David Young Law
Compliance Bulletin

April 2019

OPC's Equifax Breach Report – Security guidance and new rules for cross-border transfers

On April 9, 2019 the federal Office of the Privacy Commissioner (OPC) published two documents with significance not only for guidance and compliance but also potentially suggesting a change in the settled law and understanding of requirements for outsourcing relationships and cross-border transfers of personal information.

Equifax breach report

Firstly, it released its *Report of Findings* regarding the 2017 Equifax Data breach[1]. This report reflects the clearly deep and focused investigation by the OPC into this significant incident. From a guidance perspective, it contains important and useful analysis of Equifax's existing security systems, the deficiencies in those systems and their missing elements – providing for the first time by the OPC detailed guidance as to the fundamentals of a security system that the OPC considers compliant with the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The report underlines that Equifax's database included significant items of financial and credit information of private individuals, which the OPC determined to be sensitive information.

The basic facts of the breach were as follows. In May, 2017 hackers gained access to the systems of Equifax Inc. (parent of Equifax Canada) through a software vulnerability of which Equifax had been notified two months prior. However Equifax only became aware of the attack at the end of July by which time the hackers had accessed payment and credit files for more than 143 million individuals worldwide, including Canadians. The credit information about Canadian residents had been provided by Equifax Canada to Equifax Inc., its U.S. parent, or collected directly by Equifax Inc. on behalf of Equifax Canada. It was determined that up to 100,000 data items of personal information involving approximately 19,000 Canadians were accessed.

Not until September 7 did Equifax make any public announcement or provide any notice that its systems had been accessed by the hacker and only on October 23 did it send letters notifying the affected Canadians.

The OPC undertook a detailed security review of Equifax's systems, separately for Equifax Canada and Equifax Inc., applying substantially the same principles in each case. A key aspect of the OPC investigation was the relationship between Equifax Canada and its U.S. parent and, importantly, the accountability obligations under PIPEDA for transfers of personal information between those two entities – including requirements for user disclosure and agreement to the transfer of data to the U.S. parent.

[1] *Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information, PIPEDA Report of Findings #2019-001*.

In addition to the security analysis, the OPC's report addresses Equifax's data retention and destruction policies as well as the steps it took to minimize the harm and warn its customers once the breach was known (its breach response actions).

Consultation on cross-border data transfers

The second significant publication released by the OPC on April 9 was a notice of a *Consultation on transborder dataflows*, which one can surmise was driven by its determinations regarding cross-border transfers of data made in connection with its Equifax investigation.

In its *Report of Findings*, the OPC concluded that the data of Canadian customers provided by Equifax Canada to Equifax Inc., or collected directly by Equifax Inc., was collected and processed by Equifax Inc. *on behalf of* Equifax Canada and that such transfer of information to the U.S. parent constituted *a disclosure* by Equifax Canada requiring customer consent, and that such consent had not been obtained.[2]

The consultation document, while indicating that the OPC is seeking input on the matter, clearly articulates the OPC's new view that all transfers of personal information to a processor require individual user consent. This view is a dramatic change from the OPC's previous interpretation of the law and if confirmed would entail significant complications and changes in organizations' privacy practices and their relationships with outsource service providers. Furthermore, it would be inconsistent not only with the accepted understanding of these relationships under PIPEDA but also under the provincial privacy laws across Canada, as well as with respect to how the European Union's *General Data Protection Regulation* (GDPR) treats such relationships. The OPC indicates that it is seeking stakeholder comment and input on this new policy position, to be received by June 4, 2019.

Analysis of Equifax's security systems

The OPC reviewed the security safeguards at both Equifax Canada and Equifax Inc. looking at what was in place at the time of the breach, identifying four key areas of concern. This security analysis provides important detailed guidance regarding the systems that the OPC considers sufficient to meet PIPEDA's Security Principle.

The OPC identified, and analyzed Equifax's compliance with, the following four key areas of security procedures:

(i) vulnerability management – preventing attacks through known vulnerabilities;
(ii) network segregation – reducing the scope of access and harm in the case of a breach;
(iii) implementation of basic information security practices – to be able to appropriately manage personal information uses and identify potential unauthorized uses;
(iv) oversight mechanisms – to accurately assess the risks faced, ensure that the security program is adequate to protect against these risks, and ensure that the program including relevant policies is implemented in practice.

[2] The OPC acknowledges that this is a new position relative to its previous findings and guidance.

The OPC determined that both Equifax Canada and Equifax Inc. had unacceptable deficiencies in each of these areas, with one exception.[3] With respect to oversight mechanisms within Equifax Canada, the OPC focused on two key areas: internal and external security assessments, and internal and external penetration testing, concluding in both cases that the mechanisms in place were inadequate.

Accountability for personal information transfers to Equifax Inc.

The OPC applied PIPEDA's Accountability Principle to determine whether Equifax was compliant with respect to the personal information of Canadians received by Equifax Inc. from Equifax Canada, or collected directly by Equifax Inc. Equifax had argued that this information was collected by Equifax Inc. on its own behalf, not on behalf of Equifax Canada, and therefore the Accountability Principle did not apply.

The OPC's analysis provides very useful guidance for determining whether a relationship between two organizations is one of third party processor, as opposed to independent collectors of personal information. The OPC looked at in particular relevant documentation provided to or available to customers, including website terms of use, corporate privacy policies, the means by which data was provided (e.g. the Equifax.ca website), and whether there was any written agreement between Equifax Canada and Equifax Inc. The focus of the analysis was to determine who had control over the information. In concluding that Equifax Canada had control, the OPC considered its continuous and prominent representations to customers that it, Equifax Canada, was providing the products in question (in particular, direct to consumer credit report information and fraud protection), and that the subject products were designed in effect to "facilitate access" for individuals to their information and what Equifax Canada was doing with this information.

Having made this determination, the OPC considered what accountability tools and controls should be in place for such a relationship - where a substantial volume of sensitive personal information belonging to a large number of individuals was handled over a prolonged period of time - and provides useful guidance as to what those controls should include. In this regard, the OPC outlines the minimum requirements for the processing agreement that should be in place between the two organizations, as well as the requirements for a structured program for monitoring compliance. It found that neither of these requirements had been met by Equifax. In addition, the OPC identified compliance gaps in Equifax's breach response procedures, its information management systems, its transparency regarding staff roles and responsibilities for personal information (such as the Privacy Officer), and its monitoring of compliance in the processing of its data by Equifax Inc.[4]

Consent for transfer of data to Equifax Inc.

As noted above, the OPC determined that Equifax Canada and Equifax Inc. were third parties in a data processing relationship, and that Equifax Canada was accountable for such processing under PIPEDA's Accountability Principle. However, having made this determination, the OPC then ruled that such transfers of data also constituted a *disclosure of personal information* under PIPEDA which therefore required consent by

[3] With respect to Equifax Canada, the OPC concluded that the network segregation concern identified at Equifax Inc. was not an issue.

[4] Noting, for example that reliance on tri-annual ISO 27001 certificates provided by Ernst & Young was insufficient when Equifax Canada was aware of other information casting doubt on security compliance.

Equifax customers.[5] The OPC in previous cases and guidance has characterized such transfers as a use by the controlling organization not requiring consent.[6] The OPC indicates in its report that it will be providing further guidance in relation to consent for such disclosures. In this regard, we could consider the consultation document published concurrently with the OPC's report as an initial articulation of such guidance.

The OPC found that no consent to such transfer was obtained and in any event the information provided to customers regarding such transfer was inadequate to validate any consent that might have been obtained.[7] The OPC also found that since the data in question was sensitive, express consent was required. Finally, the OPC concluded that Equifax provided inadequate information regarding a user's available options in the event that they do not consent.

Its analysis of Equifax's consent process provides useful guidance as to what the OPC considers necessary for such consent, in particular express consent where sensitive information is involved, including in contexts not specific to third party processing. However it may be noted that if this guidance were followed in all third party data processing/outsourcing relationships, the likely result would be cumbersome and lengthy disclosure documentation, almost impossible to execute effectively given the ubiquity of such relationships in the modern economy, and to an even greater extent in the digital context.

Summary

In its *Report of Findings* on the 2017 Equifax breach the OPC provides useful guidance regarding the extent and application of security controls that should be in place for an organization that processes large quantities of sensitive personal information, as well as for the protection of such data when transferred to a third party for processing. However, in its determinations regarding compliance, the OPC characterized such transfers as a disclosure under PIPEDA, requiring user consent, which was not obtained. This determination is at odds with the accepted treatment of such relationships, not only under PIPEDA but also under the provincial private sector privacy laws as well as under the GDPR. Likely conscious of this disparity, the OPC has undertaken a *Consultation on transborder dataflows*. The proper characterization of such transfers will have critical impact not only for cross-border transfers but for all third party data processing, particularly in the digital economy.

For more information please contact:
David Young 416-968-6286 david@davidyounglaw.ca

---

[5] Making reference to the meaning under s. 7(3) and the Consent Principle – mystifying since neither of these provisions contain a definition of disclosure. As noted above, the OPC acknowledged that this determination represented a departure from its previous view regarding such information transfers.

[6] See for example, *Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered, PIPEDA Case Summary #2007-365*; *Guidelines for Processing Personal Data Across Borders,* January 2009.

[7] The OPC acknowledged that Equifax Canada acted in good faith in not obtaining express consent to such transfers, in light of its previous guidance. It might be noted however that even if such transfers were not characterized as disclosures, consistent with the OPC's prior guidance, Equifax did not comply in that it failed to disclose that such transfers may take place.