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	Bayer Inc. /Bayer AG (Organization)
Decision number (file number)	P2019-ND-087 (File #008989)
Date notice received by OIPC	June 15, 2018
Date Organization last provided information	April 11, 2019
Date of decision	June 25, 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 incident involved all or some of the following information: • name, • business address, • email, • telephone number, • fax number, • qualifications (curriculum vitae and research specialty), • password, • encrypted emails, • contracts, and • comments on study assessments. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies. Some of the information appears to qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information."

	Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." Therefore, I find that PIPA applies to the personal information about the six (6) residents of Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• A SIRIUS file directory was created on May 4, 2018 by a service provider to the Organization. • On June 11, 2018, the Organization was informed by a third party of a possible personal data breach with respect to the file directory, such that it was freely available on the internet. • On June 12, 2018, the Organization notified the service provider of the breach, and access to the directory was closed. • The directory logfiles showed two unauthorized third parties accessed and downloaded the file. One of the two third parties was the reporting third party and was asked to delete the data, which was done. The identity of the second third party is not known. Log information from before January 2018 is missing. • Due to the missing logfiles, the Organization said it was uncertain how long the data was accessible and it cannot be excluded that other unauthorized third parties gained access to all the data.
Affected individuals	The incident affected 146 health care providers and employees in Canada. In Alberta, six (6) health care providers were affected.
Steps taken to reduce risk of harm to individuals	• Closed access to the backup file. • Advised the reporting third party to delete the file directory in its possession. • Confirmed that the third party deleted the relevant data in a secure way.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on June 25, 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: *On the basis of the nature of personal data affected it seems not likely that there will be further negative consequences for the affected data subject. That refers in particular to discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.* *Information regarding system access consists of username and encrypted password. As the encryption key was also part of the backup it is possible for an unauthorized third party with respective technical skills to decrypt the passwords. A password decryption and subsequent misuse of this data - e.g. lo log on to other systems (identity theft) - cannot be ruled out completely, but seems not likely.* *Information on participation in studies as HCPs or in Patient Support Programs, expert matter information or information on qualifications are not suitable to be used for discrimination, a damage to reputation or identity theft.* *It is also not likely that unauthorized access to the business contact details stored in the folder will lead to negative consequences for the affected data subjects. In this respect one has to take into consideration that these information - as well as expert matter information or information on qualifications - are in a high number of cases already publically available from other sources, e.g. from the transparency register (clinicaltrial. gov).* *With respect to unauthorized access to contract data a certain risk for the protection of trade and business secrets cannot be ruled out. An immediate financial loss or comparable negative effect as a consequence of the misuse of personal data nevertheless seems not likely.* In my view, a reasonable person would consider that the contact and employment information at issue, as well as credentials, could be used to cause the significant harms of identity theft, fraud or financial loss, or to compromise other online accounts. Email addresses could be used for phishing purposes, increasing vulnerability to 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: *Analyses show that all personal data stored in the respective file directory have come into the possession of at least two unauthorized persons. One of the two is the reporting third party, who declared to having securely deleted the data on [the Organization's] request.* *Due to missing log files for the time period before January 30, 2018 and missing certainty on the fact which data have been available for which time, it cannot be excluded, that additional unauthorized third parties have gained access to all data. Considering the rather low number of two unauthorized accesses in the time period from January 30, 2018 up to June 12, 2018 it can be assumed, that presumably only a limited number of accesses took place.* The Organization also said, "After final analysis we assess the risk for affected persons as not being high; the data stem from their professional but not private environment". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is decreased because the breach does not appear to be the result of deliberate, malicious access. However, the Organization confirms the information was accessed by an unidentified third party, and, due to missing log files, cannot rule out the possibility that other unauthorized parties may have had access. The Organization cannot confirm how long the information may have been exposed.

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 and employment information at issue, as well as credentials, could be used to cause the significant harms of identity theft, fraud or financial loss, or to compromise other online accounts. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.

The likelihood of harm resulting from this incident is decreased because the breach does not appear to be the result of deliberate, malicious access. However, the Organization confirms the information was accessed by an unidentified third party, and, due to missing log files, cannot rule out the possibility that other unauthorized parties may have had access. The Organization cannot confirm how long the information may have been exposed.

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 in a letter dated June 25, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner