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	TrueFire LLC (Organization)
Decision number (file number)	P2020-ND-041 (File #015631)
Date notice received by OIPC	April 6, 2020
Date Organization last provided information	April 6, 2020
Date of decision	April 20, 2020
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 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 all or some of the following information: • name, • address, • payment card account number, card expiry date, and security code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. In its report to my Office, the Organization said that it "…does not accept that the privacy breach reporting provisions of the Personal Information Protection Act, 2003 C. P- 6.5 are applicable in this matter". It is not clear to me why the Organization says this. However, in my view, given the Organization is an "organization" as defined in PIPA, and the information at issue qualifies as "personal information" as defined in PIPA, PIPA applies to the extent the information was collected in Alberta.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 10, 2020, the Organization discovered that an unauthorized person gained access to its computer system and website (TrueFire.com). • The Organization reported that "… it appears that the unauthorized person could have accessed the data of consumers who made payment card purchases while that data was being entered on the Website, between August 3, 2019 and January 14, 2020."
Affected individuals	The incident affected 70 Albertans.
Steps taken to reduce risk of harm to individuals	• Working with computer forensic specialists to determine the full nature and scope of the incident and reporting the incident to law enforcement. • Monitoring all activity on the website and working with an outside computer forensic team to monitor, remediate and identify any issues. • Reported breach to the federal privacy commissioner.
Steps taken to notify individuals of the incident	The Organization reported that it "notified the 70 individuals directly by mail [on April 6, 2020]. In the notification letter, [the Organization] provided information about steps that the 70 individuals can take to protect themselves".
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 did not specifically identify the possible harm(s) that might result to individuals affected by this incident. In my view, a reasonable person would consider the financial information at issue could be used to cause the significant harms of identity theft and 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 did not specifically assess the likelihood of harm resulting from this incident but said it "…has no evidence that the unauthorized person has misused any of the information". In my view, the likelihood of harm resulting from this incident is increased because the personal information was apparently compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information may have

	been exposed for more than five months. The lack of "evidence" of misuse of the information does not mitigate against the possibility of future use of the information to cause the harms of identity theft and/or fraud.

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 the financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was apparently compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information may have been exposed for more than five months. The lack of "evidence" of misuse of the information does not mitigate against the possibility of future use of the information to cause the harms of identity theft and/or fraud.

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).

The Organization reported that it "…notified the 70 individuals directly by mail [on April 6, 2020]. In the notification letter, [the Organization] provided information about steps that the 70 individuals can take to protect themselves". The Organization did not provide a copy of its notification to affected individuals so my Office has not been able to confirm whether the notice complies with the requirements set out in the Regulation.

The Organization is required to confirm to my Office in writing, within 10 days of the date of this decision, that its notification to the individuals whose personal information was collected in Alberta complied with section 19.1 of the Regulation.

Jill Clayton
Information and Privacy Commissioner