BCLP. Client Intelligent

RetailLawBCLP

REDUCE POTENTIAL LIABILITY FOR DATA SECURITY BREACHES BY NEGOTIATING COVERAGE IN PAYMENT PROCESSING AGREEMENTS

Jan 13, 2017

Credit cards are the primary form of payment received by most retailers. In order to process a credit card, a retailer must enter into an agreement with a bank and a payment processor. Payment processing agreements often have significant impacts on a retailer's financial liability in the event of a data breach. In many cases, the contractual liabilities that flow from a payment processing agreement surpass all other financial liabilities that arise from a data breach, including the cost to investigate an incident, defend litigation, and defend a regulatory investigation.

The following checklist describes common data security related provisions to look for within most payment processing agreements:

1. **Incorporation of Payment Brand Rules.** Most payment processing agreements incorporate by reference the rules, regulations, and guidelines of the payment brands (American Express, Discovery, MasterCard, and/or Visa). When negotiating a payment processing agreement, it is important to determine whether the obligation to abide by the payment brand rules is unilateral (*i.e.,* is imposed only upon the merchant) or reciprocal (*i.e.*, is imposed upon the merchant, the acquiring bank, and the payment processor).

2. **Incorporation of the Payment Card Industry Data Security Standard.** Many payment processing agreements reference the PCI DSS and require that a merchant be, and remain, in full compliance with the requirements of the PCI DSS. When negotiating a payment processing agreement it is important to determine whether you are, or are not, currently in compliance with the PCI DSS, and whether the obligation to comply with the PCI DSS is unilateral or reciprocal. Put differently, does the agreement require just the merchant to comply with the PCI DSS or does it require all parties to comply with applicable portions of the standard? Note that even if a payment processing agreement does not expressly incorporate the PCI DSS, if the payment processing agreement incorporates the Payment Brand Rules, the Payment Brand Rules may themselves incorporate the PCI DSS by reference.

3. **Incorporation of Other Rules, Guidelines, or Procedures.** Some merchant banks and payment processors maintain their own procedures, protocols, or "operating guidelines," and attempt to incorporate those documents by reference into a payment processing agreement. If you are negotiating an agreement that incorporates bank or processor specific rules, be sure to ask for a copy of those documents. Note that many banks do not make such documents public (they are not available online); a contracting party must specifically ask for a copy or request access to a password restricted repository.

4. **Payment of Assessments.** Most merchant banks and payment processors attempt to require that a merchant indemnify them for any fine, penalty, assessment, or other contractual liability, imposed by the payment brands upon the merchant bank or the payment processor as a result of a data security incident that occurs at the merchant. In many situations these "assessments" form the greatest financial liability imposed upon the merchant after a data breach.

5. **Assignment of Rights.** If a merchant is required to indemnify a merchant bank and/or payment processor for fines, penalties, assessments, or other contractual liabilities imposed by the payment brands, the merchant has a strong interest in being able to appeal, or contest, those liabilities before they are incurred. Some merchant banks and payment processors have assigned, or subrogated, their rights vis-à-vis the payment brands to the merchants. Doing so ensures that the merchant is able to "stand in the shoes" of the bank and the payment processor to ensure that the assessments that are issued (and which the merchant must pay under an indemnification obligations) are reasonable and appropriate.

6. **EMV Compliance.** In October of 2015, the payment brands instituted new rules intended on encouraging merchants, banks, and payment processors to adopt the EMV standard (*e.g.,* chip and pin). When negotiating a payment processing contract it is important to understand what, if any, requirements are imposed upon the parties to be compliant with the EMV standard.

7. **Applicable Law:** Payment processing agreements typically contain a broad mandate that the merchant comply with applicable laws and regulations. Often such agreements will specifically reference data privacy and security laws. As with other sections in the agreement, it is important to note whether obligations to comply with privacy and security laws are unilateral or reciprocal.

8. **Subcontractors:** Does the payment processing agreement attempt to hold the merchant responsible for the acts and omissions of its third-party service providers? Some payment processing agreements also require that a merchant disclose its use of third party subcontractors that accesses/stores/transmits PCI data to its bank and/or payment processor.

9. **Exclusivity:** Does the payment processing agreement impose any restrictions on a merchant's ability to hire third parties? Does it impose any restrictions on a merchant's ability to use other payment processors or merchant banks?

10. **Confidentiality / Data Security:** Consider whether the payment processing agreement contains the following specific confidentiality and data security terms:

    - Is the merchant bank or payment processor subject to confidentiality obligations at least as protective as those to which the merchant is subject?
    - Is the bank or payment processor permitted to store / transfer payment card information outside the United States?

11. **Data Security Incidents:** Payment processing agreements typically require that a merchant notify a bank or a payment processor of a data breach. Consider whether the agreement contains a time period that may be difficult to comply with (immediate notification) or one that may be commercially practical *(*notification within 72 hours of discovery of an incident)? As with other provisions in the payment processing agreement, is the breach notification obligation unilateral or reciprocal?

12. **Reserve:** Many payment processing agreements permit a merchant bank or payment processor to establish a reserve in the event of a data security incident. Often a bank or a payment processor will attempt to negotiate a provision which permits them to fund the reserve using the proceeds from any credit card transaction. If a reserve provision is proposed consider whether there are sufficient terms to protect the merchant 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?

13. **Vendor Liability:** As discussed above, "reciprocity" is a constant theme when evaluating a payment processing agreement. In the context of liability, consider whether your payment processing agreement holds your bank and payment processor liable for breaches that occur within their systems, whether they are required to indemnify you for damages that would relate to such a breach, and whether any cap that applies to their damages is similar to any cap that applies to the merchant's damages.

For more information on this topic, please contact the author, David Zetoony, or any member of our Retail team.

MEET THE TEAM

Merrit M. Jones

San Francisco

merrit.jones@bclplaw.com
+1 415 675 3435
