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	Paskapoo Pet Services (Organization)
Decision number (file number)	P2021-ND-153 (File #017143)
Date notice received by OIPC	August 12, 2020
Date Organization last provided information	August 12, 2020
Date of decision	June 8, 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 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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information of an Alberta resident: • name, • home address, • telephone number, • email address, • pet name, • door and alarm codes (about 20% clients), and • location of hidden keys (about 5% of clients). 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	• The Organization used a third party software called "Precise Pet Care" to store and archive Services Agreements and client information associated with the provision of a variety of pet care services (pet sitting, pet boarding, dog walking, etc.). • After a client's account is created, the primary documentation and signatures are stored in pdf files within each client's account for reference and recordkeeping. • On July 14, 2020, a security researcher discovered a vulnerability within the system that potentially allowed unauthorized access to the list of files and the files themselves. • The Organization's service provider advised that the vulnerability was remedied the same day, and a second fix was implemented on July 22, 2020. The service provider also confirmed that none of the vulnerable files were accessed by anyone other than the security researcher who initially discovered the vulnerability. • The Organization was made aware of the vulnerability incident on August 8, 2020.
Affected individuals	The incident affected 345 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Suggested potentially affected individuals change their door and alarm codes, and the location of hidden keys around their houses. • Terminating relationship with its current client management software. • Reviewing how to record door and alarm codes during meetings with clients in a way to prevent them from falling into the wrong hands. • Protected client management software with strong passwords at all time.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on August 11, 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 the possible harms that may occur as a result of the breach are: *Misuse of the information could result in the access to houses and properties by using door and alarm codes (when/if valid). There could be an increase of spam email, mail and/or phone calls.* I agree with the Organization's assessment. A reasonable person would consider that the contact information, along with information about door codes and key locations could be used to

	cause the harms of theft or property damage. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all 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: *With the investigation that revealed that the vulnerable files were not accessed by anyone else than the security expert, we considered the risks to be very low.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is decreased because it did not result from malicious intent or deliberate action, and the Organization reported that the security researcher who reported the breach is the only party that accessed the information. I do not find this completely reassuring, however, as the Organization does not know how long the information was exposed and it was accessed by an unauthorized third party.

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 information, along with information about door codes and key locations could be used to cause the harms of theft or property damage or theft. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is decreased because it did not result from malicious intent or deliberate action, and the Organization reported that the security researcher who reported the breach is the only party that accessed the information. I do not find this completely reassuring, however, as the Organization does not know how long the information was exposed and it was accessed by an unauthorized third party.

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 email on August 11, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner