



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Beacon Consumer Holdings Inc. (Organization)
File number	P2017-ND-117 (File #002703)
Date notice received by OIPC	March 1, 2016
Date Organization last provided information	April 25, 2017
Date of decision	August 9, 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 those 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”	<p>The incident involved the following information:</p> <ul style="list-style-type: none">• name of contact,• name of company, and• email address. <p>This information is about identifiable individuals and is personal information as defined in section 1(1)(k) of the Act.</p> <p>The Organization reported that, of the affected individuals in Alberta, “seven were individuals and seven were corporate contacts (i.e. representatives of businesses).”</p> <p>As such, some of the information appears to qualify as “business contact information” which is defined in section 1(1)(a) of PIPA to mean “an individual’s name, position name or title, business telephone number, business address, business e-mail address, business fax number and other similar business information.”</p>

	<p>Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information “for the purposes of enabling the individual to be contacted in relation to the individual’s business responsibilities and for no other purpose.”</p> <p>In this case, I considered that the possible unauthorized access to the information was not “for the purposes of enabling the individual to be contacted in relation to the individual’s business responsibilities and for no other purpose.”</p> <p>Therefore, I find that PIPA applies to the personal information about the fourteen (14) residents of Alberta.</p>
DESCRIPTION OF INCIDENT	
<p><input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure</p>	
Description of incident	<ul style="list-style-type: none"> • On February 17, 2016, the Organization discovered a virus on its system relating to its website. • The Organization investigated and found that an unauthorized individual may have obtained access to the contact information at issue. The Organization reported that it “...does not have any direct confirmation that the information was in fact accessed.” • The Organization found that no other information was accessed. • The investigation indicated that the incident was isolated to a single occurrence.
Affected individuals	<p>The incident affected fourteen (14) individuals in Alberta of which seven (7) were individuals and seven (7) were corporate contacts (i.e. representatives of businesses).</p>
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Encouraged individuals to be aware of suspicious emails and phishing emails seeking personal information. • Provided a link to the Government of Canada’s “Get Cyber-Safe.” • Emphasized that the Organization will never ask individuals for their passwords, financial or personal information by email. • Reviewed systems and processes with a view to implementing safeguards to avoid similar incidents.
Steps taken to notify individuals of the incident	<p>On March 1, 2016, the Organization wrote to the affected email addresses to notify the contacts of the potential incident.</p>

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 did not specifically identify any harm that might result from this incident but noted that it had advised potentially affected individuals to “be on the lookout for any suspicious email scams such as “phishing” emails seeking personal information, particularly messages that purport to be from [the Organization].”</p> <p>In my view, the email addresses could be used to send unsolicited emails and for phishing. Consistent with previous breach notification decisions issued by my office, phishing 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>The Organization reported that it “has not received any information or complaints from the potentially affected contacts which would suggest that the information was accessed or misused” and that “a reasonable person would not consider that there exists a real risk of significant harm in this matter.”</p> <p>In my view, the likelihood of harm resulting in this case is increased because the incident appears to be the result of malicious intent (a website virus and potential unauthorized access).</p>
DECISION UNDER SECTION 37.1(1) OF PIPA	
<p>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.</p> <p>Email addresses could be used to send unsolicited emails and for phishing. Consistent with previous breach notification decisions issued by my office, phishing is a significant harm. The likelihood of harm resulting in this case is increased because the incident appears to be the result of malicious intent (a website virus and potential unauthorized access).</p> <p>I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organization wrote to the affected email addresses on March 1, 2016. The Organization is not required to notify the affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner