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	Beauty Express Canada Inc. D/B/A The Lice Crew (Organization)
Decision number (file number)	P2018-ND-097 (File #009131)
Date notice received by OIPC	July 6, 2018
Date Organization last provided information	July 11, 2018
Date of decision	August 3, 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 the individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 56 of PIPA "non-profit organization"	The Organization carries on business 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: • name, • telephone number, • details of appointment, • additional personal information provided by individuals. The information above is about identifiable individuals 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	• On February 13, 2018, a client contacted the Organization to report that she had done a search of her mobile phone number in Google and discovered that information about her and her child's appointment with the Organization were published on Google.

	• The Organization's IT department immediately investigated and rectified the issue. • At the time of the breach, the Organization did not have any security arrangements in place. The scheduler was unsecure. It not password protected because it was programmed for internal use only. • The scheduler was used by the Organization at all of its locations across Canada. • The Organization does not know, and is unable to determine, how long an individual's personal information in its scheduler was exposed on the internet. • The Organization is unable to determine how many individuals were affected as it has no way of knowing when the issue with the scheduler began, or of determining how many individuals had their information exposed prior to the Organization rectifying the issue. • As the scheduler contained a field for the Organization to add information provided to it by the individual, and at least in the case that was reported to the Organization, the notes field contained the name of a child, the Organization cannot say with certainty that the names of other children, or other personal information, was not contained in the notes field and exposed through the availability of the scheduler on the internet. • The Organization advised that it has no way of knowing whether anyone's information in the scheduler was accessed on the internet by a third party, however, no other complaints were made about this to the Organization.
Affected individuals	The Organization reported it is unable to determine the number of affected individuals.
Steps taken to reduce risk of harm to individuals	• The Organization immediately investigated and rectified the problem with the scheduler so the information was no longer available on the internet. • The Organization developed a strong internal booking system that only people within the Organization could access. • The booking system is protected by individual usernames and passwords for each clinic. • Every 30 days, the scheduler is updated and client bookings for the previous 30 days are removed. • Head office and the marketing department do weekly checks of client names and telephone numbers from the scheduler to ensure that everyone's information is safe.
Steps taken to notify individuals of the incident	• The Organization followed up with the complainant by telephone after the issue was rectified.

	• The Organization has not notified any other individual whose information appeared in the scheduler at the time the breach was discovered, that the personal information it had about them in the scheduler had been available on the internet. • As a result of the security measures the Organization took to respond to the incident, it advises it is now unable to determine the identity of the individuals whose information may have been exposed on the internet prior to 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.	In assessing the type of harm(s) that may result from the breach the Organization stated that "The type of harm that resulted from the breach was none of the above except for humiliation or embarrassment. That being said, this was a completely isolated complaint that was rectified by our IT department in an immediate fashion. There was no further evidence from the client that it affected her in any way and there is no proof that anyone other than her ever saw the appointment online." The Organization also stated "In our assessment, the level of sensitivity of the information was mild end because the clients name, phone number and general information were published (not address, SIN, credit card information). We do take this seriously and that is why we acted so quickly on our end and dealt with the client's concern immediately." Finally, the Organization stated "We are notifying/reporting as an abundance of caution but we do not feel as though there is a risk of significant harm because this breach was not brought to our attention by any other outside parties and it did not affect the client in a way that would have caused loss of employment, etc. Indeed, it was embarrassing but we did our utmost to remove it immediately after it was reported and safeguards were immediately put into place to ensure that this won't happen again." In my view, a reasonable person would consider that the contact and profile (appointment details) involved in this incident could be used to cause the harms of hurt, humiliation and embarrassment. Previous breach notification decisions issued by my office have found these to be 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	In assessing the likelihood that harm could result from this breach, the Organization stated "The likelihood that harm could result is low because there is no proof that anyone other than the client saw the information on line. Nothing has been reported since and the issue was immediately corrected. Security measures were not in place at the time but were immediately put into place. The

between the incident and the possible harm.	scheduler is now password protected to prevent unauthorized access and any information becoming public online. The information was sensitive (name, mobile number, booking details) but not highly sensitive (address, SIN, credit card info). To our knowledge, the information was exposed for less than 72 hours. There is no evidence of malicious intent or purpose (theft, hacking, malware). The information from the breach could not be used for criminal purposes. Only 1 individial [sic] to our knowledge was affected by the breach." In my view, there is a real risk of significant harm in this case. The Organization cannot determine how long the personal information contained in the scheduler was available on the internet. Its estimation of 72 hours was based on the length of time it took between the time the client notified the Organization that she found her information on the internet, and the time it took to rectify the problem. It does not take into consideration when the information in the scheduler became available on the internet. This increases the risk that other individuals had their personal information in the scheduler accessed on the internet. The protectionary measures undertaken by the Organization after the incident do not assist me in assessing the risk that the personal information contained in the scheduler was accessed by unauthorized third parties while it was available on the internet. The fact that the Organization has not been contacted by any other affected individuals does not mean the information was not accessed or will not be used for unauthorized purposes in the future. The Organization cannot say how many individuals had their personal information exposed on the internet, or determine how long their personal information was exposed for. My decision in this matter is consistent with a number of breach notification decisions previously issued by my Office which have found a real risk of significant harm in circumstances where an organization had no information or evidence that information was accessed without authorization, but could not rule such access out (see by way of example only, P2011-ND-001; P2011-ND-003 at paras. 16-17; P2013-ND-23; P2016-ND-51; P2017-ND-77; P2017-ND-78; P2017-ND-83).
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 personal information involved in this incident could be used to cause the significant harms of hurt, humiliation and embarrassment. Although the Organization believes no other individual was affected by the availability of the personal information being available on the internet, it cannot say with certainty that no one else's information was exposed before the Organization rectified the problem. Nor can the Organization define the length of time the information in the scheduler was available over the internet. The fact that no one else has complained to the Organization does not eliminate the possibility that an unauthorized third party accessed the personal information of individuals in the scheduler while that information was available on the internet.

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

Section 19.1(1) of the Regulation states "Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must …be given directly to the individual". However, pursuant to section 19.1 (2), "…where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

Given this, and pursuant to section 37.1(2) of PIPA which states "… the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate…", **I require the Organization to report to my office within ten (10) days of the date of this decision, that affected individuals have been notified of this incident directly in accordance with the requirements outlined in the Regulation, or, why the Organization believes that direct notification is unreasonable and how it intends to notify affected individuals indirectly.**

Jill Clayton
Information and Privacy Commissioner