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	Dormakaba International Holding GmbH (Organization)
Decision number (file number)	P2021-ND-069 (File #018742)
Date notice received by OIPC	December 15, 2020
Date Organization last provided information	January 11, 2021
Date of decision	March 9, 2021
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 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 located in Ennepetal, Nordrhein-Westfalen, Germany and 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: • first and last name, • position title, • department, • supervisor, • work telephone number, • work email address, • work address, • private telephone numbers (in exceptional cases used for business), • login name, • password, and • personnel number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported that business contact information, including business email address, was involved in the incident.

	As such, some of the information may 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 of 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." As a result, PIPA applies to the business contact information. To the extent the personal information at issue was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On November 30, 2020, a laptop in the USA belonging to the Organization was hacked. The Organization reported malware was most likely introduced through a phishing attack that spread through its global network. • The Organization said its Active Directory may have been compromised and all Windows users across countries are affected. • The Organization reported that the breach ended on December 4, 2020.
Affected individuals	The incident affected 15,500 individuals of which two (2) are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Removed the malware. • Reset passwords. • Deleted and rebuilt affected servers. • Offered training to all staff with computer access on eLearning modules: - Information security in general - Phishing - Social Engineering

Steps taken to notify individuals of the incident	The affected individuals were not notified.
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 possible harm that may result from the breach is "Loss of control of their personal information." In my view, a reasonable person would consider that the contact, identity (personnel number), and employment information, particularly in conjunction with credentials, could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Credentials could also be used to compromise other online accounts. These are all 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, *Likelihood of occurrence: Between Possible and Probable* *The following four-point scale was used for the assessment of the Likelihood of occurrence:* *1 - Unlikely* *2 - Possible* *3 - Probable* *4 - Very likely/foreseeable* *Severity of the harm: Limited* *The following four-point scale was used for the assessment of the Severity of the harm:* *1 - Negligible* *2 - Limited* *3 - Substantial* *4 - Maximum* In my view, a reasonable person would consider that 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, malware) and phishing emails were sent. The information appears to have been exposed for approximately (six) days.

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 (personnel number), and employment information, particularly in conjunction with credentials, could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Credentials could also be used to compromise other online accounts. These are all 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, malware) and phishing emails were sent. The information appears to have been exposed for approximately (six) days. **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), and confirm to my Office in writing, within ten (10) days of the date of this decision, that this has been done.**

Jill Clayton
Information and Privacy Commissioner