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	Pivot Technology Solutions Inc. (Organization)
Decision number (file number)	P2021-ND-023 (File #016502)
Date notice received by OIPC	July 22, 2020
Date Organization last provided information	July 22, 2020
Date of decision	February 23, 2021
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify the individual whose personal information was collected in Alberta.
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 incident involved all or some of the following information: • name, • address, • date of birth, • payroll information (including information with respect to deductions, RRSP, income withholdings, and benefits), • banking information (including routing and account number), • social insurance number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On June 12, 2020, the Organization became aware it was the victim of a cybersecurity attack. An unauthorized third party deployed ransomware in an attempt to encrypt the Organization's technology infrastructure. • Some of the Organization's employees experienced complications with email, however, there were no interruptions to its business operations. • On July 1, 2020, the Organization discovered that the unauthorized third party had in fact gained access to and exfiltrated the personal information of employees and independent contractors of the Organization's subsidiaries and affiliates resident in Canada including: TeraMach Technologies, Inc. and Pivot Acquisition Corp. • On July 7, 2020, the Organization determined what type of personal information of employees and independent contractors was compromised in the incident. • The Organization determined that the unauthorized user had access to its systems between June 9, 2020 and June 12, 2020.
Affected individuals	The incident affected 156 Canadians, including one (1) Alberta resident.
Steps taken to reduce risk of harm to individuals	• Conducted a detailed investigation and implemented an incident response plan, including investigating to determine the extent of breach, ensuring the external actor no longer had access to its systems. • Offered identity theft and credit monitoring services to the affected individuals for a period of 24 months. • Expedited the implementation process for Multifactor Authentication for all applications that are accessed remotely. • Implementing additional safeguards in accordance with the recommendations of the forensic firm. • Conducting a review of its security and cybersecurity measures to improve security safeguards. • Reviewing cybersecurity and privacy policies and procedures to ensure adequate data protection safeguards and security systems as well as measures to respond to potential breaches. • Notified data protection authorities. • Encouraged individuals to be vigilant and to take steps to protect themselves.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on July 23, 2020.

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, *… there are potential risks of identity theft, fraud and financial loss and embarrassment for the individual affected in Alberta...The personal information of the individual affected in Alberta involves financial and identification information that is sensitive, as it is possible that such information could be used to conduct the specified harms noted above.* I agree with the Organization's assessment. A reasonable person would consider the contact, identity, employment and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. Payroll information could also potentially be used to cause embarrassment. 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 likelihood that harm could result is moderate. While [the Organization] has no evidence that the personal information at issue has been misused by the external actor, the personal information involved in the incident is nonetheless sensitive and could be used for the purposes of identity theft and fraud. 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.* 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 and ransom demand). The Organization indicated the external actor "had in fact gained access to and exfiltrated the personal information of employees and independent contractors." The lack of evidence that the personal information at issue has been misused by the external actor to date is not a mitigating factor, as identity theft, fraud and financial loss can occur months and even years after a data breach. Further, the data may have been exposed for four (4) days.
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 the contact, identity, employment and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. Payroll information could also potentially be used to cause embarrassment. 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 an unknown third party (deliberate intrusion and ransom demand). The Organization indicated the external actor "had in fact gained access to and exfiltrated the personal information of employees and independent contractors." The lack of evidence that the personal information at issue has been misused by the external actor to date is not a mitigating factor, as identity theft, fraud and financial loss can occur months and even years after a data breach. Further, the data may have been exposed for four (4) days.

I require the Organization to notify the affected individual 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 letter on July 23, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner