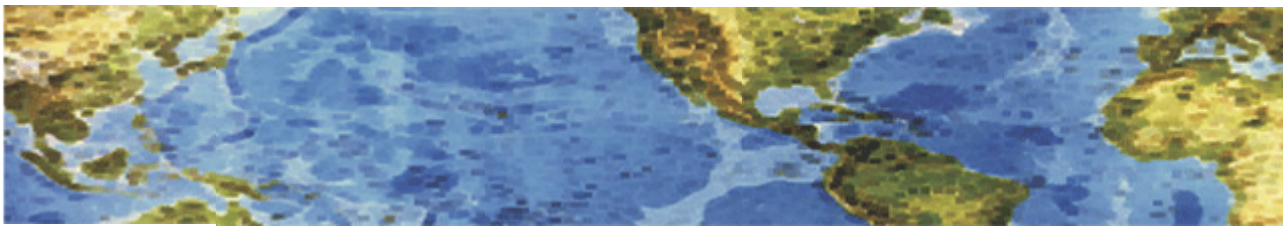
HALL ASSOCIATES



Risk-Based Decision Making Commentary
16 Oct 2013 Newsletter

Helping Companies Understand The Risks of Handling Credit Cards

These days, the vast majority of businesses selling goods and services are dependent on being able to accept credit cards as the primary form of payment, whether on location, online, or even over the phone. Few, however, seem to realize that the processing of thousands, sometimes millions, of customer credit card records carries a range of different financial risks, one of which is compliance with the Merchant Services Agreement, a contract at the heart of being able to accept credit payments.

This certainly appears to have been the case with Cicero's, a small restaurant located in Park City, Utah. Cicero's has sued its bank and the affiliated payment processor alleging, amongst other things, that they failed to inform Cicero's of its obligations under a merchant agreement to accept credit card payments. (Cicero's Inc. vs. Elavon Inc., Third Judicial District Court, Summit County, Utah) According to the complaint, Cicero's incurred claims against them exceeding $90,000 as well as other significant costs due to a potential breach of payment card information from its computer system. The good news is, by better understanding loss exposures associated with payment card information, a merchant's general obligations under common Merchant Services Agreements, and insurance options available, insurance agents and brokers can assist their clients to fully understand and manage the risks associated with handling credit cards.

Determining Payment Card Exposures

To help a client determine the severity of a credit card exposure, the agent or broker needs to assess how the merchant processes credit card transactions and also review the exact terms of the Merchant Services Agreement. Many small merchants may simply swipe the credit card through a special electronic box. The "swipe box" will capture and transmit the card information to the payment processor, but will not retain the card information. The card information gets transmitted directly to the processor via a direct telecommunications line. Because the information is not retained to the merchant's computer system, merchants using this type of system generally have a low exposure to the risks of losing payment card information.

Payment card exposures, however, are highest for merchants that process credit card transactions directly through a Point of Sale (POS) system. Typically, this is the case when the merchant swipes the payment card via a reader directly affixed to the POS system which stores the card information on the merchant's computer systems. Many merchants mistakenly believe that because a POS system encrypts card information as the card is swiped, or because the POS system is certified as "PCI Compliant," there is little to no exposure to loss.

Unfortunately, hackers have been able to circumvent these protections and Merchant Service Agreements do not protect the merchant in these cases. Payment card exposures are also significant for online merchants that process credit card payments directly on their websites, and possibly even retain the information in their computer systems to facilitate easy ordering for future orders.

The Merchant Services Agreement

Clearly, there is a range of ways a merchant can process credit card information, which will dictate the merchant's level of exposure to loss. Because there are so many different ways of handling credit card transactions, the best way to determine a client's exact exposure to loss is to examine their obligations under a Merchant Services Agreement. The Merchant Services Agreement is not based on obligations imposed by statutory or common law, but through obligations imposed under contract. Most notably, the Merchant Services Agreement requires the merchant to maintain compliance with the Payment Card Industry Data Security Standards (PCI DSS), as well as accept certain obligations in the event of payment card information breach. The PCI DSS is a set of standards promulgated by the Payment Card Industry Security Standards Council composed of all the major credit card brands. The extent of a merchant's responsibility to demonstrate compliance with the PCI DSS is based on the number of transactions that a merchant handles annually.

Specifically, merchants handling less than six million transactions a year are generally required to complete a Self-Assessment Questionnaire (SAQ). Merchants handling more than six million transactions a year are required to supply a Report on Compliance (ROC) from an approved IT-security expert. Most merchants are also required to obtain a quarterly network scan of their computers systems from an approved provider. In addition to demonstrating compliance with PCI DSS, the Merchant Services Agreement will place obligations on the merchant when a payment card company suspects that the merchant is a source of a breach. If suspected to be the source of a breach, the merchant is often required to obtain a computer forensic audit (at the merchant's expense) from a forensic auditor that has been approved by the PCI Security Standards Council. If the forensic auditor finds that the merchant is the source of a breach, the merchant may be held accountable for fines and penalties (if not in compliance with PCI DSS standards) as well as for the costs incurred to re-issue cards to consumers. As demonstrated in the Cicero's case, these costs and assessments may be substantial.

Risk Management

Once an assessment of a merchant's payment card exposures has been completed, good risk management requires implementation of appropriate risk controls as well as appropriate risk financing techniques. Note that no set of risk controls can guarantee that a loss will not occur. As such, the company should consider the use of insurance, or other risk financing techniques, to finance recovery from a loss that cannot be prevented. Careful adherence to the PCI DSS will provide a basic level of risk control, but insurance may be needed for higher exposures. Companies often fail to recognize the significant risks they carry when accepting credit card payments. This is especially true when they don't understand or properly comply with Merchant Service Agreements.

http://www.insurancejournal.com/magazines/features/2013/09/09/303861.htm?goback=.gde_4387290_member_5794770072438329348#!

http://www.zdnet.com/blog/security/targeted-spear-phishing-attacks/1032