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	Communauto Inc. (Organization)
Decision number (file number)	P2021-ND-166 (File #019902)
Date notice received by OIPC	March 5, 2021
Date Organization last provided information	March 5, 2021
Date of decision	August 26, 2021
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 operates in Alberta 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, • date of birth, • civic address, • email address, • social insurance number, • driver's licence number, • banking information, • hiring contract, • collective assurance contract, and • member 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	• Between December 19 and 20, 2020, the Organization was victim to ransomware (Sodinokibi), resulting in the encryption of a significant number of servers and workstations. • It is reported that an administrative password was compromised as a result of phishing, and was subsequently used in the attack. • The Organization reports that the threat actor exfiltrated records from its servers. It is also stated that the attackers eventually destroyed the records they exfiltrated.
Affected individuals	The incident affected 9,950 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified police. • Established a crisis unit which included external cyber security experts and lawyers. • Disconnected impacted devices. • Closed VPN access. • Changed passwords for all employees on all enterprise systems. • Verified integrity of all servers. • Hired cyber security experts to propose improvements. • Rebuilt servers in a cloud environment. • Reviewed access and permissions. • Removed sensitive information from "reconstituted server spaces". • Revised policy on use of computer equipment. • Revised personal data retention and erasure policy. • Offered credit and identity theft protection to affected employees.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on December 22, 2020, January 8, 2021, and February 8, 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 the possible harms that might result from the breach as "Unsollicited [sic] emails, phishing, identity theft (expecially [sic] employees)". In my view, a reasonable person would consider that the contact, identity, financial, and employment information at issue could be used for the purposes of identity theft and fraud. Email addresses, particularly in combination with knowledge that the individual is a client of the Organization, 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: *We believe low the possibility that an [sic] harm could result as a consequence of the attack.* *a) Personal information about the majority of clients (email address) has low sensitivity* *b) To date we have no proof that personal data have been effectively exposed* *c) The limited number, size and especially the position of the few files (2 or 3 files for clients among several hundred of thousand) concerned in the archives make them difficult to find.* *d) [Received] confirmation that files downloaded were destroyed.* *e) A credit monitoring and identity theft protection have been provided to all actual and ancient employees.* In my view, the likelihood of harm is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion and deployment of ransomware). Although the Organization reports it has "no proof that personal data have been effectively exposed", the information was nonetheless exfiltrated. Further, although the Organization reports that the exfiltrated records were destroyed, it is not clear how reliable this assertion is, nor is it known if the attackers created copies of the records before destroying them.

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, financial, and employment information at issue could be used for the purposes of identity theft and fraud. Email addresses, particularly in combination with knowledge that the individual is a client of the Organization, 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 is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion and deployment of ransomware). Although the Organization reports it has "no proof that personal data have been effectively exposed", the information was nonetheless exfiltrated. Further, although the Organization reports that the exfiltrated records were destroyed, it is not clear how reliable this assertion is, nor is it known if the attackers created copies of the records before destroying them.

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 December 22, 2020, January 8, 2021, and February 8, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner