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	Nick Milkovich Architects Inc. (Organization)
Decision number (file number)	P2021-ND-327 (File #023189)
Date notice received by OIPC	September 22, 2021
Date Organization last provided information	September 22, 2021
Date of decision	March 9, 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 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 headquartered in Vancouver, British Columbia, and is 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: • name, • physical address, • email address, and • telephone number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On April 6, 2021, the Organization was subject to a ransomware attack. The incident was discovered on the same day when an employee found they were unable to access their computer.

	• The Organization did not report how the malicious actor gained unauthorized access to conduct the attack.
Affected individuals	The incident affected 52 Canadians, including 2 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Acted to ensure the attacker no longer had access to systems. • Investigated with the assistance of external IT experts. • Retained an IT consultant to monitor systems and recommend improvements. • Updated and / or upgraded hardware and software protecting systems and data. • Implemented multi-factor authentication. • Implemented ability to report suspicious emails. • Provided staff with cybersecurity training. • Notified law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by email, letter, or phone call on September 22, 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: *It is [the Organization's] assessment that the contact information could be used for the purposes of phishing, increasing the risk of identity theft and fraud.* *The specified harms noted above, assuming they occur, are significant.* I agree with the Organization's assessment. A reasonable person would consider that the contact information at issue, including email address, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are 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 Organization] is of the view that the likelihood that harm could result is low.* *While [the Organization] has no evidence confirming that the personal information at issue has been compromised or misused by the external actor, the personal information involved in the incident could nonetheless be used for the purposes identified above.*

	The fact that the incident was caused as a result of the actions of an unknown actor with malicious intent additionally increases the likelihood that harm could result. I agree with the Organization's assessment. 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 a third party (deliberate intrusion and deployment of ransomware). A lack of reported misuse does not mitigate against future harm as phishing, identity theft, and fraud can occur months or years after a 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.

A reasonable person would consider that the contact information at issue, including email address, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion and deployment of ransomware). A lack of reported misuse does not mitigate against future harm as phishing, identity theft, and fraud can occur months or years after a 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).

I understand the Organization notified affected individuals by email, letter, or phone call on September 22, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner