AmWINS Group, Inc.

CLIENT ADVISORY

THE COST OF A DATA BREACH

Within the last twelve months, we've seen data breaches at the likes of Target, Home Depot, Dairy Queen, Staples and Neiman Marcus, and there have been countless others at lesser known retailers around the U.S. Many of these breaches involve the theft of debit or credit card information. While there is much focus on the consumer in these situations, in reality they have a relatively painless experience. Because of a variety of state and federal laws, consumers are made aware of the breach and are often provided with free credit monitoring for a year. Further, their credit or debit card is replaced and, in general, consumers aren't held accountable for any fraudulent charges.

Retailers, on the other hand, not only suffer a public relations nightmare, but are susceptible to fines, penalties, and additional costs related to the loss of payment card data. In 2006, American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. formed the Payment Card Industry Security Standards Council (PCI SSC). According to their website, the PCI SSC "develops, maintains, and manages the PCI Security Standards, which include the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) Requirements." However, penalties for noncompliance are not imposed by the PCI SSC, but rather by the "payment brands and their partners."

Essentially, you have a council that cannot legally make a retail merchant be (or stay) compliant and, in the end, has no legislative authority to order reconciliatory action. So why is the PCI SSC of concern to retailers? Merchants that want to accept payment from the member companies must comply with the standards of the five organizations and, increasingly, merchants have to adapt to a market space that is increasingly driven by the use of credit and debit cards. According to the Federal Reserve Board, in 2012 there were an estimated 122.8 billion non-cash transactions, excluding wire transfers, with a value of $79 trillion. Now imagine not having the ability to accept the five major credit card brands.

However, PCI SSC compliance doesn't alleviate all concern. If a breach occurs, the retailer can be held responsible for fraud losses, the cost to reissue cards, and any additional fraud prevention and detection costs incurred by credit or debit card issuers. These costs will impact large, financially sound retailers, but they can cripple a smaller merchant.

Traditional insurance policies are triggered by a legal action against an insured and usually exclude the breach of a contract the insured has entered into – an obvious conflict as contracts are the building blocks of the payment card industry. Basically, a merchant contracts with a payment processor or bank which allows the merchant to accept payments via a credit or debit card. This contract is a Merchant Service Agreement (MSA). When a sale occurs, the transaction is reconciled by the consumer's card issuing bank or brand and funds are deposited into the merchant's account. With a breach, it is common for card brands and banks to reconcile fraudulent charges back to the event and push associated costs back to the retailer. When the charges are pushed back on the merchant as the source of the breach, there is a contractual obligation defined by the terms of the MSA, which can include significant fines depending on the particular credit card company or other financial remedies paid back to the merchant bank. Claims made insurance policies are generally triggered by demands for damages or lawsuits; these charges don't necessarily fit that definition of claim.

How can retailers insure against the financial burden of an assessment and fines/penalties that accompany a breach and the theft of credit or debit card information? Many carriers are at a crossroads. Underwriters recognize a systemic exposure across retail merchants accepting payment cards, but providing a solution means:

1. amending the form to get around a breach of contract exclusion inherent in most policies,
2. amending the definition of claim to respond to PCI DSS actions, and
3. providing affirmative coverage for an indefensible punishment from a quasi-regulatory authority.

(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.

THE COST OF A DATA BREACH

(continued from previous page)

Further, the coverage grant is often made on the reliance that insureds are PCI compliant, yet the compliance model offers them no protection in the event of a breach. In other words, there's no immunity from punishment even if a retailer demonstrates that they are following the standards set by PCI.

Understandably, many insurers are hesitant to provide the capacity that is needed in the retail space. While there are solutions available, only a handful of markets offer full limits with coverage for most PCI-related costs. More often, carriers limit their liability by providing small limits, only picking up certain portions of the exposure, providing defense only coverage, or only covering certain types of fines.

It is increasingly important to know the costs associated with payment card breaches and be sure to find the right Cyberliability insurance solutions that will cover your client in the event of a breach. Members of the AmWINS Financial Services Practice are available to help you find and understand the solutions available in the insurance marketplace.

This article was authored by Marc Lysse, an AmWINS Financial Services Practice Member in our Atlanta, GA office.