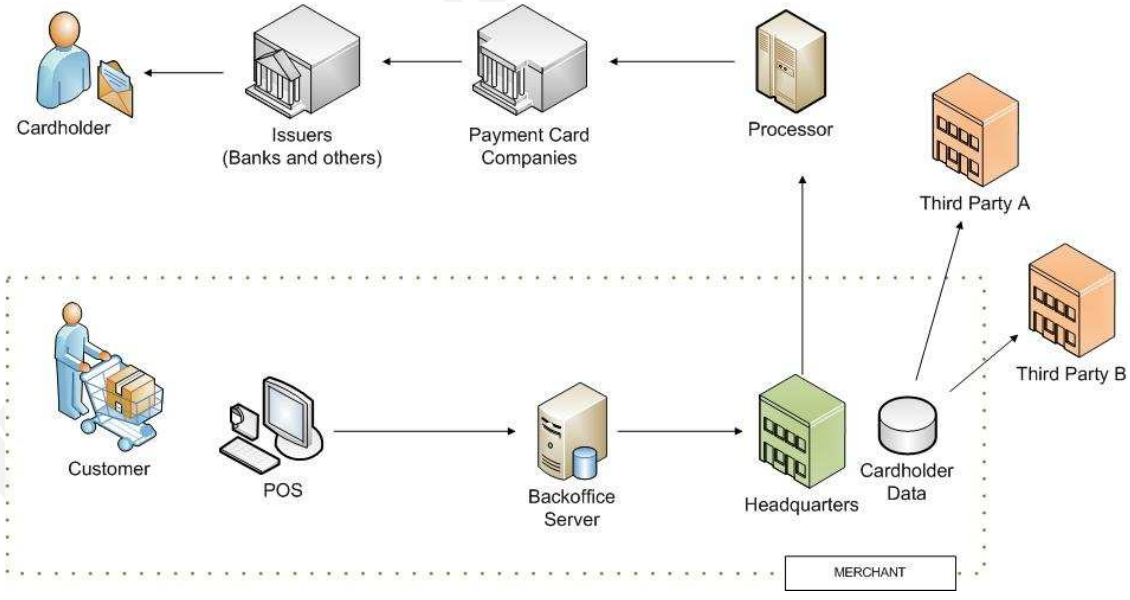

Figure 2. A merchant's cardholder dataflow

In a second scenario, the service provider outsources some of the sale channels for the merchant. As an example, only ecommerce transactions have been outsourced, but as mentioned previously, it could be any service where the third party impersonates the merchant (mail orders, telephone orders, marketing, etc). As in the first scenario, cardholder data could be compromised at any of the locations.

These two scenarios show typical cases where cardholder data could be shared between merchants and service providers.

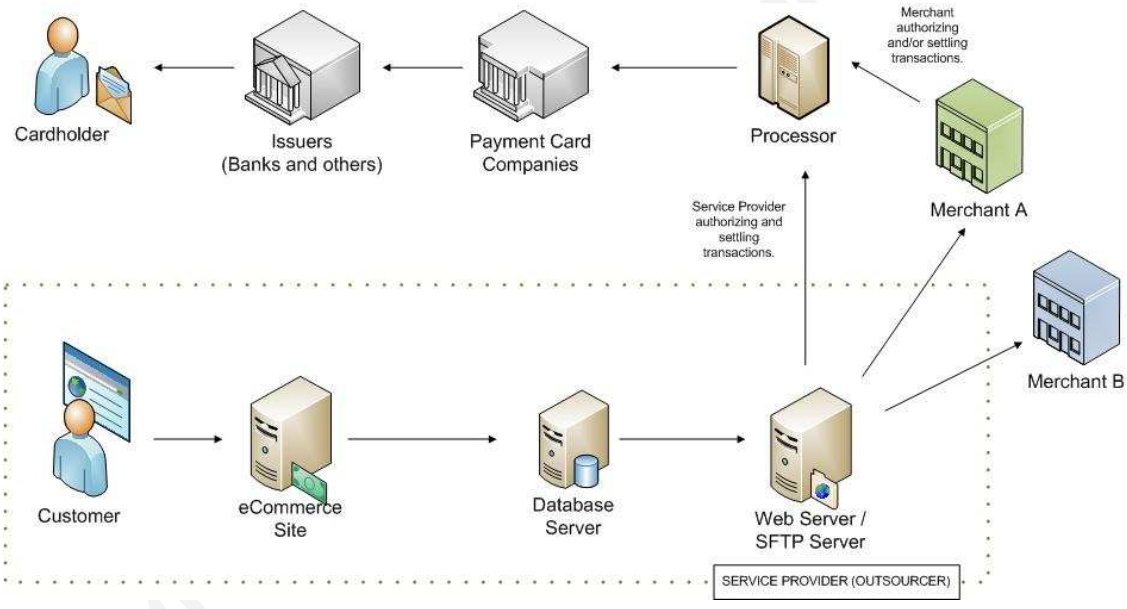

Figure 3. A service provider's cardholder dataflow

In order to understand liability, and especially when an outsourcer impersonates a merchant, it's important to understand that a customer doesn't really care whether the merchant runs their own ecommerce site or whether it has outsourced it to a third party. As

far as the customer knows, he's dealing with the merchant. In the event of a breach, annoyed customers will always target the merchant. The key here is how the merchant is able to transfer that liability to the service provider.

3.4. Sharing Cardholder Data Complicates Breach Investigation

Sharing data with third parties could make identifying the source of a breach more difficult.

Since 70% of the breaches are detected by a third party, once notified, the merchant may only have a few leads in their search to identify the source of the breach. Usually, when law enforcement notifies companies they usually cannot share evidence that may compromise their investigation. As part of the notification, the merchant sometimes is only told that suspicions of a breach exist. In a few cases, a list of compromised cards may be provided. Using those few leads, the merchant usually has to initiate the difficult task of identifying the source of that possible breach. In almost all cases, whether the breach occurred at the merchant or at one of its service providers, several issues could arise between a merchant and its service providers. A clear and well-planned agreement will be more than useful. It would be critical.

4. Contracting for PCI DSS Compliance

4.1. What Could Go Wrong?

The quick answer is anything can go wrong. Let's consider the following real cases:

Case 1: Vendor's liability

A merchant added to its ecommerce website, a system component developed and maintained by a software developer vendor. The merchant also outsourced IDS/IPS monitoring to a managed security services vendor (MSS). The system component had security vulnerabilities and the merchant was breached. In addition, to that the IDS was unable to detect the attacks because alerts on HTTP/HTTPS traffic was mistakenly disabled by the MSS vendor staff. The breach meant several millions of Dollars to the merchant, and they were unable to recoup them from any of the vendors.

Case 2: Audit rights

Another merchant outsourced most of their IT operations to a MSS vendor. In order to reduce costs, the third party uses their IT infrastructure to host several clients. When the merchant had a QSA (Qualified Security Assessor) verifying their PCI DSS compliance, the QSA asked the vendor to demonstrate PCI DSS compliance either by providing a ROC (Report On Compliance) or allowing the systems in scope to be validated. The third party refused arguing that their systems hosted other client's data and that their current agreements did not allow them to authorize a review. This obviously affected the merchant's PCI DSS compliance review.

Case 3: Forensic Reviews Expenses

A major Card Brand informed a merchant that several cards used to buy merchandise at their stores were compromised. The Brand requested the merchant to have their systems reviewed by a QIRA (Qualified Incident Response Assessor). The merchant asked one of its service providers to have its infrastructure reviewed, as well. The service provider had a QIRA conducting their review, as requested per the merchant. Later, it was identified that the breach occurred at other service provider for which the vendor shared data, as well. The first service provider spent time and money conducting the forensic review. They, obviously, requested to be compensated for that.

Case 4: Data Protection Baseline

A company was using the following clause to ensure that their service

providers implemented adequately protection:

> *Each party will protect the other party's Confidential Information from unauthorized use, access or disclosure with the same measures that the recipient takes to protect its own proprietary information of like importance, but in no event less than reasonable care.*

When the company applied for PCI DSS Compliance, the QSA reviewed one of the service provider's systems and found that cardholder data was stored in clear text. When questioned about that, the service provided argued that their proprietary information was not encrypted either, hence, a breach of contract did not exist, because they were "applying the same measures they take to protect its own proprietary information".

Case 5: Data Retention

Several merchants used the same service provider to host their e-commerce websites. The service provider hosted the data for these merchants on the same database. As a result, every back up contained data for all these merchants. One of the merchants had a lawsuit with a large client and requested the service provider to retain backup tapes until the dispute is settled. The backup retained other merchant's data that could be unnecessarily retained violating their data retention policy.

4.2. The PCI DSS Contract Chain

David Navetta, founding partner of the Information Law Group, clearly explains the importance of contracts when dealing with PCI DSS compliance.

> "Unlike security laws such as Gramm-Leach-Bliley, HIPAA and Sarbanes-Oxley, the PCI Standard and Security Program rules are not statutes or regulations enforced directly by the government. Rather, the PCI Standard and the Security Program rules are imposed and typically enforced contractually through the PCI Contract Chain.

> At the top of the chain are the payment card companies. The payment card companies establish merchant relationships by working through "merchant" or "acquiring" banks. The contract between merchant banks and payment card companies is the first contractual relationship in the payment card industry chain. The merchant banks (or payment processors working with the merchant banks) process the payment card transactions for the payment card companies they partner with. If a merchant wants to be able to accept payment cards to transact business, it must be vetted by a merchant bank (or payment processor) and enter into a contractual relationship with that merchant bank (or payment processor). Finally, merchants sometimes enter into relationships with service providers for the processing, storage or transmittal of payment card data. As the final link in the chain, merchants and service providers will enter into contractual relationships." (Navetta, 2009)

He also identified several of the legal issues of PCI DSS Compliance:

> "**(1) No Direct Contractual Relationship between Merchants and Payment Card Companies.** The significance of the chain is that there is typically no direct contractual relationship between payment card companies and merchants. Therefore, generally speaking, merchants cannot be directly required to legally adhere to Security Programs or the PCI Standard by payment card companies. Rather, if any contractual obligations do exist they are passed through the contract that exists immediately upstream from the merchant (e.g. the contract between the merchant and merchant bank or payment processor). Nonetheless, in practical terms, payment card companies may be able force compliance by leveraging their relationships with merchants and access to payment card processing.
>
> **(2) No Direct Duty for Service Providers to Comply with PCI or Security Programs.** There is typically no inherent duty for a merchant's service providers to comply with the PCI Standard. Any duty for a service provider to comply with the PCI Standard will flow contractually from the merchant to the service provider (typically not from the payment card companies to the service provider). Therefore, unless merchants

impose contractual obligations on their service providers, they may find themselves without leverage to force those service providers to become PCI compliant.

(3)A Merchant Compliance with PCI is Directly Contingent on Contractual Obligations Imposed on its Service Providers. Section 12.8 of the PCI Standard requires merchants to do the following:

If cardholder data is shared with service providers, then contractually the following is required:

12.8.1 Service providers must adhere to the PCI DSS requirements

12.8.2 Agreement that includes an acknowledgment that the service provider is responsible for the security of cardholder data the provider possesses.

If these duties are not contractually established then the merchant may not be able to establish its own compliance with PCI.

(4) Matching Upstream and Downstream Obligations and Risk. The scope of a merchant's PCI obligations (including compliance with the PCI Standard and Security Programs) is dictated by its upstream contracts with merchant banks or service providers. Merchants must protect themselves by imposing upstream PCI contractual obligations and risks downstream to their service providers. So if a merchant agrees to pay fines and penalties for failure to comply with PCI, it should also require its service providers to pay any fines and penalties imposed on the merchant because of the service provider's failure to comply.

The contractual nature of PCI makes it necessary for a merchant's legal staff to understand and become involved in the PCI compliance process. Most of the issues outlined above require legal analysis, contract drafting and negotiation. Attorneys should develop strategies for limiting liability from upstream contracts, and passing liability downstream to service providers.

One area of special difficulty is existing service provider relationships. If a merchant faces fines or the loss of processing capability because its existing service providers are not PCI

> compliant, it could be difficult to re-open negotiations and force service providers to invest the time and resources to become PCI compliant. As such, before fines and threats start coming in, a merchant's legal staff should be devising a strategy for addressing PCI contractually with existing service providers (as well as new providers). While these contractual issues are challenging, the transformation of PCI into a legal standard of care can pose even greater difficulties for an organization." (Navetta, 2009)

A link to Navetta's complete posting is included in the references.

4.2 Merchants: Clauses that should be Considered

Most of the following clauses have been selected from material for SANS LEG-412 training, *Contracting for Data Security and Technology*, and have been slightly modified to specifically cover important areas required by PCI DSS.

4.2.1 PCI DSS Compliance Clause

Consider adding the following clause to ensure that your Service Provider will meet and maintain PCI DSS compliance. As seen in case 4, a generic clause may not be sufficient to ensure that the Service Provider will implement all the security controls required by PCI DSS.

> *CUSTOMER is required to periodically demonstrate compliance with PCI DSS (Payment Card Industry Data Security Standard). The compliance process requires CUSTOMER to undergo an assessment that includes all the system components used to process, store or transmit cardholder data, and any other component that resides on the same network segment that those system components, hereafter known as "System Components in Scope". Some of those system components and/or processes have been*

outsourced to SERVICE PROVIDER.

SERVICE PROVIDER will achieve and maintain PCI DSS compliance against the current version of PCI DSS published on the PCI SSC (PCI Security Standards Council) website. As evidence of compliance, SERVICE PROVIDER will provide when requested, a current attestation of compliance signed by a PCI QSA (Qualified Security Assessor)

If SERVICE PROVIDER is unable to provide a current attestation of compliance, SERVICE PROVIDER will allow Customer's QSA to assess all the system components in scope that are hosted or managed by SERVICE PROVIDER, and the related processes used to process, transmit or store cardholder data.

SERVICE PROVIDER will create and maintain reasonable detailed, complete and accurate documentation describing the systems, processes, network segments, security controls, and dataflow used to receive, transmit, store and secure Customer's cardholder data. Such documentation will conform to the most current version of PCI DSS. SERVICE PROVIDER will, upon written request by CUSTOMER, makes such documentation and the individuals responsible for implementing, maintaining and monitoring those system components and processes available to:

a) QSAs, forensic investigators, consultants or attorneys retained by CUSTOMER to facilitate audit and review of Customer's PCI DSS compliance.

b) Customer's IT Audit Staff.

[SERVICE PROVIDER} will retain such documentation until ____ years after termination of this agreement.

4.2.2 Security Clause

PCI DSS compliance specifically describes the security controls that are required to be compliant. However, it does not include any notification requirements. The second part of this typical security clause may be necessary to require the Service Provider to notify any security incidents related with cardholder data.

SERVICE PROVIDER will use reasonable precautions, including but not limited to, physical, software, and network security measures, employee screening, training, and supervision and appropriate agreements with employees, to prevent anyone other than CUSTOMER or its authorized employees from monitoring, using, gaining access to or learning the import of CUSTOMER Data; protect appropriate copies of CUSTOMER Data from loss, corruption or unauthorized alteration; and prevent the disclosure of CUSTOMER passwords and other access control information to anyone other than authorized CUSTOMER employees.

SERVICE PROVIDER will periodically test and re-evaluate the effectiveness of such precautions. SERVICE PROVIDER will notify CUSTOMER within ____ hours, if such precautions are violated and CUSTOMER Data are affected thereby or passwords or other access information is disclosed. Notwithstanding the foregoing, SERVICE PROVIDER and its employees may use, process, view the contents of or monitor CUSTOMER Data to the extent necessary for SERVICE PROVIDER to perform under this agreement.

4.2.3 Data Retention Clause

Companies should recommend on how long data should be retained and how it should be deleted.

SERVICE PROVIDER will erase or destroy all media under its control containing copies of Customer Data not later than ____ days after the processing of such data, except where special circumstances, of which SERVICE PROVIDER has given CUSTOMER written notice, warrant longer retention. For purposes of this agreement, to "erase" means to render the relevant data unrecoverable by any means according to PCI DSS v.1.2.1. Requirement v.9.10.2

4.2.4 Data Ownership Clause

According to Benjamin Wright, SANS LEG-412 instructor, a service provider could assert an artisan's lien on data if the provider's charges are not paid. In order to avoid data being

held up during a dispute settlement consider the following clause:

> *SERVICE PROVIDER has no property interest in, and may assert no lien on or right to withhold from the CUSTOMER, any data it receives from, receives address too, or stores on behalf of the CUSTOMER.*

Don't allow a service provider the opportunity to claim that they own your data. They may sell the data to companies specialized in loyalty programs, customer relationship marketing, etc. If that data is compromised, those transactions could be pointing your company as one of the possible sources of the breach. Demonstrating that you are not responsible could be a lengthy and costly process and may cause more than one headache.

4.2.5 Archive Segregation Clause

As seen in case # 5, per e-Discovery requirements, tape backups could be retained indefinitely. Companies should consider requiring that archived data not be backed up or comingled with other customers' data if cardholder data is not encrypted.

> *All records, data and files stored by the [SERVICE PROVIDER] as archives of Customer's Data including the media on which they are stored, are the exclusively property of CUSTOMER, and SERVICE PROVIDER may assert no lien on or right to any of the same. SERVICE PROVIDER will conspicuously mark all such archival storage media as Customer's property. At Customer's request, SERVICE PROVIDER will, for [a certain fee], promptly deliver to Customer and if requested destroy any other remaining copies that Customer will no longer need.*

4.2.6 Subpoena Clause

You should consider this clause to avoid the government, through

a court, a taxing authority, an investigative agency or a regulatory body attempting to gain access to your data hosted at a third party Hosting/Managed Service Provider's infrastructure, without you having timely notice so you could monitor and contest the attempt.

> *If SERVICE PROVIDER is served with a warrant, subpoena or any other order or request from a government body or any other person for any record or files of CUSTOMER Data, SERVICE PROVIDER will, as soon, as reasonably practical and not in violation of law, deliver to CUSTOMER a copy of such warrant, subpoena, order or request and will not, without Customer's prior written consent, comply with the same unless and until required to do so under applicable law.*

4.2.7 PCI DSS Clause for Software Vendors

Companies using third-party software to process credit card transactions may consider adding the following clause:

> *Vendor warrants that the Software meets PA-DSS (Payment Application Data Security Standard) requirements, and that the CUSTOMER following Vendor's instructions detailed in the PA-DSS Implementation Guide will be able to deploy and maintain the Software according to PCI DSS (Payment Card Industry Data Security Standard) requirements. Vendor agrees to indemnify and hold Customer harmless from any claims, damages, cause of action, costs and expenses arising out of or related to any breach of the warranty set forth in this paragraph.*
>
> *In the event that security vulnerabilities are identified on the Vendor's Software, VENDOR will promptly notify CUSTOMER and will provide instructions to mitigate risk of that vulnerability being exploited. VENDOR will provide a patch release or security update within ___ days of a security vulnerability being discovered, and will provide support as necessary to properly deployed the patch or security update.*

4.3 Service Providers: Clauses that Should Be Considered

Service providers also have to consider special cases where their customers' PCI DSS Compliance may affect them.

4.3.1 Security Clause

Service Providers should consider adding a clause to limit liability as a result of Customer's actions.

> *SERVICE PROVIDER will not be liable for the disclosure, monitoring, loss, alteration or corruption of CUSTOMER Data to the extent it results from Customer's failure to implement reasonable security measures to protect against the unauthorized use of facilities, computers network access devices and passwords.*

4.3.2 Audit Clause

For the reasons described previously, a customer may request a service provider to conduct a forensic review even if there is no evidence that point to the security breach in the service provider's infrastructure. Service provider should have a clause in place to recoup the expenses of conducting a forensic review unless they were effectively the source for the data breach.

In the addition to the merchant's audit clause, service providers could add the following:

> *CUSTOMER will pay SERVICE PROVIDER [a certain fee] for complying with such requests.*
>
> *In the event that CUSTOMER requires SERVICE PROVIDER to retain the service of a forensic investigator, CUSTOMER will be charged for any expenses incurred in those assessments, provided that SERVICE PROVIDER was not responsible for a compromise in Customer's systems and/or data.*

5. Conclusion

Companies should carefully review and amend their agreements with third party service providers that handle or have access to cardholder data. Having the proper legal language in place is one of the key factors to reduce liability when dealing with third parties and limiting your companies' exposure to additional risk.

Acknowledgments

Special thanks to Tiff Cook, Verizon Business PCI DSS team, for providing technical and content review.

References

Verizon Business RISK Team. (2009). 2009 Data Breach Investigations Report. Retrieved April 3, 2009, from Verizon Business Website: http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Zetter, K. (2007). I Was a Cybercrook for the FBI. Retrieved August 21, 2009, from theregister.co.uk Website: www.wired.com

http://www.wired.com/politics/onlinerights/news/2007/01/72515

Leyden, J. (2008). Darkmarket carder forum revealed as FBI sting. Retrieved August 21, 2009, from www.theregister.co.uk Website: http://www.theregister.co.uk/2008/10/14/darkmarket_sting/

Gaudin, S. (2009). Government informant is called kingpin of largest U.S. data breaches. Retrieved February 22, 2010 from www.computerworld.com Website:

http://www.computerworld.com/s/article/9136787/Government_informant_is_called_kingpin_of_largest_U.S._data_breaches

Savage, M. (2008) Forever 21 security breach compromises nearly 99,000 payment cards, Retrieved February 22, 2010 from searchsecurity.techtarget.com Website:

http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1330903,00.html

SANS Institute. (2008). Legal 412 Contracting for Data Security and Other Technolgy. SANS Institute.

Navetta, D. (2009). The Legal Implications, Risks and Problems of the PCI Data

Security Standard. Retrieved February 22, 2010, from infoseccompliance.blogspot.com Website: http://infoseccompliance.blogspot.com/2008/02/legal-implications-risks-and-problems.html