An Introduction To PCI DSS

January 20, 2016

The Payment Card Industry Data Security Standard is a contractual standard for the protection of data regarding payment cards issued by the major card brands, including Visa, MasterCard and American Express.

The Payment Card Industry Data Security Standard ("PCI DSS") is a contractual standard for the protection of data regarding payment cards issued by the major card brands, including Visa, MasterCard and American Express. Organizations that accept payment card transactions or store, process or transmit payment card data are usually contractually obligated to comply with PCI DSS. Organizations that handle other kinds of protected or regulated data should consider PCI DSS to indicate a reasonable standard of care for data protection. Failure to comply with PCI DSS can result in serious adverse consequences, including financial assessments, liabilities and findings of regulatory non-compliance. Organizations should carefully consider procuring insurance coverage for PCI DSS non-compliance.

PCI DSS

PCI DSS provides a set of minimum technical and operational requirements to protect payment card data (e.g. cardholder name, account number and expiration date) against unauthorized access, use or disclosure. PCI DSS is comprised of 12 fundamental principles for the security of a cardholder data environment relating to network/system security, data protection, vulnerability management, access control, monitoring/testing and information security policies. PCI DSS provides details and guidance for each of those requirements and related testing procedures. Periodic validation of compliance is usually required, either through an independent audit or by submission of a self-assessment questionnaire.

Contractual Requirement and Legal Standard

Compliance with PCI DSS is required by the contracts governing participation in payment card systems, and applies to all organizations involved in payment card processing, including merchants who accept payment card transactions and service providers who store, process or transmit payment card data. Merchants are usually responsible for PCI DSS compliance by their service providers. PCI DSS has been recognized by Canadian Privacy Commissioners as an industry standard that

establishes certain minimum technological requirements for compliance with statutory obligations to safeguard personal information.

Consequences of Non-Compliance

Failure to comply with PCI DSS can result in serious adverse consequences, including contractual financial assessments (i.e. penalties) and liabilities for resulting financial harm (e.g. losses resulting from payment card fraud and mitigation costs). For example, The Aldo Group, a Canadian footwear retailer, was the victim of a cybercrime attack resulting in the theft of cardholder data that was used for subsequent fraudulent transactions with other merchants. MasterCard alleged that The Aldo Group failed to comply with PCI DSS, and as a consequence Moneris Solutions Corporation (the relevant payment card transaction processor) debited The Aldo Group's bank account for a US$4.9 million assessment for operational reimbursement and fraud recovery. The Aldo Group sued Moneris and MasterCard challenging the assessment and claiming repayment. The litigation was discontinued after a number of procedural hearings (including unsuccessful challenges to the jurisdiction of Ontario courts), presumably as part of a settlement.

Failure to comply with PCI DSS can result in adverse regulatory findings. For example, the Privacy Commissioner of Canada and the Privacy Commissioner of Alberta found that TJX Companies and Winners Merchant International breached their statutory obligation to use appropriate security safeguards to protect personal information, in part because they had not used the wireless access encryption protocol required by PCI DSS.

Insurance

Organizations that are required to comply with PCI DSS should carefully consider procuring special insurance coverage for PCI DSS non-compliance. Standard commercial insurance may limit or exclude coverage for losses and liabilities resulting from PCI DSS non-compliance. For example, when The Aldo Group asked its liability insurer to cover the financial assessment imposed by Moneris, the insurer refused on various grounds, including a policy exclusion for "contractual liability" and an argument that The Aldo Group's acceptance of the Moneris payment card processing agreement breached prohibitions in the insurance policy. The Québec Superior Court agreed with the insurer's position and dismissed The Aldo Group's claim for insurance coverage. The dispute is now before the Québec Court of Appeal.

Comment

PCI DSS compliance does not eliminate cyber risk and might not satisfy all legal obligations to protect payment card data and other kinds of protected or regulated information. There are reported instances of organizations that have been certified PCI DSS compliant but have nevertheless been victims of cybersecurity breaches. Accordingly, organizations that are certified to be PCI DSS compliant should continue to be vigilant and take appropriate measures to manage cyber risk.

By

Bradley Freedman

Expertise

Cybersecurity, Privacy & Data Protection, Technology

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749