



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	LiveGlam, Inc. (Organization)
Decision number (file number)	P2018-ND-33 (File #007487)
Date notice received by OIPC	January 18, 2018
Date Organization last provided information	January 24, 2018
Date of decision	February 28, 2018
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 an “organization” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• name,• mailing address,• billing address,• email address,• telephone number, and• credit card number and associated CVV codes. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p> <p>The information was collected from Albertans via the Organization’s website.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• The Organization recently discovered that its website was subject to an attack that began in April 25, 2017.

	<ul style="list-style-type: none"> On December 11, 2017, the Organization confirmed that an unauthorized individual may have gained access to a section of the Organization’s online store that processes customer orders.
Affected individuals	The incident affected 160 Alberta residents.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> Immediately took steps to block further unauthorized access. Engaged a forensic security firm to assist in investigating the matter. Notified law enforcement. Notified affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on January 14, 2018.
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 its notification to affected individuals stated “Because your credit card information may have been compromised, the major payment card brands have been notified of the issue so they can monitor you (sic) payment card account for fraudulent purposes.”</p> <p>In my view, the financial information at issue (payment card numbers, security codes) could be used to cause the significant harms of fraud, identity theft and financial loss. The contact information at issue, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be 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 did not specifically provide an assessment of the likelihood that significant harm would result from this incident.</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud. Further, the information may have been exposed for approximately seven months.</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.	

In my view, the financial information at issue (payment card numbers, security codes) could be used to cause the significant harms of fraud, identity theft and financial loss. The contact information at issue, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information may have been exposed for approximately seven months.

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 letter on January 14, 2018, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner