# SWETT ALERT
# October 14, 2014

## PCI Costs Coverage: What Insureds *Really* Need

As the barrage of data breaches reported in the press continues unabated, many executives are awakening to the risks a breach of their customer data poses to the financial health of their organizations. While their focus is often on the costs of notification and credit monitoring, a much overlooked liability is the financial risk arising from Payment Card Industry (PCI) fines, penalties or assessments.

Every organization, in order to process card transactions for payment, must sign a Merchant Services Agreement with either a merchant acquiring bank or a payment processor. This agreement contractually binds the organization to complete compliance with established Payment Card Industry Data Security Standards (PCI-DSS) established by the payment card brands at all times. Unfortunately, ongoing compliance is actually rare, as a firm's compliance may fluctuate from day to day. When a data breach involving payment card information occurs and the organization is found not to be PCI compliant at the time of the breach, the organization may be shocked to learn that the PCI contractual damages it has assumed in the Merchant Services Agreement may potentially equal or exceed any notification or credit monitoring expenses.

An organization often first learns of a data breach upon receipt from their merchant bank or a card brand of a Common Point of Purchase Report, which indicates that a certain amount of payment cards had incurred fraudulent charges after last being used legitimately at one common point: the organization in question may be contractually required to immediately hire a forensic firm or a PFI (PCI-Certified Forensic Investigator) to conduct a forensic investigation to determine the extent and scope of the compromise, if any, and to determine if the organization was PCI-DSS compliant at the time of the breach. The costs of the PFI can be extreme, quickly escalating into the six or seven figures range.

Upon a finding of non-compliance in any area of the PCI-DSS, the ramifications for an organization are grim. Depending on the circumstances of the breach and the size of the organization, fines can range up to $500,000. Moreover, in many cases, the payment card brands will also look to recoup operational expenses (including card reissuance costs) and counterfeit fraud recoveries incurred in connection with the event from the merchant bank if the number of cards affected exceeds the card brand's minimum threshold for assessments, which may range up to 15,000 cards in a single breach. The merchant bank will pass these costs downstream to the organization responsible for the breach. The sum of the operational expense and counterfeit fraud recoveries often amounts to a total assessment of $3 to $5 per affected card, though higher amounts are common. The organization's merchant bank often collects these assessments, fines and penalties by directly withholding a portion of the payment due to the organization from its routine settlement accounts at the bank until fully repaid. And while an appeal is possible, it also carries additional costs and is rarely

successful.

For a small organization, these costs could prove fatal to their financial health. And of course, failure to pay these amounts, or remediate the applicable PCI-DSS deficiencies can result in potentially the worst outcome of all: the inability for an organization to process credit and debit card payments, the lifeblood of most consumer facing organizations.

For those organizations choosing to purchase Cyber liability coverage, not all insurers offer PCI coverage but for those that do, the PCI coverage offered can vary significantly. Some insurers offer coverage for PCI fines or penalties only via a sublimit. Others recognize the significant PCI exposure beyond fines and penalties and are now expanding coverage to include fraud assessments, card reissuance costs, case management fees and PFI investigation expense at either full policy limits or via a sublimit. However, it is important to note that the organization must be able to attest in writing that they are PCI compliant at the time of applying for the coverage.

Please talk to your Swett & Crawford Professional Services Group broker for further information on this potential exposure to your company and any other questions you may have as it relates to securing or enhancing your Privacy and Network Security Liability coverage.

Thank you to Mark Smith, Director - Swett & Crawford's Professional Services Group for his expert insight. Mark has been an industry educator and resource for cutting edge iss ues such as cyber liability, leading Swett & Crawford's Cyber Liability specialty team. In this role, Mark has worked closely with carriers in drafting their cyber policies and has led dozens of cyber focused workshops for retail agents, their clients or industry groups on cyber issues.

Winner of the *Business Insurance* Readers' Choice Award for Best Insurance Wholesaler every year awarded since 2005