



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Real Estate Council of Alberta (Organization)
Decision number (file number)	P2017-ND-55 (File #004267)
Date notice received by OIPC	November 9, 2016
Date Organization last provided information	November 9, 2016
Date of decision	May 15, 2017
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the affected individuals pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is incorporated in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved email addresses of tenants and owners. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information is about residents of Alberta.
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On November 1, 2016, the Organization sent two separate emails to owners and tenants respectively to notify them about the license suspension of a property management company.• In both cases, email addresses of all recipients were included in the "To" line instead of the "BCC" line, disclosing all email addresses to the recipients. Fourteen (14) of the emails bounced back as un-deliverable.• On November 3, 2016 an employee of the suspended brokerage firm reported the error to the Organization.

Affected individuals	The Organization reported 145 individuals may be exposed to harm as a result of the incident.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Contacted all email recipients, explained what took place and asked them to delete the email. • Reviewing and updating emailing practices to help ensure this type of human error does not occur again. • Cautioned all staff to take care and take adequate measures when sending email, including close email review before sending group/mass emails. • Providing privacy and information management training to staff annually.
Steps taken to notify individuals of the incident	The affected individuals were notified by email on November 4, 2016.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>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.</p>	<p>The Organization reported that “The potential harm includes the potential for tenants and owners to receive unsolicited emails, to potentially experience phishing scams or SPAM emails.” The Organization also reported that only email addresses were exposed, and not names, and that “An email address may contain a name, identifying an individual, but is likely less sensitive in and of itself. For example, in and of itself, this information alone would likely not result in identity theft.”</p> <p>In my view, the information at issue in and of itself cannot reasonably be used for identity theft or fraud. However, email addresses in conjunction with affected individuals’ known association with the Organization and the suspended brokerage could be used to profile and target affected individuals through phishing. This is a significant harm.</p>
<p>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.</p>	<p>In assessing the likelihood of harm resulting from this incident, the Organization noted that:</p> <ul style="list-style-type: none"> • “tenant and owner email addresses were disclosed only to other tenants and owners (in two separate emails)”; • only “email addresses with no other identifying information was disclosed”; • recipients “were quickly advised...about the unauthorized disclosure and were asked to delete the email”; and, • the emails contained a confidentiality disclosure at the bottom of the email.

	<p>Further, the “unauthorized disclosure occurred as a result of inadvertence and not malicious intent.” However, the Organization also reported that “We believe the risk of harm may increase because a relatively large number of email addresses were disclosed.”</p> <p>In my view, despite the fact the incident resulted from human error and not malicious intent, the relatively large number of unauthorized recipients, and the inability to confirm that all emails were deleted and not further distributed increases the likelihood of harm resulting from this incident.</p>
--	---

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 information at issue, in and of itself, cannot reasonably be used for identity theft or fraud. However, email addresses in conjunction with affected individuals’ known association with the Organization and the suspended brokerage could be used to profile and target affected individuals through phishing. This is a significant harm. Despite the fact the incident resulted from human error and not malicious intent, the relatively large number of unauthorized recipients, and the inability to confirm that all emails were deleted and not further distributed increases the likelihood of harm resulting from this incident.

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

I understand the Organization notified affected individuals by email on November 4, 2016. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner