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	Goodlife Fitness Centres Inc. (Organization)
Decision number (file number)	P2019-ND-037 (File #007973)
Date notice received by OIPC	March 6, 2018
Date Organization last provided information	March 6, 2018
Date of decision	February 19, 2019
Summary of decision	There is a real risk of significant harm to some of the individuals affected by this incident. The Organization is required to notify those individuals 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 Organization reported the information was in three general types of contracts: • Standard contract: name, address, services purchased, total purchase price and, where applicable, details regarding quantum and timing of monthly payments; • Contracts for members associated with certain companies: information identified above plus telephone number, email address and home club; • A limited number of contracts included the above information, as well as date of birth, company name and emergency contact number. No financial data, social insurance numbers or other highly sensitive identification were included in any of the above cases. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• The Organization was testing a new membership database which would send membership contracts by email, and on March 1, 2018 the first live delivery of contracts to members started. • On March 2, 2108, the Organization discovered an error in the system, which was not detected during testing, whereby some members inadvertently received other members' contracts. • The Organization received emails and telephone calls from members who had received the contracts of other members.
Affected individuals	The incident affected 485 individuals.
Steps taken to reduce risk of harm to individuals	• Compiled lists detailing members who received the wrong contract and a list of members whose contract was sent to the wrong person. • Asked those members who received contracts in error to delete them immediately and confirm deletions. • Made telephone calls to those who received contracts in error to follow-up on the request to delete.
Steps taken to notify individuals of the incident	Affected individuals were notified by email March 3, 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 that "In general, harm is anticipated to be minimal. Affected individuals may suffer distress at the thought of their information being in unknown individuals' hands, however the type of information, in most cases, is very limited. Financial loss, damage to or loss or [sic] property, would be at very low risk of occurrence. A slightly higher risk may be present in the cases where the individual's birth date and company name were included, as that information, coupled with name and address could potentially be used to commit identity theft. " In my view, a reasonable person would consider that the information included in the standard contracts could not reasonably be used to cause significant harm. Email addresses included in the contracts for members associated with certain companies, however, could be used for phishing purposes, increasing affected individuals' vulnerability to the significant harms of identity theft and fraud. The additional identity information (date of birth) included in a limited number of contracts could be used to cause the significant harms of 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 that "For the most part, the information is not highly sensitive, and, as noted below, steps were taken very quickly to limit the amount of exposure. The error was internal and inadvertent and no third parties were involved. There was no malicious intent or purpose. The disclosure of additional information that could, potentially, be used for identity theft or fraud affected only 40 of the total 485 individuals affected." In my view, a reasonable person would consider that the likelihood of harm is reduced as the incident did not result from malicious intent, but rather an email error. Further, the Organization followed up with the unintended recipients to request they delete the email. However, the Organization's report of the breach did not indicate how successful these efforts were. In addition, the number of unintended recipients increases the likelihood of significant harm.

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 some of the affected individuals.

A reasonable person would consider that the information included in the standard contracts could not reasonably be used to cause significant harm. Email addresses included in the contracts for members associated with certain companies, however, could be used for phishing purposes, increasing affected individuals' vulnerability to the significant harms of identity theft and fraud. The additional identity information (date of birth) included in a limited number of contracts could be used to cause the significant harms of identity theft and fraud.

The likelihood of harm is reduced as the incident did not result from malicious intent, but rather an email error. Further, the Organization followed up with the unintended recipients to request they delete the email. However, the Organization's report of the breach did not indicate how successful these efforts were. In addition, the number of unintended recipients increases the likelihood of significant harm.

Pursuant to section 37.1 of PIPA, the Organization is required to notify the affected individuals whose personal information was included in the contracts for members of certain companies, and the limited contracts. I understand the Organization notified all affected individuals by email March 3, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner