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	START Architecture Inc. (Organization)
Decision number (file number)	P2021-ND-219 (File #019470)
Date notice received by OIPC	February 16, 2021
Date Organization last provided information	February 16, 2021
Date of decision	November 8, 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 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: • social insurance number, • bank/financial account number / bank account number and bank name, bank account number, • routing number, • income / pay, salary, payment history (employee pay stub), • date of birth / date of birth (employee and employee dependants), • tax identification number and, • business number (BN) in Canada. 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 January 25, 2021, the Organization discovered suspicious activity from one of its email accounts. • The Organization determined that an employee with the Organization was a victim of a phishing attack that compromised their email mailbox login credentials. • Between January 14, 2021 and January 25, 2021, the perpetrator used the credentials to send further phishing emails from the impacted person's account.
Affected individuals	The incident affected 20 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Launched its response protocol and took immediate action to lock down the impacted account. • Alerting individuals who were sent phishing emails to prevent others from being victimized by the phishing scheme. • Offered employees free credit monitoring for a period of twelve (12) months. • Established two-factor authentication. • Provided Cyber Security information and will be providing a Cyber Security presentation with mandatory attendance required.
Steps taken to notify individuals of the incident	The affected individuals were notified by email on January 25, 2021 and by letter on February 16, 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 potential unauthorized disclosure of the personal information, as well as reputational harm to the organization as a result of a loss of confidence of the employees impacted.* In my view, a reasonable person would consider that the contact, identity, tax, employment and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.
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 that the likelihood that significant harm will result is "Possible, but not likely" and its notice to affected individuals said, "We want to stress that we are not aware of any misuse of this information." 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, phishing).

	The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. The personal information at issue may have been exposed for approximately two (2) weeks.

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, tax, employment and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. 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, phishing). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. The personal information at issue may have been exposed for approximately two (2) weeks.

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 the affected individuals by email on January 25, 2021 and by letter on February 16, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner