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	Dixon & Associates (Organization)
Decision number (file number)	P2023-ND-018 (File #023963)
Date notice received by OIPC	November 10, 2021
Date Organization last provided information	May 11, 2023
Date of decision	September 11, 2023
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those 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 a law firm and an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • office documents, • copies of personal identification, and • banking documents. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 23, 2021 the Organization received a ransomware email. • The office staff discovered the breach when attempting to log on to computers.
Affected individuals	The Organization reported that the incident affected an unknown number of Albertans.

Steps taken to reduce risk of harm to individuals	• Shutdown of the existing system of electronic records and replaces by a restored and enhanced system of record keeping/electronic communications. • Updated and improved security.
Steps taken to notify individuals of the incident	Affected individuals were not notified.
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.	In its November 8, 2021 report to this office, the Organization reported the possible harms that may occur as a result of the breach is, "*possible disclosure of personal/private information*". In my view, a reasonable person would consider the contact, identity and the financial information at issue could be used to cause the significant harms of identity theft, fraud, embarrassment, hurt or humiliation.
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.	In its original Privacy Breach Report dated October 26, 2021, the Organization reported that the likelihood of harm that will result is "*Unknown*". In response to a follow-up email sent by this office to the Organization, the Organization reported, "*There has been absolutely no indication from anyone whatsoever of any further activity, positive or negative, since the event itself, and no further activity of any kind has been engaged in whatsoever."* In my view, a reasonable person would consider 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, ransom demand). The lack of reported incidents resulting from this breach to date is not a mitigating factor. Identity theft and fraud can occur months and even years after a data breach.
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. The contact, identity and the financial information at issue could be used to cause the significant harms of identity theft, fraud, embarrassment, hurt or humiliation. 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, ransom	

demand). The lack of reported incidents resulting from this breach to date is not a mitigating factor. Identity theft and fraud can occur months and even years after a data breach.

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).

Where contact information for affected individuals is readily available, the Organization is required to notify affected individuals in Alberta in accordance with section 19.1 of the Regulation. The Organization is required to confirm to my Office, within ten (10) days of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.

Where contact information for affected individuals is not readily available, I require the Organization to confirm to my Office in writing, within ten (10) days of the date of this decision, how it proposes to notify affected individuals indirectly, and confirm the affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.

Cara-Lynn Stelmack
Assistant Commissioner, Case Management