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	Spreadshirt, Inc. (Organization)
Decision number (file number)	P2022-ND-040 (File #022848)
Date notice received by OIPC	August 19, 2021
Date Organization last provided information	August 19, 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 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's head office is in Greensburg, PA, USA. 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: • first name, • last name, • address, • phone number, • name of bank account holder, • bank account number, • bank name, and • bank routing number. 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. The Organization reported, *"We do not believe that...tax identification number was accessed. This data is stored in a part of our network that we believe the attacker was not able to reach."*

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Early in July 2021, the Organization discovered evidence of unauthorized access to employee computers. • The Organization concluded that a criminal deliberately targeted its network in an attempted ransomware attack. • The attacker did not succeed in encrypting the Organization's systems, however, the Organization believes that the attacker was able to access and copy data from its internal networks. • The attacker used a keylogger to acquire employee login credentials and certificates. • In turn, credentials and certificates allowed the attacker to access the Organization's VPN Gateway. • The Organization reported, *"We do not know exactly what information the attacker was able to copy from our networks."*
Affected individuals	The incident affected 10,248 individuals including 20 whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Hired an external cybersecurity expert to analyze its systems and assist the Organization to plan new security features. • Took remedial steps including but not limited to: - resetting all employee login credentials; - blocking potentially affected accounts; and - deactivating all gateways to its VPN;
Steps taken to notify individuals of the incident	Affected individuals were notified by email on July 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, "*It is possible to attempt ACH fraud using a person's bank account number."* In my view, a reasonable person would consider the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Since the Organization cannot identify the exact information the attacker was able to copy, it is not clear what other possible harms may exist.

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, *It is possible to target individual consumers for ACH fraud. However we do not know if this is likely and have no basis to draw a conclusion about this.* In my view, 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, attempted ransomware attack). The personal information may have been exposed for approximately 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 the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Since the Organization cannot identify the exact information the attacker was able to copy, it is not clear what other possible harms may exist.

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, attempted ransomware attack). The personal information may have been exposed for approximately 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 affected individuals by email on July 8, 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