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	Royal Glenora Club (Organization)
Decision number (file number)	P2018-ND-003 (File #005319)
Date notice received by OIPC	April 3, 2017
Date Organization last provided information	October 3, 2017
Date of decision	January 2, 2018
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is incorporated under Part 9 of the *Companies Act* and qualifies as a "non-profit organization" as defined in section 56(1)(b) of PIPA. Under sections 56(2) and (3), PIPA only applies to personal information that is collected, used or disclosed by non-profit organizations in connection with a commercial activity. In this case, the Organization reported that "We generate out [sic] revenues from member fees, private lessons, registered programs, food and beverage outlet, and banquets." In my view, the Organization's operation of a recreational facility is a commercial activity. In Order P2017-07, an Adjudicator with my Office found that employees hired to perform functions necessary to carry out a commercial activity are hired "in connection with" that commercial activity. The information at issue in this incident is the personal information of employees of the Organization. The Organization reported that "The individuals that were affected by the breach worked as a housekeeper, cook and kitchen staff, banquet server, or maintenance worker." These are functions that are necessary to carry out the Organization's commercial activity of operating a recreational facility.

	I have jurisdiction because the information at issue was collected in connection with a commercial activity, as contemplated in section 56(3) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • social insurance number, • banking information, and • amount of pay. 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	• On March 23, 2017, a deposit report containing the personal information at issue for 15 of the Organization's employees was inadvertently attached to earnings statements that were emailed to all other employees. • The Organization investigated and found the error was caused by a programming problem. • The incident was discovered the same day.
Affected individuals	The incident affected 15 Alberta employees.
Steps taken to reduce risk of harm to individuals	• Rectified the setting issues and now able to view emails being sent out prior to sending. • Made changes to the accounting software system. • Purchased a credit monitoring subscription for one year for all affected employees.
Steps taken to notify individuals of the incident	Eleven of the affected individuals were notified in person or by telephone on March 23, 2017, and messages were left for the other four. Notices were mailed out on March 23, 2017.

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 harms that might result from this incident include "potential financial loss, fraud, identity theft and negative effects on a credit record." I agree with the Organization. The identity, financial and employment information at issue could be used to cause the harms of identity theft, fraud and financial loss, and may have a negative effect on credit records. In addition, the employment information (amount of pay) could be used to cause the harms of embarrassment, hurt and humiliation. 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 "Financial loss risk should be low as most of the individual changed there [sic] bank accounts within the day the breach occured [sic]. Fraud and identity theft risk would be low to meduim [sic]. The information was sent our [sic] to fellow staff members. Approx 171 individual of which some of those emails were recalled. (unable to verify how many) I would like to believe that our employees are people who do not engage in fraud or identity theft…". I agree with the Organization that the risk of fraud and identity theft may be reduced given that the incident resulted from human error and not malicious intent, and the information was sent to employees known to the Organization. However, the Organization was not able to recall all of the emails, and the affected individuals are likely to have personal and professional relationships with the unintended recipients, increasing the likelihood of hurt, humiliation or embarrassment resulting from the incident.

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.

The identity, financial and employment information at issue could be used to cause the harms of identity theft, fraud and financial loss, and may have a negative effect on credit records. In addition, the employment information (amount of pay) could be used to cause the harms of embarrassment, hurt and humiliation. These are all significant harms.

I agree with the Organization that the risk of fraud and identity theft may be reduced given that the incident resulted from human error and not malicious intent, and the information was sent to employees known to the Organization. However, the Organization was not able to recall all of the emails, and the affected individuals are likely to have personal and professional relationships with the unintended recipients, increasing the likelihood of hurt, humiliation or embarrassment resulting from the incident.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that eleven of the affected individuals were notified in person or by telephone on March 23, 2017, and messages were left for the other four. Notices were mailed out on March 23, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner