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	Envision Property Management Ltd. (Organization)
Decision number (file number)	P2018-ND-118 (File #009591)
Date notice received by OIPC	August 28, 2018
Date Organization last provided information	August 28, 2018
Date of decision	September 4, 2018
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual in pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information about an occupant of a unit of a residential condominium property that the Organization manages: • telephone number, and • email address. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• In June 2018, thieves broke in to the group mailbox at a residential condominium property the Organization manages and stole mail from a number of mailboxes including one individual's new credit card.

	• The Organization's office was subsequently contacted by telephone by a person who identified himself as being with the Calgary Police Service. The caller requested a telephone number and email address for an occupant of the condominium property (the individual whose credit card had been stolen). • The Organization's staff member who answered the phone believed the call was from law enforcement and provided the individual's telephone number and email address. It now appears that the caller was not with the Calgary Police Service. • After the call to the Organization's office, someone (either the same person or an associate) called the individual on two occasions; the second call used a "spoofing" call-display technology to make it appear the call was coming from the Calgary Police Service non-emergency telephone number. • The Organization understands the individual declined to provide personal information during the first call, but during the second call the individual was fooled by the "spoofing" call-display technology into believing the call was from Calgary Police Service and provided his date of birth and middle name. • The information provided by the individual enabled the mail thieves or an associate of theirs to activate the stolen credit card and begin making charges against the credit card.
Affected individuals	The Organization reported the information disclosed concerned one (1) occupant of the condominium property. The Organization also noted that the individual's girlfriend may also be affected; however, in my view, this is not the case as the information at issue is about the affected individual only.
Steps taken to reduce risk of harm to individuals	• The Organization reported that the affected individual notified law enforcement. • Established a policy that no information will be disclosed by telephone to anyone claiming to be from the Calgary Police Service, but only to persons identifying themselves as police upon personal attendance at the Organization's office by a uniformed police officer.
Steps taken to notify individuals of the incident	The Organization reported that it was notified of the incident by the affected individual himself, and "no steps were taken … to notify individuals, as any affected individuals were already aware of the incident".

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 type of harm that may and did result from [the Organization's] breach is unwanted telephone or email contact.* *Further harm, in the nature of fraud, identify theft, and other effects from what occurred subsequently, resulted only from [the individual's] own subsequent disclosure of his own more sensitive personal information (date of birth and middle name). [The Organization] understands that [the individual's] telephone number and email address would not have enabled, and did not enable, the perpetrator(s) to commit any fraud. The perpetrator(s) was/were only able to activate and use [the individual's] credit card with the more sensitive personal information that [the individual] himself provided to the perpetrator(s).* *…* *[The Organization] does not anticipate there would be any humiliation, or damage to [the individual's] reputation, as …banks and credit bureaus would readily believe the information from [the individual] as to what occurred.* The Organization also reported that the individual contacted news media about what occurred. The Organization does not believe that public disclosure of what occurred would lead to humiliation or other damage to the affected individual, and noted that the contact with media was initiated by the affected individual. In my view, a reasonable person would consider that the information disclosed by the Organization (telephone number and email address) could be used to cause the harm of phishing, or potentially spear-phishing, particularly if combined with other known information about an individual. Numerous breach notification decisions issued by my office have identified phishing and spear-phishing as significant harms (see #P2001-ND-011, for example).
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 "…the likelihood that harm could result is very low, absent (as in this case) the affected person himself subsequently disclosing additional, more sensitive personal information". In my view, a reasonable person would consider there is a real risk of significant harm in this case. The unauthorized disclosure of personal information by the Organization was the result of malicious intent (individual impersonating a police officer). The information disclosed

	was subsequently combined with other information known to the perpetrator(s), and used to contact the affected individual with the aim of obtaining more sensitive information. That is, it appears likely that as a direct result of the breach, the affected individual was contacted by the perpetrators of a targeted and sophisticated spear-phishing attack. This attack was ultimately successful as the affected individual's credit card was used for fraudulent purposes. Although I understand the individual has not been held responsible for those purchases, it nonetheless remains the case that the perpetrators of this attack have a significant amount of information about the affected individual that may, in the future, be used to cause additional 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 the affected individual.

A reasonable person would consider that the information disclosed by the Organization (telephone number and email address) could be used to cause the harm of phishing, or potentially spear-phishing, particularly if combined with other known information about an individual. Numerous breach notification decisions issued by my office have identified phishing and spear-phishing as significant harms (see #P2001-ND-011, for example).

The unauthorized disclosure of personal information by the Organization was the result of malicious intent (individual impersonating a police officer). The information disclosed was subsequently combined with other information known to the perpetrator(s), and used to contact the affected individual with the aim of obtaining more sensitive information. That is, it appears likely that as a direct result of the breach, the affected individual was contacted by the perpetrators of a targeted and sophisticated spear-phishing attack. This attack was ultimately successful as the affected individual's credit card was used for fraudulent purposes. Although I understand the individual has not been held responsible for those purchases, it nonetheless remains the case that the perpetrators of this attack have a significant amount of information about the affected individual that may, in the future, be used to cause additional harm.

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

I understand the Organization reported that it was notified of the incident by the affected individual himself, and therefore "no steps were taken … to notify individuals, as any affected individuals were already aware of the incident".

I require the Organization to confirm to my office within ten (10) days of the date of this decision that it has directly notified the affected individual in compliance with the Regulation.

Jill Clayton
Information and Privacy Commissioner