Washington on the Verge of Enacting PCI Bill

March 16, 2010

Earlier this month, the Senate and House of Representatives in Washington passed a new PCI bill, HB 1149. The bill now awaits the Governor's signature but, if signed into law, will provide financial institutions with a cause of action against businesses or payment processors that fail to take reasonable care to guard against unauthorized access to account information where that failure is found to be the proximate cause of the breach. This new cause of action in Washington is similar to the existing statute in Minnesota and shows that payment card industry data security standards ("PCI DSS") compliance continues to be codified on a state by state basis. If the bill is signed, the law will go into effect July 1, 2010.

Under the bill, account information is defined as: (i) the full, unencrypted magnetic stripe of a credit card or debit card; (ii) the full, unencrypted account information contained on an identification device (an "identification device" is defined as an item that uses radio frequency identification technology or facial recognition technology"); or (iii) the unencrypted primary account number on a credit card or debit card or identification device in combination with an unencrypted cardholder name, expiration date, or service code. The bill also provides that a processor or business suffering a data breach of its account information may now be liable to a financial institution for "reimbursement of reasonable actual costs related to the reissuance of credit and debit cards" incurred by the financial institution as part of efforts to mitigate current or future damages to its cardholders.

Notably, the bill exempts processors, businesses, and vendors from liability if the account information was encrypted at the time of the breach or if the business was "certified compliant with the payment card industry data security standards" in effect at the time of the breach. A business is considered compliant if its PCI DSS compliance was validated by an annual security assessment conducted no more than one year prior to the breach. If signed into law, the bill will represent another incentive for companies to become PCI DSS compliant and another area of potential liability in the absence of such certification.