Office of the
Information &
Privacy Commissioner
for British Columbia
Protecting privacy. Promoting transparency.

September 30, 2014

Jim Lightbody
Interim CEO and President
BCLC
2940 Virtual Way
Vancouver, BC V5M 0A6

Dear Jim Lightbody:

BCLC—Investigation re resignation of former CEO and President—OIPC File No. F14-58367

Background

Members of the public have raised concerns with my office regarding whether former British Columbia Lottery Corporation ("BCLC") CEO and President Michael Graydon had inappropriate access to BCLC's networks after his resignation earlier this year. In response to these concerns, my office initiated an investigation of this issue on July 22, 2014, in accordance with my authority under s. 42(1)(a) of the *Freedom of Information and Protection of Privacy Act* ("FIPPA").

Issue

The issue in this investigation is whether BCLC had reasonable security arrangements in place at the time of the departure of former CEO and President Michael Graydon to protect personal information in its custody or under its control against such risks as unauthorized access, collection, use, disclosure or disposal as required by s. 30 of FIPPA. Our investigation focussed solely on the personal information Mr. Graydon could have accessed following his departure from BCLC.

Relevant Timeline

The following is a brief timeline of the key dates surrounding Mr. Graydon's departure:

- January 29, 2014 – Mr. Graydon advised BCLC that he was resigning effective March 31, 2014.
- February 4, 2014 –Mr. Graydon's last day at work as decided by BCLC's Board after they accepted his resignation.

- February 6, 2014 – BCLC remotely deleted the information on Mr. Graydon's work-issued Blackberry (information on his work-issued iPad could not be remotely deleted) and changed his password for his email account.

- February 14, 2014 – BCLC entirely removed Mr. Graydon's access to BCLC systems.

Evidence from OIPC Investigation

BCLC met with my investigators and provided them with all information to which Mr. Graydon has access after his last day of work with BCLC. In considering BCLC's responsibilities under s. 30 of FIPPA, my investigators identified two main concerns.

First, upon completion of his last day of work on February 4, 2014, BCLC did not require Mr. Graydon to return his work-issued mobile devices, nor did BCLC ensure it deleted all personal information from these devices. BCLC's access logs show that Mr. Graydon did log into his BCLC account after his departure. It was not until two days after Mr. Graydon's last day of work that BCLC remotely deleted the information from his Blackberry. Further, while BCLC changed the password for Mr. Graydon's email account on February 6 and did not inform him of the new password, they could not remotely delete information from his work-issued iPad. This meant that Mr. Graydon retained access to existing emails on his iPad as of February 6, 2014.

My investigators were able to view all of the emails that Mr. Graydon had on his mobile devices as well as the emails he sent and received from his BCLC email account on February 5 and 6. Most emails related to BCLC corporate matters and did not contain any personal information. A small number of emails contained opinions of employees and a relatively minimal amount of other personal information relating to individuals in the gaming industry. No emails contained the personal information of BCLC customers.

Our second concern is that Mr. Graydon had access to his BCLC account containing some personal information until February 6, 2014. Mr. Graydon had access, but did not view, a limited amount of personal information from old resumes. He did not have access to customer data. Mr. Graydon retained access to corporate (non-personal) information on the BCLC servers until February 14, 2014.

BCLC informed my investigators that there was a formal procedure in place for the departure of employees prior to Mr. Graydon leaving BCLC where an exiting employee's manager was assigned responsibility for departure of the employee. However, BCLC's procedure did not assign responsibility for overseeing the departure of the Chief Executive Officer and President.

In addition, BCLC's information security policy required that remote access to information systems be terminated within one day of an employee's departure. However, Mr. Graydon's access was not completely terminated for 10 days. BCLC told my investigators that it granted an exception to its normal process of not allowing staff to retain their mobile devices for Mr. Graydon, but acknowledge that it should have deleted the information from his mobile device prior to his departure.

Analysis

Section 30 of FIPPA requires a public body such as BCLC to make reasonable security arrangements to protect personal information in its custody or under its control. Reasonableness is an objective standard that varies depending on the situation, but does not require perfection.

In looking at the circumstances of this situation, it was not reasonable for BCLC to have exempted Mr. Graydon from returning his work-issued mobile devices or, at a minimum, deleting all of the personal information from these devices. Similarly, it was not reasonable for BCLC to allow Mr. Graydon unauthorized access to personal information in BCLC's custody or under its control after his departure. These are very basic steps that my office would expect of any public body concurrent with an employee's departure.

As a result, I find that BCLC did not have reasonable security arrangements in place to protect the personal information in its custody or control at the time of Mr. Graydon's departure from BCLC and was in contravention of its obligations under s. 30 of FIPPA. This contravention of FIPPA resulted in an unauthorized disclosure of a limited amount of personal information to Mr. Graydon after his February 4, 2014 departure from BCLC.

BCLC did not notify individuals affected by Mr. Graydon's unauthorized access because they believed the nature of the personal information involved presented no serious risk of harm. I agree with BCLC's assessment. Mr. Graydon had legitimate access to all this personal information prior to his departure, the information was not particularly sensitive and there was no evidence he had inappropriately used it after his departure.

BCLC's Changes to its Procedure for Departing Employees

BCLC was quickly aware of its improper handling of Mr. Graydon's exit. On February 7, 2014, three days after Mr. Graydon's last day, BCLC incorporated additional controls into its procedure for departing employees. These changes included assigning responsibility to the Human Resources department rather than to the exiting employee's manager. Included in those responsibilities is the deactivation of building and system access as well as the responsibility for retrieving work-issued mobile devices. I note

that the information security management standard with respect to work-issued mobile devices is to require departing employees to return them.[1]

Having a central point of responsibility and clear accountability for the departure of employees is critical for any public body as it promotes awareness and consistency of the appropriate steps to take when an employee departs. Had these measures been in place and properly followed prior to Mr. Graydon's departure, BCLC would not have contravened the personal information security requirements of s. 30 of FIPPA. I am satisfied that BCLC's changes to its procedure for departing employees have mitigated the risk of a reoccurrence of a similar incident.

Due to the complaints from the public that initiated this investigation, I will be posting a copy of this letter on my office's website.

Sincerely,

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for Britsh Columbia

pc: Angela Swan, Director, Information Privacy & Security, BCLC

[1] See ISO/IEC 27001:2013(E) A.8.1.4 Return of Assets.