FEBRUARY 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Regulatory Enforcement Action Emphasizes Need for an Information Security Governance Framework

Recent enforcement action by the Canadian and Australian Privacy Commissioners and the United States Federal Trade Commission provides important guidance for compliance with personal information protection laws. Most importantly, organizations must establish an information security governance framework to ensure that appropriate practices, systems and procedures for the protection of personal information are established, consistently understood and effectively implemented.

Regulatory Enforcement Action – Ashley Madison Data Breach

In 2015, the Ashley Madison discrete affair website operated by Avid Life Media ("ALM") was subject to a cyber-attack by hackers who published the details (including sensitive personal information) of approximately 36 million Ashley Madison user accounts. The data breach was jointly investigated by the Canadian and Australian Privacy Commissioners and resulted in lawsuits by the United States Federal Trade Commission (FTC) and a number of U.S. states.

In August 2016, the Privacy Commissioners issued a joint report setting out findings that ALM had committed numerous breaches of the Canadian *Personal Information Protection and Electronic Documents Act* and the *Australian Privacy Act 1988* and published settlement agreements between ALM and the Privacy Commissioners. In December 2016, the FTC announced that ALM had agreed to settle the FTC and state lawsuits by making a $1.6 million settlement payment and agreeing to a stipulated order. The joint report, settlement agreements and stipulated order provide important guidance for compliance with personal information protection laws.

Privacy Commissioners' Joint Report

Canadian personal information protection laws require organizations to protect the security, confidentiality and integrity of the personal information they hold by using security safeguards (i.e. technological, physical and organizational measures) appropriate to the sensitivity of the information based on a meaningful, context-based assessment of financial, reputational and other risks likely to result from a data security breach.

The Privacy Commissioners' joint report states that the "most broadly applicable lesson" arising from the Ashley Madison data breach is that "it is crucial for organizations that hold personal information electronically to adopt clear and appropriate processes, procedures and systems to handle information security risks, supported by adequate expertise (internal or external)". The joint report further states that it is not sufficient for any organization that holds large amounts of personal information of a sensitive nature to address information security without "an adequate and coherent governance framework".

The joint report emphasizes that a documented information security governance framework is necessary to ensure that information security risks are properly managed through appropriate processes, procedures and systems that are consistently understood and effectively implemented. The joint report explains that an information security governance framework should include: (1) documented information security policies, procedures and practices; (2) an explicit risk management process (e.g. documented periodic and pro-active assessments of privacy threats, and evaluations of security practices to ensure that security arrangements are, and remain, fit for purpose); and (3) adequate privacy and security training for all staff (including senior management).

ALM's settlement agreements with the Privacy Commissioners require ALM to establish, document and implement an appropriate information security framework and information security practices. For more information about the Privacy Commissioners' joint report, see BLG bulletin *Ashley Madison Security Breach: Lessons Learned and Valuable Recommendations for all Businesses*.

FTC/State Lawsuits

The FTC and state lawsuits against ALM were settled based on a stipulated order that requires ALM to establish, implement and maintain a comprehensive, fully documented information security program, including appropriate administrative, technical and physical safeguards reasonably designed to protect the security, confidentiality and integrity of personal information held by ALM. The mandated program must include the following:

- The designation of an employee to coordinate and be responsible for ALM's information security program.
- The identification and assessment of internal and external risks to the security, confidentiality and integrity of personal information in each area of ALM's operations (e.g. employee training and management, information systems and prevention, detection and response to data security incidents) and the assessment of the sufficiency of existing safeguards to control those risks.
- The design and implementation of reasonable safeguards to control identified risks, and regular testing and monitoring of the effectiveness of those safeguards.
- The development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from ALM, and requiring the service providers to implement and maintain appropriate personal information safeguards.
- The periodic evaluation and adjustment of the information security program in light of the results of regular testing and monitoring, material changes to ALM's operations or business arrangements or any other relevant known circumstance.

The stipulated order also requires ALM to engage an independent, qualified third party to conduct periodic assessments of ALM's information security program for the next twenty years.

Comment

A documented, appropriate information security governance framework will not only help an organization comply with personal information protection laws, but it will also help an organization and its directors and officers comply with other legal duties and obligations regarding risk management and the protection of regulated, protected and sensitive information. For more information regarding some of those legal duties and obligations, see BLG bulletins *Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents*; *Regulatory Guidance from the Canadian Securities Administrators*; *Cybersecurity Guidance from Investment Industry Organization*; *PCI DSS Requirements for Incident Response Plan*; *Data Incident Notification Obligations*; *Guidance for Corporate Directors* and *Cyber-Risk Management Guidance from Financial Institution Regulators*.

Privacy commissioners, regulators and industry organizations have issued helpful guidance for establishing an information security governance framework based on accepted industry standards and best practices. For example: *Interpretation Bulletin: Safeguards*; *Interpretation Bulletin: Accountability*; *Getting Accountability Right with a Privacy Management Program*; *Privacy Toolkit for Businesses – A Guide for Businesses and Organizations*; *Securing Personal Information: A Self-Assessment Tool for Organizations*; *Protecting Personal Information: A Guide for Business*; *Start with Security – A Guide for Business*; *The NIST Cybersecurity Framework and the FTC*; *OSFI Cyber Security Self-Assessment Guidance*; *IIROC Cybersecurity Best Practices Guide*; and *CSA Staff Notice 11-332 Cyber Security*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG Cybersecurity Group – Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Kevin L. LaRoche	Ottawa	613.787.3516
David Madsen	Calgary	403.232.9612
Ira Nishisato	Toronto	416.367.6349

For more information about cyber risk management and BLG's related legal services, please see the BLG website.

BLG Vancouver
1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com