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	Sprott Money Ltd. (Organization)
Decision number (file number)	P2020-ND-030 (File #014072)
Date notice received by OIPC	December 4, 2019
Date Organization last provided information	December 11, 2019
Date of decision	March 4, 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, • mailing address, • telephone number, • email address, and • credit card number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• The Organization's website Sprottmoney.com was compromised as a result of malicious code uploaded by an unauthorized third party.

	• The breach occurred on November 1, 2019 and was discovered on November 7, 2019.
Affected individuals	The incident affected 17 individuals.
Steps taken to reduce risk of harm to individuals	• Removed the script. • Informed individuals to check credit cards for suspicious activity and recommended replacement of existing credit cards with a new number. • Will provide 12 months of identity theft and credit monitoring free of charge. • Updating security patches, login passwords, and system upgrades to prevent this from happening again. • Launching a new website with enhanced cloud server technology.
Steps taken to notify individuals of the incident	Affected individuals were notified in writing on December 11, 2019.
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 there is "Potential for Credit Card information to be compromised." In my view, a reasonable person would consider the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. In addition email address could be used for phishing purposes, increasing vulnerability to 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 reported that "With this type of hack, there is some chance that the hacker obtained personal information of a small number of customers." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action, malicious code). The information appears to have been exposed for 6 days.
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 contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. In addition email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action, malicious code). The information appears to have been exposed for 6 days.

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 the Organization notified affected individuals in writing on December 11, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner