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	Fearless Faith Inc. (Organization)
Decision number (file number)	P2019-ND-071 (File #012210)
Date notice received by OIPC	February 28, 2019
Date Organization last provided information	February 28, 2019
Date of decision	June 3, 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 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 operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported that it "…is unable to determine what information the unauthorized third party may have accessed. For some affected individuals, the types of data potentially impacted include name, address, email, phone number, credit card information, and some service details, including a limited number of audio/visual recordings with clients. In a very few cases, the information included date of birth due to a service offering for which date of birth was relevant." 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 January 30, 2019, the Organization discovered that an unknown third party had obtained access to the Organization's Drop Box account.

	• The Organization investigated and determined that the unauthorized access may have begun on or about February 8, 2018.
Affected individuals	The Organization reported that it identified 26 Canadians whose credit card information may be been included in the information that was accessed, including 10 who are resident in Alberta.
Steps taken to reduce risk of harm to individuals	• Forced a password reset for access to the Drop Box account and implemented two-factor authentication. • Examined all files within the Drop Box account to identify individuals whose personal information has been affected. • Reviewing document retention practices to implement further controls for the safeguarding and destruction of personal information.
Steps taken to notify individuals of the incident	The 26 Canadian residents whose credit card information may have been compromised were notified on February 26, 2019 by email.
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 "…identified 26 Canadians (of which 10 are resident in Alberta) whose credit card may have been included in the information that may have been accessed. Of these individuals, the risks are somewhat lower for 11 Canadians whose credit cards had expired… [the Organization] has notified the individuals with expired credit cards on the basis that the OIPC would consider the combination of an unauthorized access and credit card information to increase the risk of phishing activity (even if there is no financial harm) given that the OIPC considers the risk of phishing to create a real risk of significant harm. However, [the Organization] has made these notifications without any admission that the test for notification for these individuals has been met". In my view, a reasonable person would consider that identity (date of birth) and financial information (credit card information) could be used to cause the significant harms of identity theft and fraud. It is not clear to me from the Organization's report of the incident whether the credit card information had expired before the time of the unauthorized access or before the Organization discovered the incident. Nonetheless, this information, even after expiry, could be used in combination with other personal information (such as service details) to cause significant harm. Email addresses could be used for phishing purposes, increasing 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 did not specifically assess the likelihood of harm resulting from this breach, other than to note that "the risks are somewhat lower" for individuals whose credit cards have expired and that the OIPC "… would consider the combination of an unauthorized access and credit card information to increase the risk of phishing activity". In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the incident is the result of malicious intent (deliberate action). The Organization did not report recovering the personal information. It appears the information may have been exposed for almost 11 months before the access was discovered.

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 identity (date of birth) and financial information (credit card information) could be used to cause the significant harms of identity theft and fraud. It is not clear to me from the Organization's report of the incident whether the credit card information had expired before the time of the unauthorized access or before the Organization discovered the incident. Nonetheless, this information, even after expiry, could be used in combination with other personal information (such as service details) to cause significant harm. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased as the incident is the result of malicious intent (deliberate action). The Organization did not report recovering the personal information. It appears the information may have been exposed for almost 11 months before the access was discovered.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, and includes identity (date of birth), financial (credit card information, whether or not expired) and/or email address, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

The Organization reported that it notified the 26 Canadian residents whose credit card information may have been compromised on February 26, 2019 by email. **However, I require the Organization to confirm to my office, in writing, within 10 days of the date of this decision, that it has notified affected individuals in accordance with this decision.**

Jill Clayton
Information and Privacy Commissioner