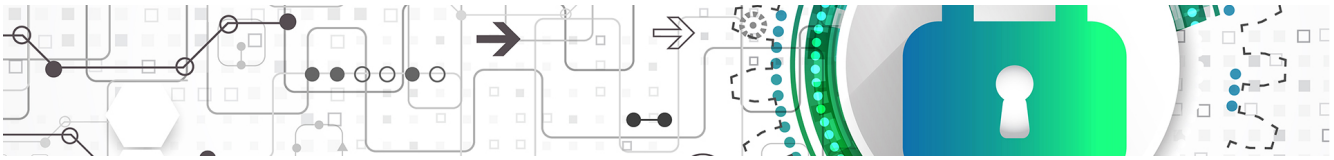

Oh, Hack! What to Do After a Breach: OPC Releases its Breach Guidance in Final Form

October 30, 2018

By Amanda Branch

The Office of the Privacy Commissioner of Canada (the "**OPC**") has released its breach guidance, "What you need to know about mandatory reporting of breaches of security safeguards", in final form (the "**Guidelines**"). In September, the OPC released draft guidance for consultation and invited interested parties to provide feedback. You can read our article here.

Most significantly, the Guidelines provided clarification on who is responsible for reporting a breach. The language in the draft guidelines left organizations concerned that the controlling organization and the service provider both had an obligation to report a breach to the OPC, which would be problematic in light of existing business arrangements and operational practices.

The Guidelines reiterate that the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") requires an organization to report a breach involving personal information under its control. PIPEDA's accountability principle provides that an organization remains responsible for the personal information it has transferred to a third party. Generally speaking, in a situation where a "principle organization" has transferred personal information to a third party for processing, and a breach occurs while the personal information is with the third party processor, it is reasonable to interpret the principle organization as having control over the personal information. The principle organization would be responsible for reporting that breach.

As the Guidelines note, business relationships can be very complex, and determining who has personal information "under its control" should be assessed on a case by case basis. Continuing the above example, the OPC states that if that third party processor is using or disclosing the same personal information for other purposes, it is no longer simply processing the personal information on behalf of another organization. In this context, it is acting as an organization "in control" of the information.

The Breach of Security Safeguard Regulations come in to force on November 1, 2018.