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	Edmonton Humane Society (Organization)
Decision number (file number)	P2019-ND-023 (File #010741)
Date notice received by OIPC	November 20, 2018
Date Organization last provided information	November 20, 2018
Date of decision	February 15, 2019
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	Pursuant to section 56(2), PIPA "does not apply to a non-profit organization or any personal information that is in the custody of or under the control of a non-profit organization", except in the case of personal information that is collected, used or disclosed in connection with any commercial activity. "Non-profit organization" is defined in section 56(1) to mean an organization "that is incorporated under the *Societies Act* or the *Agricultural Societies Act* or that is registered under Part 9 of the *Companies Act*." In this case, the Organization is a registered non-profit organization under the *Societies Act*. The Organization operates an animal shelter and provides community programs and services related to animal welfare. The Organization reported the "personal information related to this breach was gathered from low income applicants in order to assess eligibility for a subsidized or free veterinary services program". In my view, this is information collected in connection with a commercial activity and therefore PIPA applies.

Section 1(1)(k) of PIPA "personal information"	The Organization reported that it "…is not aware of the full extent of the information that was disclosed. However, it is believed that the documents disclosed may have included T4s, tax assessments and returns, bank statements and pay stubs, which may have contained personal information including the clients' names, dates of birth, addresses, e-mail addresses, telephone numbers, Social Insurance Numbers (SINs), employment histories, income information, and banking and financial 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	• A technical malfunction in the Organization's website's server caused the server to randomly draw client information from a database and populate the website with the information. • For a period of time between October 2017 and February 2018, when one clicked on photos of animals on the website's adoption page, the website would show a PDF image of financial information provided by EHS clients. The website did not give access to the database of client information or the server that stored the client information. Rather, the website simply posted random images. • The problem was corrected on February 28, 2018 through a "patch" developed by the website's service provider. • The Organization became aware of the breach in January 2018 after it was directly brought to management's attention by two individuals whose information was disclosed. One of the individuals contacted the Organization because someone had taken a "screenshot" of the information on the website and posted it to social media. Another individual reported the incident to the RCMP, who then contacted the Organization.
Affected individuals	The Organization reported the incident affected 389 individuals.
Steps taken to reduce risk of harm to individuals	• Corrected the website issue and the technical malfunction. • Hired a new contractor for the website and website support, replaced the website, and the client information is now stored on a server that is not connected to the website. • Considering retaining an expert in cyber security to review the Organization's IT universe and undertake penetration testing of our IT firewalls.

	• Ensuring all staff that deal with personal information receive training and are made aware of their obligations pursuant to PIPA. • Reviewed and revised the Organization's Privacy Policy and forms to ensure that they are up to date and meet the requirements of PIPA.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent by Fedex on November 20, 2018
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 disclosure of sensitive financial information combined with personal identifying information has the potential to result in identity theft, financial loss, fraud, and negative effects on an individual's credit record". In my view, a reasonable person would consider that the sensitive contact, identity, financial, and employment information at issue could be used to cause the significant harms of identity theft and fraud, as well as phishing (leading to an increased risk of fraud or identity theft). The information could also be used to cause the significant harms of hurt, humiliation, and embarrassment.
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: *Assessing the likelihood that harm will result is somewhat difficult given that [the Organization] is not aware of the extent of the information that was posted online, nor the number or identity of all of the individuals whose information may have been viewed. Although there is the potential that all 389 individuals who provided information to [the Organization] under the PALS program could have been affected, at this time [the Organization] is only aware of five individuals whose information was actulally [sic] posted and reviewed. Unfortunately, [the Organization] is not able to determine whether any other individuals were affected, as the server was decommissioned and there is no longer any auditing capabilities available.* *Overall, the following factors suggest that there may not be a substantial likelihood of harm occurring:* *1) The website issue has been resolved since February 28, 2018, and the technical malfunction that led to the privacy breach no longer occurs;* *2) Any one piece of information would likely not have been posted to the website for a long period of time (since the server*

	refreshed the image every 30 minutes); 3) *There was no access to the server or compromise to [the Organization's] records. Rather, the only information exposed consisted of random PDF images posted by the website;* 4) *At this time, only five individuals have been identified as having their personal information disclosed on the website and who appear to have been potentially affected; and* 5) *[The Organization] is not aware of any impacts or harm experienced by these five individuals as a result of the website error.* In my view, despite the fact the incident did not result from malicious intent but rather a technical error, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was exposed for a period of approximately 5 months. The Organization does not know the extent of the information that was posted online, nor the number or identity of all of the individuals whose information may have been viewed. The Organization also reported that the personal information of at least one individual was further disclosed on social media.

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 sensitive contact, identity, financial, and employment information at issue could be used to cause the significant harms of identity theft and fraud, as well as phishing (leading to an increased risk of fraud or identity theft). The information could also be used to cause the significant harms of hurt, humiliation, and embarrassment.

Despite the fact the incident did not result from malicious intent but rather a technical error, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was exposed for a period of approximately 5 months. The Organization does not know the extent of the information that was posted online, nor the number or identity of all of the individuals whose information may have been viewed. The Organization also reported that the personal information of at least one individual was further disclosed on social media.

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 Organization notified affected individuals by letter sent by Fedex on November 20, 2018. The Organization is not required to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner