Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Financière des Professionnels (Organization)
Decision number (file number)	P2022-ND-024 (File #021683)
Date notice received by OIPC	June 14, 2021
Date Organization last provided information	June 14, 2021
Date of decision	April 25, 2022
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization's head office is in Montreal, Quebec. The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported the incident involved some or all of the following information of some current and former clients and employees: • name, • social insurance number, • address, • email address, • date of birth, • passport number, • banking information (institution, branch number, transit), • chequing account number, credit card number), and • customer account number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On February 11, 2021, the Organization became aware of a business email compromise. • Two (2) employees of the Organization alerted it that some of their contacts had received a phishing email. • Eight (8) Microsoft Office 365 accounts were found to have been compromised. Phishing emails were sent from an Organization corporate email address to some of its clients. • The Organization reported there was no indication that its servers had been accessed. • On April 6, 2021, intrusion alerts were triggered. An unauthorized third party gained access and certain personal information may have been exfiltrated.
Affected individuals	The incident affected approximately 16,845 individuals, including 22 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Provided complimentary identity theft and credit monitoring solutions, free of charge for 60 months. • Retained cybersecurity firm to monitor the dark web to ensure that data potentially taken is not leaked to the public. • Notified Montreal police about the incident as well as relevant authorities. • Taking a number of additional measures to strengthen its systems, for example, implemented multi-factor authentication, implemented an audit logs retention policy, and installed software on the servers to enhance remote monitoring.
Steps taken to notify individuals of the incident	Affected individuals were notified by email or letter on May 31, 2021 and June 17, 2021.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported, *Some of the information may be usable to conduct identity theft, to conduct fraudulent banking activities, and for future phishing attempts.* In my view, a reasonable person would consider that the contact, identity, employment and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing

	the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported the likelihood that the harm will result is *"Low likelihood. We have not [sic] indication so far that the data is being misused*." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion into an employees' email account). The Organization confirmed that there was an unauthorized access to personal information.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.

In my view, a reasonable person would consider that the contact, identity, employment and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion into an employees' email account). The Organization confirmed that there was an unauthorized access to personal information.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email on March 16 and March 17, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance