JANUARY 2018

CYBERSECURITY BULLETIN

Borden Ladner Gervais

VTech Data Breach Enforcement Actions – Guidance for Data Security and Privacy Law Compliance

The January 2018 resolution and settlement of VTech data breach enforcement actions by the Privacy Commissioner of Canada and the United States Federal Trade Commission provide important guidance for data security and compliance with personal information protection laws. Most importantly, organizations should establish a comprehensive information security management framework.

The Data Security Breach

VTech is a global provider of Internet-connected, electronic learning products for children and related online services and child-directed apps, games and other content. In November 2015, a hacker gained access to VTech's computer environments and data. The hacker initially accessed one environment using a well-known, commonly exploited security vulnerability known as "SQL injection". The hacker then used various methods to gain access privileges, move between several environments, and access and exfiltrate customer data. VTech could not identify the data affected, and therefore assumed that all data in the compromised environments could have been accessed or copied.

The compromised data included information collected by VTech from children and their parents using VTech products and other devices, including parents' account information (e.g. name, email address, password, secret question/answer and history of device purchases), information about children (e.g. name, gender, birthdate, photos and voice recordings) and chat messages between parents and their children. The breach affected over 500,000 Canadians and over 5 million Americans.

VTech issued a news release and reported the breach to the Privacy Commissioner of Canada. The hacker explained his reasons for the attack to Vice.com. The hacker was arrested, and the accessed data recovered from his devices. There was no indication that the hacker disclosed the data to anyone other than a news reporter.

In response to a complaint by an affected VTech customer, the Privacy Commissioner of Canada commenced an investigation to assess VTech's compliance with the Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA). The United States Federal Trade Commission ("FTC") commenced a lawsuit against VTech for alleged violations of the U.S. *Children's Online Privacy Protection Act* (COPPA) and the *Federal Trade Commission Act*.

On January 8, 2018, the Privacy Commissioner announced that he had completed the investigation and issued a Report of Findings that VTech had failed to adopt adequate security measures to protect sensitive personal information collected from its customers (including children), but had since remedied identified security deficiencies. On the same day, the FTC announced that VTech had settled the FTC lawsuit by way of a Stipulated Order that requires, among other things, VTech to pay a $650,000 civil penalty and implement a comprehensive data security program. The Report of Findings and Stipulated Order provide important guidance for compliance with personal information protection obligations.

Privacy Commissioner's Report

The Privacy Commissioner's Report explains that PIPEDA requires organizations to protect the security, confidentiality and integrity of the personal information they hold by using security safeguards (i.e. physical, organizational and technological measures) appropriate to the sensitivity of the information and other circumstances (e.g. the amount, distribution and format of the information and the method of storage).

The Report notes that VTech held extensive, highly sensitive personal information that could be used for purposes of phishing or identity theft, and significant personal information of children that could be used to create rich individual profiles for potentially malicious activity. The Report finds that, given the sensitivity of the information under VTech's control and the number of individuals (including children) affected, VTech was required to use heightened safeguards to protect the information. The Report concludes that VTech did not implement adequate safeguards to protect customers' personal information. The Report identifies the following deficiencies in VTech's information security practices:

- **Testing/Maintenance:** VTech did not have a program of regular testing and maintenance to identify and mitigate system vulnerabilities.
- **Administrative Access Controls:** VTech did not have adequate administrative access controls to limit administrative account access to authorized individuals who require it and to limit access rights and privileges to those required for each user's role.
- **Cryptography:** VTech did not use adequate cryptography to protect sensitive information. Information was stored or transmitted without cryptographic protection, password cryptography was inadequate, and decryption keys were not adequately protected.
- **Logging/Monitoring:** VTech did not have a regular monitoring and logging program to detect and mitigate potential threats.
- **Information Security Management Framework:** VTech did not have a comprehensive information security management framework, including a program of regular training, compliance monitoring, risk assessment and policy review, to ensure adequate personal information protection.

The Report explains that the Privacy Commissioner considered the complaint to be resolved because, after the breach was discovered, VTech implemented measures to address the deficiencies in its information security practices, including by implementing a comprehensive data security policy that provides for the creation of a data security governance board to ensure, among other things: (1) staff awareness regarding the policy and data security; (2) policy compliance; and (3) annual risk assessments, best-practice benchmarking and reviews so that the policy and associated data security measures remain adequate. The Report notes that VTech's settlement of the FTC lawsuit requires VTech to implement a comprehensive data security program that is subject to ongoing audits to ensure its continued adequacy.

FTC Lawsuit Settlement

The FTC lawsuit was settled based on a Stipulated Order that requires, among other things, VTech establish, implement and maintain a comprehensive, fully documented information security program designed to protect the security, confidentiality and integrity of personal information collected directly or indirectly by VTech. The mandated program must include administrative, technical, and physical safeguards appropriate to VTech's size and complexity, the nature and scope of VTech's activities and the sensitivity of the personal information, including the following components:

- **Responsibility:** The designation of an employee to coordinate and be responsible for VTech's information security program.
- **Risk Assessment:** The identification and assessment of internal and external risks to the security, confidentiality or integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction or other compromise of the information, and the assessment of the sufficiency of existing safeguards (e.g. employee training and management, information systems and information handling practices, and the prevention, detection and response to attacks, intrusions or other system failures) to control those risks in each area of relevant operations.
- **Safeguards:** The design and implementation of reasonable safeguards to control identified risks, and regular testing or monitoring of the effectiveness of those safeguards.
- **Service Providers:** The development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information received from VTech, and requiring (by contract) service providers to implement and maintain appropriate safeguards.
- **Evaluation:** The periodic evaluation and adjustment of the information security program in light of the results of required testing and monitoring, changes to VTech's operations or business arrangements or any other relevant known circumstance.

The Stipulated Order also requires VTech to engage an independent, qualified professional to conduct periodic assessments of VTech's information security program for the next twenty years, and to satisfy other compliance verification requirements.

Comment

The information security practices detailed in the Privacy Commissioner's Report and the FTC's Stipulated Order are consistent with cyber risk management guidance previously issued by privacy commissioners, regulators and self-regulatory organizations, and with information security practices detailed in regulatory reports and lawsuit settlements relating to other data security breaches.

Organizations and their directors and officers should take note of VTech's commitment to establish and maintain a comprehensive information security management framework. A documented framework is a fundamental and necessary data security practice because it helps ensure that security risks are properly managed through appropriate processes, procedures and systems that are consistently understood and effectively implemented. In addition, a framework can help an organization and its directors and officers comply with other legal duties regarding risk management and the protection of regulated, protected and sensitive information.

For more information, see BLG bulletins: *Regulatory Enforcement Action Emphasizes Need for an Information Security Governance Framework*; *Cybersecurity Guidance from Canadian Securities Administrators*; *Cyber Risk Management Guidance for Corporate Directors*; *G7 Cybersecurity Guidelines for the Financial Sector*; *G-7 Guidelines for Cybersecurity Assessment*; *Settlement of Uber Privacy/Data Security Complaint – Cybersecurity Guidance*; *Settlement of Walmart Canada Photo Centre Data Breach Lawsuits – Lessons Learned*. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity Law Group assists clients with legal advice to help manage cyber risks and to respond to data security incidents. Information about BLG's Cybersecurity Law Group is available at blg.com/cybersecurity.

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

Borden Ladner Gervais

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900
Montréal, QC, Canada H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide St W, Suite 3400, Toronto, ON, Canada M5H 4E3
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com