JANUARY 2019

CYBERSECURITY BULLETIN

Borden Ladner Gervais

OSFI Issues Advisory on Technology and Cybersecurity Incident Reporting

On January 24, 2019, the Office of the Superintendent of Financial Institutions (OSFI) issued an *Advisory* setting out OSFI's expectations for federally regulated financial institutions regarding the prompt (within 72 hours) reporting of "high or critical severity" technology and cybersecurity incidents. The Advisory will be effective on March 31, 2019.

OSFI and Cybersecurity

OSFI is an independent Canadian federal government agency that regulates and supervises federally regulated financial institutions (FRFIs), including all banks in Canada and all federally incorporated or registered trust and loan companies, insurance companies, cooperative credit associations, fraternal benefit societies and private pension plans subject to federal oversight.

Over the past few years, OSFI has emphasized the importance of cybersecurity and issued guidance to help FRFIs implement appropriate policies and practices to manage cyber risks and effectively respond to cyber incidents. OSFI's *Cyber Security Self-Assessment Guidance* (2013) explains that a FRFI's senior management should regularly review the FRFI's cyber risk management policies and practices to ensure that they remain appropriate and effective in light of changing circumstances and risks, and that a FRFI's board of directors (or board committee) should regularly review and discuss the FRFI's cyber risk management practices. The Guidance includes a detailed questionnaire focusing on six key issues: (1) organization and resources; (2) cyber risk and control assessment; (3) situational awareness; (4) threat and vulnerability risk management; (5) cybersecurity incident management; and (6) cybersecurity governance. For more information, see the BLG bulletins *Regulatory Guidance for Cyber Risk Self-Assessment* (2013) and *Cyber-Risk Management Guidance from Financial Institution Regulators* (2015).

OSFI's *2018-19 Departmental Plan* explains that OSFI intends to re-examine "OSFI's role in, and approach to, enhancing cyber security at Canadian financial institutions" and to assess its options for "overseeing the management of cyber risk by financial institutions".

The Advisory

OSFI's *Advisory on Technology and Cyber Security Incident Reporting* applies to all FRFIs, and sets out OSFI's expectations for FRFIs regarding the reporting of "Technology and Cyber Security Incidents" affecting FRFI operations. The Advisory will be effective on March 31, 2019, and will supersede all prior instructions from OSFI for technology and cybersecurity incident reporting. The Advisory does not supersede OSFI's *Cyber Security Self-Assessment Guidance*.

Key Definition – Technology or Cyber Security Incident

The Advisory defines "Technology or Cyber Security Incident" as an incident that has "the potential to, or has been assessed to, materially impact the normal operations of a FRFI, including confidentiality, integrity or availability of its systems and information". The Advisory explains that "materiality" should be defined by the FRFI in its "incident management framework", which are a required set of policies/procedures detailed in OSFI's *Cyber Security Self-Assessment Guidance*. The Advisory explains that a FRFI should consult its OSFI Lead Supervisor if the FRFI is in doubt about the materiality of an incident.

Criteria for Reporting

The reporting requirements set out in the Advisory apply to Technology or Cyber Security Incidents assessed by a FRFI to be of a "high or critical severity level". The Advisory does not define "high or critical severity", but explains that a reportable incident may have any of the following characteristics:

- Significant operational impact to key/critical information systems or data.
- Material impact to FRFI operational or customer data, including confidentiality, integrity or availability of such data.

- Significant operational impact to internal users that is material to customers or business operations.
- Significant levels of system/service disruptions.
- Extended disruptions to critical business systems/operations.
- Number of external customers impacted is significant or growing.
- Negative reputational impact is imminent (e.g. public/media disclosure).
- Material impact to critical deadlines/obligations in financial market settlement or payment systems.
- Significant impact to a third party deemed material to the FRFI.
- Material consequences to other FRFIs or the Canadian financial system.
- A FRFI incident has been reported to the Office of the Privacy Commissioner or local/foreign regulatory authorities.

The Advisory provides examples of reportable incidents – cyber attack, service availability incident, third-party breach and extortion threat, each with actual or potential material impacts on the FRFI or its customers.

Initial Reporting Requirements

A FRFI must submit an initial written report to both its OSFI Lead Supervisor and OSFI's Technology Risk Division (by email) as promptly as possible, but no later than 72 hours after determining that a Technology or Cyber Security Incident must be reported.

The initial report must include detailed information (specified in the Advisory) about the incident, to the extent the information is known or best estimated, including: a description of the incident and its impacts (including privacy and financial) on the FRFI, its clients and third parties; the current status of the incident; the date for internal incident escalation to senior management or the board of directors; actions taken or planned to mitigate the incident; the known or suspected root cause of the incident; and the name and contact information for the FRFI incident executive lead and liaison with OSFI.

Subsequent Reporting Requirements

OSFI expects FRFIs to provide subsequent updates on a regular basis (e.g. daily) as new information becomes available and until all relevant details about the incident have been provided to OSFI. OSFI may request that a FRFI change the method and frequency of the updates. OSFI also expects FRFIs to provide situation updates, including short-term and long-term remediation actions and plans, until the incident is contained/resolved. In addition, after incident containment, recovery and closure, OSFI expects the FRFI to report on the FRFI's post-incident review and lessons learned.

Comment – Preparing For Compliance

The incident reporting obligations set out in the Advisory apply in a much wider range of circumstances than breach reporting and notification obligations under Canadian personal information protection laws, due to the broad definition of "Technology or Cyber Security Incident". The Advisory indicates that an incident may be reportable if the incident has been reported to the Office of the Privacy Commissioner.

The incident reporting obligations set out in the Advisory are similar to the cybersecurity incident reporting obligations for Canadian investment dealers proposed (but not yet finalized) by the Investment Industry Regulatory Organization of Canada. See BLG bulletin *Canadian Investment Industry Regulator Proposes Mandatory Cybersecurity Incident Reporting*.

The Advisory will soon come into force. Consequently, FRFIs should now begin assessing and improving their systems, policies and procedures, and designating and training required personnel (both internal employees and external advisors), so that they are able to promptly submit incident reports in compliance with the Advisory. Following are some suggestions:

- **Cybersecurity Maturity:** A FRFI should use OSFI's *Cyber Security Self-Assessment Guidance* to assess the FRFI's current cybersecurity maturity (including the status of the FRFI's "Cyber Security Framework") and implement an appropriate plan for required improvement.
- **Incident Management Framework:** A FRFI should ensure that it has an appropriate incident management framework so that each potential Technology and Cyber Security Incident is immediately escalated to designated and properly trained personnel for investigation, assessment and response in accordance with a written incident response plan that is consistent with applicable legal requirements, regulatory guidance and relevant best practices, including the guidance in OSFI's *Cyber Security Self-Assessment Guidance*. For more information, see BLG bulletins *Cyber Incident Response Plans – Test, Train and Exercise* and *Data Security Incident Response Plans – Some Practical Suggestions*.

- **Policies/Procedures – Reporting to OSFI:** A FRFI should have written policies and procedures so that designated and trained personnel make and document informed assessments (i.e. materiality and impact) and decisions about reporting Technology and Cyber Security Incidents to OSFI in accordance with the Advisory.
- **Legal Privilege:** A FRFI should have an appropriate legal privilege strategy to help avoid inadvertent and unnecessary disclosures of privileged legal advice regarding Technology and Cyber Security Incidents, or inadvertent waiver of legal privilege. For more information, see BLG bulletins *Cyber Risk Management – Legal Privilege Strategy (Part 1)*, *Cyber Risk Management – Legal Privilege Strategy (Part 2)*, *Legal Privilege for Data Security Incident Investigation Reports*, and *Loss of Legal Privilege over Cyberattack Investigation Report*.
- **Contracts with Third Parties:** A FRFI should ensure that its contracts with relevant third parties (e.g. information technology and data processing service providers, including cloud service providers) contain appropriate provisions so that the FRFI is able to comply with the incident reporting obligations set out in the Advisory.
- **Other Reporting, Notification and Disclosure Obligations:** A FRFI should be mindful of its other legal obligations to report, notify and disclose Technology and Cyber Security Incidents imposed by statute (including personal information protection laws and securities laws), contract and common law and civil law. For more information, see BLG bulletins *Data Incident Notification Obligations*, *Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents*, *Preparing for Compliance with Canadian Personal Information Security Breach Obligations* and *Privacy Commissioner's Guidance for Compliance with PIPEDA's Breach of Security Safeguards Obligations*. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

François Joli-Coeur
T 514.954.3144
fjolicoeur@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

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