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	Pfizer Canada ULC (Organization)
Decision number (file number)	P2020-ND-077 (File #016095)
Date notice received by OIPC	June 10, 2020
Date Organization last provided information	June 10, 2020
Date of decision	July 24, 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 about current employees and certain retirees of the Organization. • name, • position/title, • mailing address, • home telephone number, • date of birth, • social insurance number, • salary for each year employed, • bank account details, • citizenship, • hire date and, • termination date and garnishment information, if applicable. The following information is at issue for individuals who are not current or former employees of the Organization but worked for companies acquired by the Organization and for whom the Organization manages and provides pension or benefits.

	• name, • position/title, • mailing address, • residential or cell phone number, • date of birth, and • social insurance number. 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 18 2020, the Organization's payroll services provider became aware of suspicious activity on its network. • An investigation found that on January 25, 2020, an unauthorized third party gained access to one of the service provider's servers. • The service provider determined that the threat actor was able to remotely gain access to its systems via a remote desktop using name and valid password of an active customer account; however, it was unable to determine how the threat actor compromised the customer account to gain access to its environment. • On April 8, 2020, the service provider determined that the threat actor also accessed a server that contained a file with personal information of the Organization's current and former employees and/or pension or legacy benefits beneficiaries. The service provider could not determine whether the threat actor exfiltrated the file. • On May 14, the service provider notified the Organization of the incident. • The service provider and the Organization worked together to ensure that affected individuals were notified of the incident.
Affected individuals	The incident affected 9,640 individuals, which includes approximately 315 Albertans.
Steps taken to reduce risk of harm to individuals	<u>The service provider:</u> • Conducted an investigation into the incident. • Took servers off the network. • Disabled domain administrator accounts and recreated new accounts. • Implemented Local Administrator Password System (LAPS).

	• Updated anti-virus policies and initiated forced scanning. • Updated cybersecurity tools. • Shut down remote access capability. • Is monitoring inbound and outbound traffic from its systems. • Notified and cooperated with law enforcement authorities. • Notified the Organization. • Offered complimentary credit monitoring services and identity restoration services to affected individuals. • Engaged external legal counsel. • Engaged third-party forensic consultants to assist with its investigation. • Worked with the Organization to notify affected individuals. • Implemented new endpoint monitoring security software to the entire network where supported. • Migrated the affected environment to a new hosted environment. <u>The Organization:</u> • Is reviewing cybersecurity and privacy policies and procedures. • Commenced a global data retention initiative that involves reviewing and potentially reducing the amount of personal information held regarding current and former employees and the length of time such personal information is retained. • Notified the privacy officer, law enforcement, and privacy regulators.
Steps taken to notify individuals of the incident	Current employees and retirees were notified by mail on June 8, 2020. The remaining individuals were notified on July 8, 2020.
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" *In light of the malicious nature of the Incident and the type of personal information involved, it is possible that affected individuals (assuming they are not deceased) may be the subject of fraud, identity theft or other financial loss may occur to affected individuals as a result of the Incident.* In my view, a reasonable person would consider that the contact, identity, financial and employment information at issue could be used to cause the significant harms of identity theft, fraud and/or financial loss.

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… *… the likelihood of harm to affected individuals is moderate to high. While neither [the service provider or Organization] have evidence of actual harm to affected individuals …[the service provider], with the assistance of its forensic IT expert, has determined that certain data was exfiltrated from its environment. However, it has been unable to definitively determine whether the [the Organization's] File was actually exfiltrated. Due to nature of the Incident and the sensitive nature of the personal information at issue there is a moderate to high risk to affected individuals. "* 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). Although it has not been determined definitively whether the Organization's file was actually exfiltrated, the Organization did report that some data was exfiltrated from the service environment. Further, the information may have been exposed for approximately 3 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 the contact, identity, financial and employment information at issue could be used to cause the significant harms of identity theft, fraud and/or financial loss.

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). Although it has not been determined definitively whether the Organization's file was actually exfiltrated, the Organization did report that some data was exfiltrated from the service environment. Further, the information may have been exposed for approximately 3 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 the Organization notified affected individuals by mail on June 8, 2020 and on July 8, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner