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	Identifix, Inc. (Organization)
Decision number (file number)	P2019-ND-008 (File #010753)
Date notice received by OIPC	November 21, 2018
Date Organization last provided information	November 21, 2018
Date of decision	February 4, 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 those individuals whose 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: • name, • mailing address, and • credit card number for two Canadian residents. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• An unauthorized individual sent an email to certain of the Organization's employees that contained an attachment through which the individual appears to have gained unauthorized access to the employees' email accounts.

	• The email accounts contained certain personal information about individuals who have transacted business with the Organization. • The Organization discovered the incident on October 24, 2018, after identifying unauthorized emails sent from an employee's email account. • The Organization's investigation found that an unauthorized user(s) gained access to two email accounts and, while there, could have accessed certain personally identifiable information stored in the accounts. • The breach occurred on September 21, 2018 and ended on October 2, 2018.
Affected individuals	The incident affected 11 individuals, including 2 Canadian residents.
Steps taken to reduce risk of harm to individuals	• Engaged a third party forensics firm and investigated. • Reset the access credentials of the compromised users. • Conducting additional employee training on phishing attempts. • Notifying potentially affected individuals about this incident and providing information and resources to help these individuals protect themselves. • Providing identity-theft monitoring to the affected individuals at no cost to the recipients.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent November 21, 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 "In some cases, information incidents that affect credit card numbers could potentially result in attempted identity theft or fraudulent transactions involving a card." I agree with the Organization's assessment. Financial information (credit card number) could be used to cause the significant harms of identity theft or fraud.
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 that "The information involved in this incident includes credit card numbers. The Commissioner has held credit card numbers to be highly sensitive. Out of an abundance of caution, [the Organization] is notifying potentially affected individuals about this incident. [The Organization] is providing information and resources (including identity-theft monitoring) to help these individuals protect themselves."

	The Organization also said that its "…investigation has not found any evidence that this incident involves any unauthorized access to or use of [the Organization's] internal computer systems or network" and that it "…is not aware of any fraud or misuse of information as a result of this incident." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the deliberate malicious action of an unknown third party (phishing) and unauthorized emails were sent.
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. Financial information (credit card number) could be used to cause the significant harms of identity theft or fraud. A reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the deliberate malicious action of an unknown third party (phishing) and unauthorized emails were sent. I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand affected individuals were notified by letter sent November 21, 2018. The Organization is not required to notify the affected individuals again.	

Jill Clayton
Information and Privacy Commissioner