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	Performive, Inc. (Organization)
Decision number (file number)	P2022-ND-041 (File #022846)
Date notice received by OIPC	August 17, 2021
Date Organization last provided information	August 17, 2021
Date of decision	May 19, 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 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 headquartered in Marietta, Georgia, USA. 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, *"Performive is a cloud service provider, hosting data and websites for various businesses... Some Performive clients elect to pay using personal credit cards. As a result, the Company collects certain personal information about the payor and their credit card information."* The incident involved the following information: • name, • address, • email address, and • credit card. 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. Some of the information appears to qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone

	number, business address, business e mail address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." Therefore, I find that the information that may be otherwise considered business contact, is personal information and PIPA applies to the extent that the personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or about June 14, 2021, the Organization identified unusual user activity on its network. • The Organization determined an unauthorized third party was able to access a portion of its network using a compromised SSH key. • The Organization disabled the compromised SSH key. • The Organization reported that the unauthorized activity occurred between June 3, 2021 and June 12, 2021. • Initially, the Organization believed only encrypted personal information had been accessed. • On or about July 2, 2021, the Organization discovered that the encryption keys were also compromised and that non-encrypted personal information had been compromised.
Affected individuals	The incident affected 489 individuals including 50 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Provided additional security training. • Implemented two-factor authentication, along with other security measures. • Provided two years of complimentary identity theft protection services to affected individuals. • Provided affected individuals with steps they could take to help protect their financial accounts. • Notified major credit card brands of the incident.

	• Continually evaluates and modifies practices and controls to enhance the security and privacy of personal information.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on August 18, 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 did not specifically provide an assessment of the likelihood that significant harm would result from this incident. However, in its notification to affected individuals, the Organization stated, *To protect you from potential misuse of your information, we are offering a complimentary two-year membership to TransUnion myTrueIdentity. This credit monitoring service will notify you by email of critical changes to your TransUnion Credit Report. This product is completely free to you, and activating these services will not hurt your credit score. For more information on identity theft prevention and TransUnion myTrueIdentity, including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter.* *This letter also provides other precautionary measures you can take to protect your personal information. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity regularly. If you detect any suspicious charges, contact your bank immediately.* *You may also wish to contact the bank that issued the credit card that you used with your Performive account to determine if the card can be cancelled and re-issued with a new number.* In my view, a reasonable person would consider that the contact and credit card information could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing 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	The Organization did not specifically provide an assessment of the likelihood that significant harm would result from this incident. 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). Although the

between the incident and the possible harm.	Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information were to be used for fraudulent purposes. Finally, the information may have been exposed for approximately 9 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 that the contact and credit card information could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing 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 an unknown third party (deliberate intrusion). Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information were to be used for fraudulent purposes. Finally, the information may have been exposed for approximately 9 days.

I require the Organization to notify the affected individuals whose 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 August 18, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance