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	McAfee Ireland Ltd. (Organization)
Decision number (file number)	P2018-ND-124 (File #004253)
Date notice received by OIPC	November 7, 2016
Date Organization last provided information	July 20, 2018
Date of decision	September 17, 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 the 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in this incident: • name, • telephone number, • email address, • computer support service subscription and service history. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization offers a computer support service, TechMaster, through a vendor based in India.

	• On or around June 2016, the Organization was made aware that some TechMaster customers were receiving telephone calls from one or more individuals falsely claiming to represent TechMaster. The caller(s) claimed that the customer owed additional fees, was owed a refund, had been over-refunded, or was experiencing issues with their account all with the objective of social engineering financial gain. • In some instances, the caller requested remote access to the customer's computer or device and/or asked the customer to log onto their banking site in order to process payment or to send payments to the caller directly by other means. A small number of customers were convinced to send money or allow remote machine access. • The caller(s) appear to have access to the customer's name, telephone number, email address, and, in some cases, TechMaster product subscription and service history. • An investigation was initiated by the vendor and a separate investigation was initiated by the Organization to identify the caller(s) and their means of stealing the customers' information.
Affected individuals	The Organization received calls from 16 Alberta residents, reporting that they received fraudulent telephone calls from someone claiming to be a representative of the Organization or TechMaster. However, the Organization reported there are 281 Alberta residents who subscribe to TechMaster who are potentially affected by this incident.
Steps taken to reduce risk of harm to individuals	• Both the vendor and the Organization initiated investigations. • The vendor made several changes to its architecture to further secure customer information. • All TechMaster customers were notified of the ongoing fraud and were provided means to contact the Organization with information about any suspicious calls.
Steps taken to notify individuals of the incident	The Organization initially notified customers by email on June 23, 2016, and thereafter sent a follow up notice on July 25, 2016. Information was posted on the TechMaster website. A subsequent written notice was sent on about October 27, 2016 after the Organization learned the caller may have accessed customer information.

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 the incident could result in "Financial Harm. Callers attempt to convince TechMaster customers to share information relating to financial accounts, allow remote access to their computers and/or bank accounts, to send payments or to refund alleged "overpayments" by sending payments via PayPal, MoneyGram, or similar means". I agree with the Organization's assessment. A reasonable person would consider that the information at issue could be used to cause the significant harms of identity theft and fraud. Contact information (including email address) in conjunction with subscriber information could be used for unsolicited targeted telephone calls and phishing attacks. Previous breach notification decisions issued by my office have found phishing to be a significant harm.
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 "This information appears to have been accessed for the purpose of contacting customers with the intent to perpetuate financial fraud. A small number of TechMaster customers have been convinced to send money or allow remote machine access; however, all TechMaster customers have been warned repeatedly of the risk (and [the Organization] will continue with periodic updates and warnings until the threat has been eliminated) and thus the likelihood of significant additional harm is low." The Organization also reported that no Alberta residents have "reported that the caller had access to the TechMaster subscription details or service history, and none of them has reported providing sensitive information or transferring funds to the caller". In my view, the likelihood of harm resulting from this incident is increased because the personal information has been accessed and used for malicious purposes (social engineering for financial gain). The Organization does not appear to know how the information was compromised. In some cases, actual harm has been realized by customers. Despite the fact no Alberta residents have reported access to subscription details or actual harm, this does not preclude such harm from occurring in the future.
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 in this case.	

In my view, a reasonable person would consider that the information at issue could be used to cause the significant harms of identity theft and fraud. Contact information (including email address) in conjunction with subscriber information could be used for unsolicited targeted telephone calls and phishing attacks. Previous breach notification decisions issued by my office have found phishing to be a significant harm.

The likelihood of harm resulting from this incident is increased because the personal information has been accessed and used for malicious purposes (social engineering for financial gain). The Organization does not appear to know how the information was compromised. In some cases, actual harm has been realized by customers. Despite the fact no Alberta residents have reported access to subscription details or actual harm, this does not preclude such harm from occurring in the future.

The Organization is required to notify the affected individuals whose information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization initially notified customers by email on June 23, 2016, and thereafter sent a follow up notice on July 25, 2016. Information was posted on the TechMaster website. A subsequent written notice was sent on about October 27, 2016 after the Organization learned the caller may have accessed customer information. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner