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	Olson Curling Inc. (Organization)
Decision number (file number)	P2020-ND-172 (File #015781)
Date notice received by OIPC	May 8, 2020
Date Organization last provided information	May 27, 2020
Date of decision	December 3, 2020
Summary of decision	There is a real risk of significant harm to individuals affected by this incident. The Organization is required to notify the 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 Organization reported the incident involved the following: *1) 80% was internal corporate paperwork. 2) Customer/vendor mailing addresses. 2) Purchase transactions (customers and ours). 3) Deposit receipt slips (with backup photocopied cheques). 4) Credit card details for telephone orders (est. 40-50). 5) Blank cheques, packing slips and invoices for 2 companies. 6) Corporate bank and credit statements.* The Organization said that some of these documents may have included personal information such as: • name, • billing and shipping address, • email address (may include business email address), • product purchase details, • photocopied cheques (that may have business information on them), and • credit card details (a limited number of phone-in orders with full card details).

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of this information may also 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 theft of 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." As a result, PIPA applies to the business contact information. Much of the information at issue appears to be about corporations/businesses, however, and not individuals (e.g. Corporate bank and credit statements). This is not personal information as defined in PIPA, and the Act does not apply.
DESCRIPTION OF INCIDENT	
☒ loss	❑ unauthorized access ❑ unauthorized disclosure
Description of incident	• The Organization uses a third party service provider for document shredding and destruction services. • On April 24, 2020, thieves broke into and stole the service provider's truck, which contained the Organization's files. • The truck was recovered the same day. Some of the material that was in the truck was discarded and found in an alley in a new construction area not far from where the truck was stolen. • Material was recovered from that location and the area checked to ensure nothing remained. The service provider informed the Organization that it is confident most of the Organization's documents/files were recovered. The service provider destroyed the found boxes upon retrieval of the stolen truck. • The service provider advised that the police speculate the truck may have been stolen to use in the theft of goods and the contents of the truck were discarded for that purpose.

	• The Organization was informed of the incident on April 27, 2020 by the service provider, as well as another party whose information was also in the truck, and the police.
Affected individuals	The incident affected approximately 300 to 400 individuals.
Steps taken to reduce risk of harm to individuals	The Organization reported the service provider implemented or plans to implement the following new security measures: • Install dashcam and interior camera in truck. • Install truck alarm. • Hardwire truck with GPS tracking with geofencing alerts. • Upgrade padlocks. • Enhanced perimeter security cameras. • Working towards ISO 27001 Information and Data Security Certification.
Steps taken to notify individuals of the incident	The affected individuals were not notified of the incident.
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: *In our opinion, the potential harms should be very limited due to the age of the files (all 7+ years old). The higher harm possibility is what someone could do with full billing and shipping address details.* In my view, a reasonable person would consider that the contact, credit card and banking information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' 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 between the incident and the possible harm.	With respect to the likelihood of harm resulting from this incident, the Organization reported "… our believe (sic) is very minimal, if any." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (theft of vehicle with documents inside). The Organization can not be sure that all documents were recovered. Although the service provider reported that the "police speculate the truck may have been stolen to use in the theft of goods near the new construction area and the material was discarded to make room for those items", I do not find this to be reassuring. The

	police, the service provider and/or the Organization can only speculate as to the motives of the thief.

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, credit card and banking information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to 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 (theft of vehicle with documents inside). The Organization can not be sure that all documents were recovered. Although the service provider reported that the "police speculate the truck may have been stolen to use in the theft of goods near the new construction area and the material was discarded to make room for those items", I do not find this to be reassuring. The police, the service provider and/or the Organization can only speculate as to the motives of the thief.

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

Section 19.1(1) of the Regulation states that the notification must "… be given directly to the individual…", although section 19.1(2) says "… the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

For those documents that contained the individual's full credit card details, the Organization reported that notification would not be possible because, "Unfortunately this was the only form of information for these transactions and we have no electronic back-ups for any of these details on these few transactions (i.e. customer names, addresses, credit card details, etc.)."

I accept that direct notice is unreasonable where the Organization is not able to identify affected individuals or does not have contact information. **I require the Organization to confirm to my Office in writing, within ten (10) days of the date of this decision, how it proposes to notify affected individuals indirectly.**

Jill Clayton
Information and Privacy Commissioner