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	YSS Corp. (Organization)
Decision number (file number)	P2021-ND-161 (File #018079)
Date notice received by OIPC	September 8, 2020
Date Organization last provided information	September 8, 2020
Date of decision	August 25, 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 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 incident involved all or some of the following information: • name, • address, • social insurance number, • date of birth, and • banking information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 15, 2020, the Organization was informed that on or about May 9 or 10, 2020, an unknown individual gained entry to the Organization's Head Office in Calgary.

	• The Organization determined that no paperwork, including personnel or payroll records, was missing and, accordingly, it initially believed that there was no loss of or unauthorized access to personal information. • On August 4, 2020, the local police service (CPS) contacted the Organization as a part of an ongoing investigation involving the Organization's branded inventory, and advised that CPS had recovered fake IDs (although not related to any of the Organization's employees) and fraudulent cheques. • The Organization is unable to determine whether information may have been accessed and/or copied by the individual or individuals who unlawfully accessed the office.
Affected individuals	The incident affected approximately 160 individuals.
Steps taken to reduce risk of harm to individuals	• Offered all potentially affected individuals one year of credit monitoring. • Rekeyed and activated a pass card entry system. • Requested that elevator access to the Head Office be locked, with enhanced security. • Digitizing all personnel files, with all paper copies being certified as shredded. • Enhanced security and engaged a new IT firm to enhance cyber security. • Cooperating with the local police service in its ongoing investigation.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on September 8, 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 that it… *… has no evidence of any actual or attempted use of any improperly accessed personal information. However, based on the information potentially accessed and/or taken, there is the potential for identity theft or fraud and negative effects on the potentially affected individuals' credit records.* I agree with the Organization's assessment. A reasonable person would consider the contact, identity, and financial information potentially at issue could be used to cause the harms of 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 that it … *… assesses the likelihood of harm resulting from the breach, assuming that personal information was accessed and/or copied, as high.* *…Moreover, CPS indicated that in the course of its investigation it recovered fake ID's and fraudulent cheques, believed to have been made using information obtained through similar unlawful access to other businesses. Accordingly, while there is no information regarding any actual improper use of personal information obtained from [the Organization's] Head Office, if personal information was taken or accessed, it is highly likely it could be used in a manner which would harm potentially affected individuals.* I agree with the Organization's assessment. A reasonable person would consider that the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in) and the Organization cannot rule out whether personal information was accessed or used improperly.

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, and financial information potentially at issue could be used to cause the harms of identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in) and the Organization cannot rule out whether personal information was accessed or used improperly.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individuals were notified by email on September 8, 2020. The Organization is not required to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner