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	Primerica Financial Services (Canada) Ltd. (Organization)
Decision number (file number)	P2018-ND-60 (File #007714)
Date notice received by OIPC	February 8, 2018
Date Organization last provided information	March 16, 2018
Date of decision	June 18, 2018
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 and is reporting this incident on its own behalf.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • investment account number, • social insurance number, and • financial information. 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 January 15, 2018, a pop-up notification appeared on the computer screen of a representative of the Organization, stating a virus was detected on the computer. The notification instructed the representative to call "Microsoft" to remove it from the system.

	• The representative called the number and spoke to an individual who identified himself as a "Microsoft employee". The individual offered a service to remove and protect against malicious software. • The representative gave the individual her credit card information. The individual also had full access to the representative's computer for about 30 minutes. • The representative became suspicious and called her credit card company to request more information about the transaction. The credit card company confirmed it was a scam. • The representative immediately turned off the computer and took the computer to a repair ship to have all the malware removed. • Although the representative was aware of the hacker's actions during the incident, she did not see files being accessed, copied, deleted or manipulated in any way. • The Organization said there is a chance the hacker accessed the clients' files using other methods not visible to the representative.
Affected individuals	The incident affected 2 individuals.
Steps taken to reduce risk of harm to individuals	• Removed malicious software. • Monitoring investment accounts for suspicious activity. • Filed a report with the Canadian Ant-Fraud Centre.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone on January 18, 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 that "Due to the loss/unauthorized access of the (personal information) it is likely that there is a risk of damage, detriment or injury to the individuals involved. The harm can include humiliation, damage to reputation or relationships, financial loss and identity theft/fraud...". Further, "The harm is potentially significant due to the sensitivity of the information contained in the documentation." In my view, the identity and the financial information at issue could be used for the purposes of identity theft and fraud. 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.	The Organization reported that "It is likely that there is a risk of damage, detriment or injury to the individuals involved" for a number of reasons, including that the information was obtained via unauthorized access into the representative's laptop, the individual(s) who perpetrated the breach is unknown, the information has not been returned, the information is electronic and easily duplicated, the information is highly sensitive, and the information could be used for criminal purposes. I agree with the Organization. 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 and installation of malware). Further, the information may have been available to the unknown third party exposed for approximately 30 minutes.

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 identity and the financial information at issue could be used for the purposes of identity theft and fraud. These are significant harms. 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 and installation of malware). Further, the information may have been available to the unknown third party exposed for approximately 30 minutes.

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 by telephone on January 18, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner