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	Solara Condominium Corporation (Organization)
Decision number (file number)	P2018-ND-129 (File #8694)
Date notice received by OIPC	May 17, 2018
Date Organization last provided information	May 27, 2018
Date of decision	August 13, 2019
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 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, • resort address, • email address, • information about payment of condominium fees, • list of unit numbers, • GST records, and • potentially other financial and personal information about owners, such as arrears. 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	• An Executive member of the Organization's board was provided with a USB drive which contained confidential owner information. • On April 17, 2018, the Organization discovered that when the member ceased to hold the role on the Board, the USB stick was not returned. • The Organization reported that the loss was discovered when "…the former Executive member's…husband sent an email to the current Board confirming [the former member] still possessed the USB drive which contained information and that the … information [was used] to access owner GST information." • The former member denied having kept any information.
Affected individuals	The incident affected approximately 200 individuals.
Steps taken to reduce risk of harm to individuals	Demanded the return of the USB drive from the former member; at the time of reporting, the USB had not been returned/located.
Steps taken to notify individuals of the incident	The Organization reported that "…owners were notified on May24, 2018 of the potential disclosure of information", but did not provide a copy of the notification.
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 "There could be the possibility of fraud as many aspects of the owners personal information is available, negative effects on credit for any owners in arrears of payment of fees." In my view, the contact and financial information could be used to cause the harms of identity theft and fraud, as well as embarrassment and humiliation. 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 it… *…believe[s] the former Executive member's motives are to discredit the current Board and despite access having access [sic] to all owner … there does not appear to be any sign that the information has been used to harm owners. The former Executive member has been in possession of the information since October 2015 and there has not been any evidence of malicious intent expect [sic] the use of owner email information and, of late, GST information by owner. Although the information could be used for criminal*

	purpose like fraud, there has been no indication fraud has occurred. In my view, the likelihood of harm resulting from this incident is increased because the personal information has not been recovered and, while the Organization believes it is in the possession of the former Executive member, the former members denies having it. The lack of reported incidents resulting from this incident to date is not a mitigating factor, as identity theft and fraud, as well as phishing, hurt, and humiliation 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.

The contact and financial information could be used to cause the harms of identity theft and fraud, as well as embarrassment and humiliation. 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 personal information has not been recovered and, while the Organization believes it is in the possession of the former Executive member, the former members denies having it. The lack of reported incidents resulting from this incident to date is not a mitigating factor, as identity theft and fraud, as well as phishing, hurt, and humiliation can occur months and even years after a data breach.

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 the Organization reported that "…owners were notified on May24, 2018 of the potential disclosure of information", but did not provide a copy of the notification. **I require the Organization to provide a copy of the notification to affected individuals to my office within 10 days of the date of this decision.**

Jill Clayton
Information and Privacy Commissioner