Global Data Privacy and Security Team

Bryan Cave's Global Data Privacy and Security Team works with data security and risk assessment issues to routinely help clients before a breach happens analyze and improve upon their ability to respond to, and minimize the liability from, a breach if (or when) one occurs.

For more Information Contact:

David A. Zetoony
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
T: 202 508 6000

One Boulder Plaza
1801 13th Street, Suite 300
Boulder, CO 80302-5386
T: 1 303 444 5955

Courtney Stout
Associate
courtney.stout@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
1 202 508 6076

To join Bryan Cave's data privacy and security distribution list visit Bryan Cave Data Matters.

BRYAN CAVE

Negotiating the Details: Credit Card Processing Agreements for Retailers

Credit cards are the primary form of the payment that most retailers receive. In order to process credit cards a retailer must enter into an agreement with a bank and a payment processor that will process credit card transactions on its behalf. Those agreements can be daunting and often have significant impacts on a retailers financial liability in the event of a data breach. Indeed, in many cases the contractual liabilities that flow from the credit card processing agreement surpasses all other financial liabilities that arises from a breach including litigation, regulatory investigations, and the cost of conducting an investigation.

The number of companies that offer payment processing services for in-store (point of sale) transactions in the United States. [1]

102

The amount of Target's contractual liabilities to its payment processor in connection with just one of the four major payment brands.[2]

67
MILLION

The word count of a typical payment processing agreement.

25,000

Key contract provisions in card processing agreements include:

☑ Card Network Rules, PCI / EMV and related obligations:

- Incorporation of Card Network Rules:
  - Is Vendor required to comply with card network rules? Does the contract specifically reference the security rules of the card networks – DISC, CISP or other?
  - Is Vendor required to comply with PCI DSS?
  - Is there a requirement to comply with processor's or merchant bank's Operating Guidelines? Was a copy provided to Vendor?
- Incorporation of EMV Compliance: Does the contract or correspondence confirm the services will be EMV compliant by October 2015?

☑ Applicable Law: Is there a requirement for Vendor to comply with applicable laws and regulations? Does the provision reference privacy and data security laws?

☑ Subcontractors: Is Vendor responsible for acts and omissions of third party providers? Is Vendor required to disclose any third party subcontractor that accesses/stores/transmits PCI data?

☑ Exclusivity: Are there any restrictions on retailer's ability to hire third parties?

☑ Confidentiality / Data Security:

- Is Vendor subject to confidentiality obligations at least as protective as those in the processor agreement?

[1] http:www.visa.com/splisting/searchGrsp.do (last viewed Sept. 2015) (search conducted of "payment processing POS / Card present" and "United States").
[2] Robin Sidel, "Target to Settle Claims Over Data Breach: Retailer to pay Visa issuers up to $67 million," Wall Street Journal (Aug. 18, 2015).

  - Data storage: Does Vendor agree not to store / transfer PCI data or sensitive consumer data outside the US?
  - Is Vendor required to maintain security safeguards or have other data security requirements?
  - Does Vendor provide representations or warranties about data security or the provision of services generally?
  - Does the confidentiality provision require Vendor to notify retailer to give retailer a chance to obtain a protective order prior to disclosing confidential information in response to a request from a regulator or other third party?

- ☑ Data Incident:
  - Is Vendor required to notify retailer immediately of a data breach involving retailer data?
  - Is Vendor required to cooperate in a data breach?
  - Is Vendor required to comply with payment card network rule requirements in the event of a data breach (e.g., does the agreement require Vendor to hire a PFI)?
- ☑ Reserve:
  - Does the Vendor have an unlimited right to establish a reserve?
  - Are there reserve terms to protect the retailer, such as:
    - A cap on the total reserve amount?
    - A daily cap on the percentage of sales Vendor may withhold when establishing a reserve?
    - Is the reserve amount tied to a calculation based on objective risk criteria?
    - Is there a termination of the reserve and payment of funds?
    - Is the reserve comingled with other merchant's funds?
- ☑ Service Level Agreement:
  - Does the Vendor have measurable, object performance criteria?
- ☑ Vendor Liability:
  - Is Vendor liable for data breaches that occur within its systems?
  - Does Vendor indemnify retailer for damages resulting from a data breach that occurs within its systems?
  - Is there a mutual disclaimer of types of damages?
  - Is there a mutual liability cap? An enhanced liability cap for data breach? Or, what is excluded from the cap?
  - Is Vendor liable for assessments from card networks resulting from a data breach that occurs within its systems? Does retailer have a right to appeal, or step into the shoes of the vendor to contest a card network assessment resulting from a data incident?
  - Note whether retailer has unlimited or uncapped liability to Vendor.
- ☑ Audit:
  - Does retailer have a general audit right? A regulatory audit right?
  - Does retailer have a right to conduct a security audit?
  - Is Vendor required to provide an annual SSAE 16?
  - Does retailer have a right to terminate if a material deficiency in Vendor's SSAE 16 report is noted that puts PCI data at risk.
  - Is remediation required?
- ☑ Insurance: Is Vendor required to have insurance?
  - Does the insurance exclude or significantly sublimit the contractual liabilities incurred by the vendor?
  - Does the insurance exclude or significantly sublimit PCI related expenses?
  - Is the insurance limit within the ballpark of that which would cover a catastrophic breach (e.g., $2 * quantity of data involved)?
  - Is the Vendor required to maintain the insurance, with similar substantive terms, throughout the life of the contract?
- ☑ Term:
  - What is the term?
  - Does this agreement automatically renew? If so, how long is the renewal period?
  - What date is the deadline for submitting a notice of non-renewal?
- ☑ Termination and Termination Assistance:
  - Be clear on events of default and the standards for termination of the contract.
  - Is the Vendor obligated to continue providing services in the event of termination / expiration?
  - Is Vendor obligated to help transition data regardless of reason for termination?
- ☑ Business continuity and disaster recovery:
  - Does the Vendor have adequate business resumption and disaster recovery plans?
  - Does the contract address procedures when data is inaccessible?
- ☑ Dispute resolution or arbitration provisions: