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	Microsoft Corporation (Organization)
Decision number (file number)	P2019-ND-187 (File #013292)
Date notice received by OIPC	May 15, 2019
Date Organization last provided information	May 15, 2019
Date of decision	December 13, 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 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 Organization's notice to affected individuals said the breach… *… could have allowed unauthorized parties to access and/or view information related to your email account (such as your e-mail address, folder names, the subject lines of emails, and the names of other e-mail addresses you communicate with), as well as the content of your e-mail account (such as e-mail contents and attachments)….* This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 30, 2019, the Organization received an external report about a person online selling access to the Organization's consumer Outlook.com email accounts.

	• The Organization investigated and confirmed that the seller was providing valid credentialed access to an internal support tool. • The credentials were from a call centre support supervisor who worked for the Moroccan office of a company providing customer support services to the Organization. The supervisor had, against policy, given credentialed access directly to five support agents on his team who supported consumer email products. • The Organization reported its "…investigation also has included a review of the internal authentication logs for the support supervisor's credentials. This review identified suspicious authentication activity going back at least 12 months".
Affected individuals	The incident affected 102,211 accounts, including 7,077 in Canada.
Steps taken to reduce risk of harm to individuals	• Disabled the credentials. • Terminated the employment of the call centre support supervisor and suspended the support agents. • Quarantined hardware and systems for forensic examination. • Initiated a full review of the service provider company's infrastructure, security and physical security and internal policies regarding the sharing of credentials. • Eliminated access to consumer email content from all of the service provider's staff. • Restricted the level of access necessary to access email content and re-examining the appropriate use for all levels of access within this support tool. • Continuing to investigate additional security measures that could enhance prevention and detection of the malicious misuse of its support tool. • Offered 12 months of identity monitoring at no charge. • Reported incident to data protection authorities.
Steps taken to notify individuals of the incident	Affected individuals were notified on April 12, 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's notice to affected individuals said "As a result [of this incident], you may receive phishing emails or other spam mails. You should be careful when receiving any e-mails from any misleading domain name, any e-mail that requests personal information or payment, or any unsolicited request from an untrusted source…". In my view a reasonable person would consider that, depending on the potentially accessible contents of various affected email accounts, the information could be used to cause the harms of identity theft and fraud. At the very least, email account information

	could be used for phishing purposes, increasing vulnerability to 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 did not specifically assess the likelihood of harm resulting from this incident but, as noted above, it advised affected individuals to "…be careful when receiving any e-mails from any misleading domain name, any e-mail that requests personal information or payment, or any unsolicited request from an untrusted source…". In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a rogue employee (deliberate action, sharing credentials). The Organization has identified suspicious activity dating back at least 12 months.

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 that, depending on the potentially accessible contents of various affected email accounts, the information could be used to cause the harms of identity theft and fraud. At the very least, email account information could be used for phishing purposes, increasing vulnerability to 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 a rogue employee (deliberate action, sharing credentials). The Organization has identified suspicious activity dating back at least 12 months.

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 affected individuals were notified on April 12, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner