AmWINS Group, Inc.

CLIENT ADVISORY

CYBER COVERAGE FOR BANK ASSESSMENTS: WHAT MERCHANTS AND THEIR INSURANCE BROKERS NEED TO KNOW

Coverage under a cyberliability insurance policy with respect to assessments levied on behalf of a financial institution or payment processing entity varies quite significantly throughout the marketplace. The nuances of the coverage differences will continue to grow as more and more companies begin to recognize the exposure inherent in electronic payment processing.

Monetary fines are levied by the card brands against merchants as a result of non-compliance with the payment card industry data security standards (PCI-DSS) which are set by the payment card industry security standards council (PCI SSC). A very important distinction lies within the definition of fines, costs or expenses as respects common cyber policy language. “Fines” are often merely reserved for costs levied directly against an insured for the breach of PCI standards set by the PCI SSC. The fines, which are punitive in nature, result from failing to comply with the standards. On the other hand, “assessments” are costs specifically associated with liabilities arising out of a Merchant Service Agreement (MSA). The card brands are looking to recoup expenses that resulted from a security breach by the merchant. Assessments can be costs resulting from a breach of the card brand rules, costs passed along to the merchant through the withholding of funds by a merchant bank, card reissuance expenses, fraud losses and a number of other liabilities arising out of obligations under an MSA.

To further clarify this distinction, merchants that accept payment cards are placed into a payment card network (i.e. VISA or MasterCard) by the bank or financial institution with whom they enter into a MSA. At the time of a sale, merchants submit card information to a bank or financial institution, which passes it through the payment card network to the cardholder’s payment card issuer (i.e., Citibank or Bank of America). Once approved, the funds flow back through the bank to the merchant. In the event of a data breach, a payment card company may assess fines or other amounts on the bank involved. The bank will then seek to pass that liability along to the merchant, which is often achieved through the withholding of funds owed to the merchant. As an oversimplified example, consider this: The merchant may be waiting for the card company to pay them $100,000 for all their billings during the month. If they get fined, they may only get $60,000 paid to them with the other $40,000 being withheld as a fine. As a result, this has proven quite costly given the disruption of cash flow.

Currently pending in federal court, apparel retailer Genesco is involved in litigation against VISA for assessments levied as a result of a data breach. Upon confirmation from a forensic audit, the retailer was found guilty of three different PCI-DSS violations, resulting in a $13 million assessment. That assessment was levied against the banks involved, which Genesco had to indemnify under the terms of their MSA. The suit against VISA is an attempt to recover the assessment costs absorbed by Genesco. However, it has been speculated by the court that if the breach did not involve actual theft of data, then the assessment may be deemed an unenforceable penalty.

There are a few places to look in order to truly understand the payment card exposure for a given client; it’s important to both review the MSA and understand exactly how the merchant processes credit card transactions. A company may simply be processing through a swipe box that doesn’t retain card information or they could be processing transactions through a point of sale (POS) system, which does store card information, thus multiplying the exposure. Essentially, an MSA places obligations on a merchant when a payment card company views the merchant as the potential source of the breach, which can result in the merchant paying for a forensic audit as well as additional fines or penalties.

(continued on next page)

CONTACT

To learn more about how AmWINS can help you place coverage for your clients, reach out to your local AmWINS broker or marketing@amwins.com.

AmWINS Group, Inc.

CLIENT ADVISORY

CYBER COVERAGE FOR BANK ASSESSMENTS: WHAT MERCHANTS AND THEIR INSURANCE BROKERS NEED TO KNOW

(*continued from previous page*)

Insurance carriers are approaching coverage for assessments in a variety of ways, which magnifies the importance of closely reviewing the policy form and endorsements. Some cyber products are clearly defining PCI fines, expenses and costs via policy form, which may reference assessments arising out of a MSA. Carriers can even include coverage for costs or amounts levied as part of a MSA per the definition of damages. Some even go as far as carving back their exclusionary wording to clearly address this particular coverage detail. However, not all carriers directly acknowledge this distinction which could play an increasingly significant role for many businesses, especially companies with high frequency payment processing.

Alternatively, there are a number of carriers that don't address the distinction of assessments levied out of liability under a MSA. Subsequently, they are not only ignoring this important distinction, but their approach to the contractual exclusion seems to all but outright exclude any coverage for liability arising out of any contract or agreement.

Companies must confront the reality that their most significant liability threat as a result of a data breach or unauthorized disclosure may not come from the consumer, but from their business partners. Those business partners include banks and payment card processors. Although fines vary depending on the volume of payments processed by the merchant and the number of violations, companies that experience a data breach can be fined and assessed millions of dollars as a result of their obligations under a MSA. Merchants and their legal representative should closely review their payment card agreements and have a very direct dialog with their insurance broker and underwriters to be certain that the coverage matches their needs and expectations.

Please feel free to reach out to your AmWINS professional lines broker with any questions or coverage needs.

This article was authored by Trey Waldrep, a professional lines broker at AmWINS Brokerage in Dallas, TX.