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	Kids & Company Ltd. (Organization)
Decision number (file number)	P2017-ND-161 (File #007149)
Date notice received by OIPC	November 23, 2017
Date Organization last provided information	November 24, 2017
Date of decision	December 4, 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 *Personal Information Protection Act* (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"	The incident involved all or some of the following information: • name, • telephone number, and • email address. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from residents of Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization reported that a form on its previous website was hacked, allowing for a list of potential customer/client names, email addresses, and telephone numbers to be leaked and posted on another website (Pastebin).

	• The Organization believes the incident occurred in December 2016. • The incident was discovered on February 22, 2017, when the Organization received an email from a customer stating that the customer's personal information had been posted to Pastebin. • The Organization discovered that approximately 4,000 to 5,000 names, phone numbers and email addresses were hacked and posted on Pastebin.
Affected individuals	The incident affected 4,000 to 5,000 individuals. The number of affected Albertans is unknown.
Steps taken to reduce risk of harm to individuals	• Removed information from Pastebin. • Launched an enhanced IT security and privacy policy. • Created one form where customers can input their contact details. • Secured new website through SSL and anti-phishing scripts. • Up-to-date security measures were implemented.
Steps taken to notify individuals of the incident	None
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 that the incident involved the "Unauthorized release of names, personal phone numbers, and email addressses [sic]. This could result in email hacking from a brute force attack, or spam emails and phishing and unwanted phone calls." I agree with the Organization. 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.
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 "in this case, the names, emails and phone numbers are listed separately, and appear to be unsorted, making it difficult to associate a specific name with a phone number or email." Further, "The information has been removed from Pastebin and so the risk of future email spam and hacking has been minimized, and we have increased our website security so that the information collected on the form adheres to current security standards."

	The Organization also said "This potential for harm is increased by the evidence of malicious intent. However, we believe that the risk has been mitigated as the data is no longer available….Though security measures were in place, the form was hacked at an unknown point in time. During this time, we were in the midst of redeveloping our website with enhanced security protocols." In my view, the likelihood of harm is increased because the incident resulted from deliberate action indicating malicious intent, and the circumstances suggest the information at issue was the target. Although it may be "difficult to associate a specific name with a phone number or email", matching names to emails is not required in order for email addresses to be used to cause the harm of phishing. Although the personal information has been removed from the Pastebin website, the Organization does not know how long it was exposed, or whether or not it was copied or used.

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 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 is increased because the incident resulted from deliberate action indicating malicious intent, and the circumstances suggest the information at issue was the target. Although it may be "difficult to associate a specific name with a phone number or email", matching names to emails is not required in order for email addresses to be used to cause the harm of phishing. Although the personal information has been removed from the Pastebin website, the Organization does not know how long it was exposed, or whether or not it was copied or used.

The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and is required to confirm to my Office, within ten (10) days of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.

Jill Clayton
Information and Privacy Commissioner