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	Primevest Equities Inc. (Organization)
Decision number (file number)	P2019-ND-151 (File #006270)
Date notice received by OIPC	August 16, 2017
Date Organization last provided information	June 6, 2018
Date of decision	August 21, 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 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, • social insurance number, and • credit card number. 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 July 28, 2017, the Organization was not able to access its file server. Later the same day, the Organization received an email saying that hackers had copied the Organization's data and were demanding a ransom or the information would be released.

	• The Organization disconnected the compromised server and contacted law enforcement. • The file server contained mostly templates but did not contain client or employee data. • The Organization reported "The concern would be if they also hacked into any of the other computers on the same network as the file server, as one of them contains (encrypted) client credit card data, as well as client credit applications, and staff payroll information. To date, there is no evidence of this, and in fact the hackers believe they are hacking an entirely different company…".
Affected individuals	The incident affected 9 individuals.
Steps taken to reduce risk of harm to individuals	• Shutdown the server and contacted law enforcement. • Changed all passwords. • Confirmed no viruses, ransomware or otherwise on the system. • Advised affected individuals on how to monitor their credit for free and advised of credit monitoring services. • Changed IT service providers.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally and by letter on July 31, 2017.
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 "Should the hackers have breached other PC's on the network, potential for identiy [sic] theft, financial loss/ fraud." In my view, a reasonable person would consider the contact, identity and financial information potentially at risk 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 reported that "There is no evidence at this time that any of the other computers were involved in the breach." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, ransom demand). Although the Organization reported "there is no evidence" that other networked computers were compromised, it did not provide any evidence, such as audit logs, to support this conclusion, nor its belief that the hackers were trying to hack different company.

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, identity and financial information potentially at risk 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 compromised due to the malicious action of an unknown third party (deliberate intrusion, ransom demand). Although the Organization reported "there is no evidence" that other networked computers were compromised, it did not provide any evidence, such as audit logs, to support this conclusion, nor its belief that the hackers were trying to hack different company. I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals verbally and by letter dated July 31, 2017, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.	

Jill Clayton
Information and Privacy Commissioner