CANADA (PIPEDA) BREACH NOTIFICATION REQUIREMENTS OVERVIEW

For Aptora Customers with Affected Canadian Residents (Outside Quebec)

Incident: DragonForce Cybersecurity Incident
Incident Date: June 22, 2026
Prepared By: Aptora Corporation

Purpose

This overview summarizes the requirements under the **Personal Information Protection and Electronic Documents Act (PIPEDA)** for organizations whose information was hosted by Aptora and whose databases may have been affected by the June 22, 2026 cybersecurity incident.

This document applies to Canadian organizations outside the Province of Quebec and is provided for informational purposes only. It is not legal advice.

Who Has the Notification Responsibility?

For customers using Aptora's hosted environment:

- **Aptora** generally acts as a technology service provider (data processor/service provider).
- **The customer** generally remains the organization responsible for the personal information (data controller) and is responsible for determining whether notification is required under PIPEDA.

Aptora's responsibilities include:

- Promptly notifying affected customers.
- Providing available technical information.
- Cooperating with customer investigations.
- Assisting customers in understanding what information may have been affected.

Information Potentially Involved

Depending upon your database, information may include:

- Names
- Addresses

- Email addresses
- Telephone numbers
- Dates of birth
- Social Insurance Numbers (if maintained)
- U.S. Social Security Numbers
- Banking information
- Payment card information
- Employee records
- Customer records
- Payroll information
- Tax information

Individual Notification

Under PIPEDA, organizations must notify affected individuals **as soon as feasible** if it is reasonable to believe the breach creates a **real risk of significant harm**.

Factors include:

- Sensitivity of the information.
- Probability the information will be misused.
- Nature of the threat actor.
- Evidence of unauthorized acquisition.

Given the facts of this incident, customers should carefully evaluate whether the threshold has been met.

Office of the Privacy Commissioner of Canada (OPC)

If there is a real risk of significant harm, organizations must generally notify:

- Office of the Privacy Commissioner of Canada
- Affected individuals

Organizations must also maintain breach records regardless of whether notification is ultimately required.

Identity Theft Protection

PIPEDA does not require organizations to provide free credit monitoring.

However, organizations should strongly consider recommending or offering identity theft protection where Social Insurance Numbers, financial information, or payment information may have been involved.

Recommended Consumer Guidance

Affected individuals should:

- Monitor financial accounts.
- Obtain credit reports from Equifax Canada and TransUnion Canada.
- Consider fraud alerts.
- Report suspicious activity immediately.
- Watch for phishing and identity theft attempts.

Customer Legal Review Checklist

☐ Canadian residents identified

☐ Real Risk of Significant Harm assessment completed

☐ OPC notification evaluated

☐ Individual notification evaluated

☐ Breach record retained

☐ Identity protection considered

This overview should be reviewed with qualified Canadian privacy counsel before notifications are issued.