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	Tyler J. Arnold Professional Corporation, operating as Arnold & Arnold, and P. David Arnold Professional Corporation, consultant for Arnold & Arnold (Organization)
Decision number (file number)	P2022-ND-042 (File #023990)
Date notice received by OIPC	November 22, 2021
Date Organization last provided information	November 22, 2021
Date of decision	June 7, 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 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: • client and other contact names, • email address, • phone numbers, • banking information, and • other confidential information that is typically exchanged between clients, suppliers, and law firms. 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 November 18, 2021, a staff's email was hacked. • The Organization's IT support advised that either the hacker was able to decipher the staff's email login and password or staff member clicked on a malicious email link.

	• The hacker sent approximately 250 emails with a virus link to contacts from the staff's account. • Some of the contacts called the Organization to report the fraudulent email they received.
Affected individuals	The incident affected approximately 250 individuals.
Steps taken to reduce risk of harm to individuals	• Notified the RCMP and the Law Society of Alberta among other entities.
Steps taken to notify individuals of the incident	The Organization notified contacts and other clients who have called or emailed the Organization about the fraudulent email received to not open the email with the virus. The notification provided by the Organization does not meet the requirements of section 19.1 of the PIPA Regulation.
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, *Clients and contacts that received the email and clicked on the virus link could have the same hack on their computers and Outlook and clients and contacts' information in emails could have been accessed by the hacker.* In my view, a reasonable person would consider that the contact, identity 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, *We have not received any complaints from clients or contacts that they have suffered harm. We are taking steps to protect our law firm's bank accounts based on the advice we have received from our banks.* 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).

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. A reasonable person would consider that the contact, identity 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). 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). **The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and is required to confirm to my Office, within ten (10) days of the date of this decision, that all affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.**

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance