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	Life Fitness, a division of Brunswick Corporation (Organization)
Decision number (file number)	P2021-ND-049 (File #008807)
Date notice received by OIPC	May 31, 2018
Date Organization last provided information	May 31, 2018
Date of decision	March 2, 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 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, • email address, • date of birth, • age, • account username, • height, • weight, and • Facebook UserID. 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	• LFconnect is a fitness app available from the Organization that tracks workout data. Data from the app's crash reports were stored on a Google database. • On April 24, 2018, the Organization received an email from a third party security firm advising that it had discovered a firebase database that contained crash reports for the LFconnect mobile application. The crash reports were for data between April 2016 and May 2017. • The Organization reported that it has no evidence that the data was actually accessed by any third party with any intent to do harm.
Affected individuals	The incident affected 3,900 individuals. The Organization did not respond to requests to confirm how many Alberta residents were affected by the incident.
Steps taken to reduce risk of harm to individuals	• Decommissioned the firebase database and deleted the data. • Took additional steps to review any other data and how it is or has been secured. No other instances have been discovered.
Steps taken to notify individuals of the incident	The Organization reported that affected individuals were notified by email and a notice posted on its website.
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 might result from this incident is "None. We have no evidence that the data was accesssed [sic] with any intent to do harm. Further, given the limited data elements, the information could not be used for identity theft, fraud, credit record or damage or loss of property.**"** In my view, a reasonable person would consider that the contact and identity information at issue could be used to cause the harms of identity theft and fraud. Credentials could be used to compromise other online accounts. Health information (weight and height) could be used to cause hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. 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 that "Given that this database was not conspicuously visible and would require technical skills to access, and we have not noted any suspicious activity on any of the affected accounts, we have concluded that the risk of harm is relatively low." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the

	database was discovered by at least one third party who reported the breach to the Organization. The Organization cannot rule out the possibility that other unauthorized parties accessed the data. It is not clear how long the information may have been exposed. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing and the use of stolen credentials can occur months and even years after a data breach.

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 identity information at issue could be used to cause the harms of identity theft and fraud. Credentials could be used to compromise other online accounts. Health information (weight and height) could be used to cause hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the database was discovered by at least one third party who reported the breach to the Organization. The Organization cannot rule out the possibility that other unauthorized parties accessed the data. It is not clear how long the information may have been exposed. The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing and the use of stolen credentials can occur months and even years after a data breach.

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 email and by posting a notice on its website. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner