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	Fendrihan Ltd. (Organization)
Decision number (file number)	P2016-ND-16 (File #P2748)
Date notice received by OIPC	June 5, 2014
Date Organization last provided information	March 7, 2016
Date of decision	March 15, 2016
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 incorporated in Ontario and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • home address, • credit card number, • phone number, and • email address. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the information was collected in Alberta from Alberta residents.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure

Description of incident	The Organization's website was the target of a malware attack, resulting in unauthorized access to the personal information of customers of the Organization.
Affected individuals	Three (3) individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Vulnerability on server fixed and investigation launched. • Retained forensic IT consultant to assist with the investigation. • Offered one free year of credit monitoring services. • Notified Organization's payment processor. • Reported the incident to the Office of the Information and Privacy Commissioner of Alberta (OIPC).
Steps taken to notify individuals of the incident	Notification sent by mail on June 4, 2014.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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.	In its report to the OIPC, the Organization did not specifically assess the harm that could result from this incident. However, the notification sent to the affected individuals offered them credit monitoring services, which suggests possible identity theft, fraud and financial loss. In my view, the personal information involved is sensitive and could be used to cause the harms of identity theft, fraud and financial loss. 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.	In its report to the OIPC, the Organization did not specifically assess the likelihood of harm resulting from this incident. The notification sent to the affected individuals advised of "a breach that affected your personal information", without further information on the assessment of the likelihood of harm. In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent and the Organization confirmed the information at issue was stored on the compromised server and was accessed after the malware was installed.

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. The personal information involved is sensitive and could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent and the Organization confirmed the information at issue was stored on the compromised server. 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 the affected individuals in a letter dated June 4, 2014, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner