REPORTING AND RECORDING BREACHES OF SECURITY SAFEGUARDS – THE OPC RELEASES NEW RESOURCES FOR BUSINESSES

Posted on September 28, 2020

Categories: Insights, Publications

Earlier this month, the Office of the Privacy Commissioner of Canada ("**OPC**") released a number of new resources to assist organizations with their breach assessment, reporting and recording obligations under the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"). These include:

1. A series of videos that businesses can use to introduce their personnel to breach basics.

2. The OPC's final report regarding its first round of breach record inspections (the "OPC Report").

3. A secure portal for reporting breaches.

Each of these developments is discussed further below.

Video Series

The OPC has created a series of six (6) videos related to breaches of security safeguards pursuant to PIPEDA. The topics include:

- Introduction to breach reporting
- Assessing the risks of significant harm
- Business obligations for reporting breaches
- How to submit a breach report
- When and how to notify people and organizations
- Keeping the necessary records

Each video is only a few minutes long, and covers some basic principles related to breach requirements pursuant to PIPEDA. Accordingly, these videos will likely be most helpful to persons who have little or no familiarity with the relevant PIPEDA requirements.

The OPC's Final Report on 2019 Breach record inspections

The OPC Report sets out findings and recommendations from the OPC's first pro-active inspection of the breach records that businesses are required to keep pursuant to PIPEDA. More particularly, Section 10.3 of PIPEDA provides that: "[a]n organization shall, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control" (emphasis added), and pursuant to the Regulations, such report must:

- contain information that enables the OPC to verify compliance with the organization's breach reporting and notification obligations; and
- be kept for a minimum of 24 months.

The OPC concentrated its first assessment of compliance with these breach recording obligations on seven Canadian telecommunications companies (the "**Telecoms**"), and it inspected 237 sample records kept by the Telecoms.

The OPC's has published its detailed report of its findings on its website.

Key findings

Generally, the OPC found that the Telecoms appeared to take their PIPEDA obligations seriously. However, certain key issues were identified in the OPC Report, including:

- **Insufficient information for real risk of significant harm ("RROSH") assessment:** The OPC found that 40% of the sample breach records did not have sufficient information for the OPC to adequately assess whether a breach created a RROSH. In this regard, the OPC noted that if an organization intends to withhold part of a breach record on the basis of solicitor-client privilege, it must still ensure that the record provided to the OPC contains all of the information prescribed by PIPEDA.
- **Potential misapplication of RROSH test.** The OPC also found that 20% of sample records described breaches where the OPC did not agree that there was no RROSH, or had insufficient information for the OPC to determine whether a breach created a RROSH. Unfortunately, the OPC did not provide further details of the situations where it disagreed with the RROSH assessment, which could have provided organizations with helpful guidance regarding when the threshold has been met.
- **Human error is a significant cause of breaches.** The OPC found that 39% of breaches were caused by human error (whereas only 21% of breaches likely involved intentional, unauthorized disclosures). This finding demonstrates, once again, that training employees is critical to data security and breach prevention.

The OPC Report also provides four examples of breaches, with its assessment of whether they meet the RROSH test. These examples include common scenarios such as employee snooping, misdirected correspondence, a

lost laptop, and a SIM card swap. Unfortunately, the OPC did not consider ransomware attacks where the evidence suggests that data has been encrypted but not exfiltrated, which could have been helpful to a number of organizations given the recent rise in ransomware.

However, the OPC did provide a number of tips for assessing RROSH, including that organizations should obtain input from different members of its breach response team and also use a checklist or matrix that allows for a consistent assessment of all breaches. Importantly, the OPC stressed that, in every case, both the sensitivity of the information and the probability of misuse must be considered, and also addressed in the organization's breach records.

Finally, the OPC's Report contains a number of tips and suggestions, which organizations can take into account when designing or improving their breach program. In particular, the OPC urges organizations to take steps to improve their ability to identify and correct systemic issues or trends. This can include:

- Ensuring sufficient detail in breach records, and retaining such records for a sufficient period of time, to identify such issues;
- Considering blind spots that might indicate under-reporting within the organization;
- Sharing privacy and breach knowledge across different business lines, and also sharing breach experiences with other organizations in the same industry; and
- Engaging with executive and senior management who can contribute to embedding privacy within the culture and decision-making processes of the organization.

The OPC's Report provides some helpful insight into its position on breach reporting and recording obligations under PIPEDA.

Breach Reporting Portal

The OPC's new portal will allow businesses to submit their breach reports and associated documents, and instantly receive a file number to facilitate future communications with the OPC regarding the incident. To submit a breach report via the portal, the organization must first provide an email address, and then a link will be sent to that address to allow submission of the report.

Conclusion

Breaches remain one of the primary concerns for organizations in a variety of industries. The additional resources released by the OPC will be a welcome development to many businesses as they work toward building or improving their breach prevention and response frameworks.

However, for many organizations, a lot of questions remain unanswered. In particular, the threshold for

determining when a RROSH exists remains elusive. The four examples provided by the OPC provide some guidance, but a number of common scenarios are still unclear to many organizations. Furthermore, the suggestion that the OPC disagreed (or may have disagreed) with up to 20% of the decisions made by the Telecoms is concerning, particularly as it may signal that the OPC is interpreting the threshold for breach reporting as being relatively low.

by Lyndsay A. Wasser and Chiedza Museredza

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.