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	Angeion Group (Organization)
Decision number (file number)	P2021-ND-195 (File #018645)
Date notice received by OIPC	December 8, 2020
Date Organization last provided information	December 8, 2020
Date of decision	October 15, 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 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 operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA. The Organization's head office is in Philadelphia, Pennsylvania, U.S.A.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, 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 information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On July 17, 2020, the Organization learned that between March 30, 2020 and May 4, 2020, an unknown unauthorized third party remotely accessed the corporate email box of an employee. • The email box included personal information associated with claims administration files and related communications.

	• The Organization reported that the cause of the unauthorized access has not been determined. • The breach was discovered on July 17, 2020 in the course of investigating another matter involving the same email box.
Affected individuals	The incident affected 67,677 individuals, including 3 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Secured the compromised email box. • Obtained the advice and assistance of outside consultants. • Investigated to determine the scope of the incident, identify potentially affected individuals and confirm the jurisdiction for each. • Notified law enforcement of the incident. • Took action to prevent similar incidents from occurring in the future, including enhanced employee training and security. • Offered free identity monitoring services to affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on December 4, 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: *If the perpetrator in fact accessed a particular individual's social insurance number, there would be a risk that the perpetrator could misuse that information.* In my view, a reasonable person would consider that name and social insurance number could be used to cause the harms of 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 reported it… *… has not been able to determine whether or not any particular individual information in the email account was in fact accessed by the perpetrator. [The Organization] also is not aware of any misuse of any individual's information. Accordingly, although the likelihood of harm appears low, out of an abundance of caution, [the Organization] is notifying relevant individuals and regulators.* 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. The lack of reported incidents

	resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Further, it appears the email account was exposed for approximately thirty-five (35) 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 name and social insurance number could be used to cause the harms of 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 an unknown third party. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Further, it appears the email account was exposed for approximately thirty-five (35) 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).

I understand the Organization notified affected individuals by letter on December 4, 2020 in accordance with the Regulations. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner