Cassels

Mandatory Breach Notification Under PIPEDA: Clock Is Ticking For Companies Without Security Breach Response Plans

Marco Ciarlariello, Bernice Karn

April 19, 2018

In 2015, Parliament enacted the *Digital Privacy Act* (the "Act"), a statute that provides for certain amendments to the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). However, not all provisions of the Act came into force in 2015; the enactment of certain sections of the Act that would create a new Division 1.1 to PIPEDA to deal with mandatory breach notification and record keeping obligations in respect of security breaches was delayed, pending the development of regulations prescribing the process for breach notification (the "Regulations"). On April 18, 2018, these Regulations were published in final form and on November 1, 2018, both Division 1.1 of PIPEDA and the Regulations will come into force.

Under the new provisions, each organization will be required to keep and maintain a record of “every breach of security safeguards involving personal information under its control.”[1] Where there has been a breach and the organization believes that a real risk of significant harm to individuals exists, then under these new provisions, the organization must notify: (i) the individuals affected, (ii) the federal Office of the Privacy Commissioner of Canada (the "Commissioner"), and (iii) in some cases, other organizations such as government institutions, if such a notification could reduce or mitigate the harm caused by the breach. “Significant harm” has a broad definition and includes “bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.”[2] The new provisions outline three factors that are relevant in determining whether a breach creates a real risk of significant harm: (a) the sensitivity of the personal information involved in the breach; (b) the probability that the personal information has been, is being or will be misused; and (c) any other “prescribed factor” (i.e., as established by regulation).[3]

The final Regulations are substantially the same as the draft Regulations released for public consultation on September 2, 2017 (please see our original commentary on the draft Regulations here). Compared to the draft Regulations, the final Regulations fine-tuned language relating to content, form and manner of breach reports to the Commissioner and the notifications that organizations must make. The final Regulations also provide for organizations to submit additional information to supplement a breach report already provided to the Commissioner, but do not consider a report to the Commissioner as a form of record an organization may use to fulfill its record-keeping obligations under Division 1.1.

Notifications must be made “as soon as feasible after the organization determines that the breach has occurred.”[4] The Regulations allow for notifications to be made directly (e.g., by email or phone call to individuals) or indirectly (e.g., through public communication such as publishing a notice on an organization’s website) to affected individuals. Indirect notification is suitable in circumstances where: (i) direct notification would be likely to cause further harm, (ii) the cost of direct notification would be likely to cause undue hardship, or (iii) the organization does not have contact information for the affected individual.

Each notification must contain information that allows “the individual to understand why the breach is significant to them and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm” along with any other prescribed information.[5] Per the new Regulations, prescribed information includes the requirement to provide specific details about the breach such as when it occurred, what personal information was affected, and contact information that an affected individual may use to obtain further information about the breach. The steps that individuals may take to reduce harm will depend on the nature of the breach, but these measures could include obtaining a new social insurance (SIN) or driver’s license number.[6] For example, if a breach involved consumer credit card information, an organization might suggest that affected individuals cancel the credit cards affected by the breach in order to mitigate the potential for identity theft or misuse of their payment cards.

In light of current events such as the Facebook and Cambridge-Analytica scandal, the announcement of the new security breach provisions and corresponding Regulations coming into force is timely. While these amendments to PIPEDA provide some guidance on how to respond to privacy breaches, it remains to be seen how organizations will practically apply concepts such as the factors for notification when assessing whether a breach poses a “real risk of significant harm.”

Privacy advocates have been calling on the government to enact these provisions since the Act received royal assent in 2015.[7] As noted above, the data breach reporting Regulations will come into force at the same time as the security breach provisions later this year. The delay has been and is, in part, serving as advance notice and providing organizations the time to implement processes, written policies and systems for monitoring, tracking and reporting data breaches.[8] For organizations that have used this time to develop the necessary policies and procedures for breach response, their hard work is finally paying off. But for those who have yet to do so, the deadline is now clear – November 1st, 2018.

For a full copy of the Regulations and the Government’s Regulatory Impact Analysis Statement, please click here.

For more information, please contact the authors of this article or any member of our Information Technology & Data Privacy Law Group.

The authors of this article gratefully acknowledge the contributions of articling student Tegan O’Brien.

[1] *Personal Information Protection and Electronic Documents Act* SC 2000, c 5 Division 1.1 at 10.3(1).
[2] *Personal Information Protection and Electronic Documents Act* SC 2000, c 5 Division 1.1 at 10.1(7).
[3] *Personal Information Protection and Electronic Documents Act* SC 2000, c 5 Division 1.1 at 10.1(8).
[4] *Personal Information Protection and Electronic Documents Act* SC 2000, c 5 Division 1.1 at 10.2(2).
[5] *Personal Information Protection and Electronic Documents Act* SC 2000, c 5 Division 1.1 at 10.1(4).
[6] Office of the Privacy Commissioner of Canada, "Key Steps for Organizations in Responding to Privacy Breaches", available at https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gl_070801_02/
[7] Amanda Connolly, "Companies will now have to tell Canadian consumers when their privacy is breached – and do it quickly", available at https://globalnews.ca/news/4122202/data-breach-canada-privacy-commissioner/
[8] Breach of Security Safeguards Regulations: SOR/2018-64, C Gaz Vol. 152, No. 8, available at <http://gazette.gc.ca/rp-pr/p2/2018/2018-04-18/html/sor-dors64-eng.html> ; the same comment was made in the Regulatory Impact Analysis Statement accompanying the draft Regulations released for public consultation in 2017, C Gaz Vol. 151, No. 35 available at <http://www.gazette.gc.ca/rp-pr/p1/2017/2017-09-02/html/reg1-eng.html>.