EPIC Insurance Brokers & Consultants

CLIENT ADVISORY

DEMYSTIFYING PCI DSS LIABILITY

YOU CAN OUTSOURCE CREDIT CARD PROCESSING BUT NOT LIABILITY!

Many business owners have misconceptions about their obligations and legal exposures if they experience a breach of payment card data. Outsourcing your company's payment card processing to a third-party does not mean you have also outsourced the risk you take on when you accept payments by credit card. Companies are still subject to the PCI DSS - Payment Card Industry Data Security Standards – and any failure to comply with PCI DSS will expose your company to a wide range of potentially significant liabilities in the event of a breach.

WHAT IS PCI DSS?

Created by the five payment brands (American Express, Discover Financial Services, JCB International, Mastercard, and Visa, Inc.), PCI DSS stands for the Payment Card Industry Data Security Standards. While not de facto law, the Security Standards are technical requirements that govern the appropriate security posture for any entity who stores, processes, and/or transmits cardholder information.[1]

MERCHANT SERVICE AGREEMENTS

A Merchant Service Agreement is the contract between a company that wishes to accept credit cards as payment for services and an acquiring bank or other institution that sets forth the terms and conditions under which the company can accept and process payment card transactions. Using a Payment Processing company may simplify the point of sale process, but it does not absolve a retail merchant of the responsibilities assigned to it by the terms and conditions of its agreement. The card brands also allow issuing banks to opt out of their settlement process and allow direct action by the banks to the entity that was breached. If a retailer is found to be out of compliance with the PCI DSS guidelines, they can face fines and penalties by the credit card companies in addition to the normal costs of responding to a breach.

DON'T MAKE ASSUMPTIONS WHEN IT COMES TO LIABILITY...

Check your contracts!
Check your policy!

COVERAGE SOLUTIONS

A comprehensive cyber insurance product provides coverage for fines, penalties, or assessments imposed by a Merchant Service Agreement against an insured company in the event of noncompliance with Payment Card Security Standards in connection with a data breach. Forensic costs, customer notifications and costs of credit monitoring for affected consumers are examples of other 1st party benefits of a cyber policy. Some policies will now even respond for the costs of chargebacks and fraud recoveries from bank institutions.

According to the FBI, it's not a question of "if" a company will be hacked, but "when". Cyber Insurance can be a key tool for a company in responding to and surviving a breach. Call us today to place coverage or review your current policy!

Additional Resources:

PCI Security Standards Association - Self Assessment: https://www.pcisecuritystandards.org/pci_security/completing_self_assessment
American Express – Are You PCI Compliant? https://www.americanexpress.com/en-us/business/trends-and-insights/articles/are-you-pci-compliant-1/
[1] https://thompsonburton.com/cybersecurity-law/2018/05/10/misperception-around-risk-liability-outsourcing-payment-processing/