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	Hayward Pool Products Canada, Inc. (Organization)
Decision number (file number)	P2021-ND-247 (File #020936)
Date notice received by OIPC	February 24, 2021
Date Organization last provided information	February 24, 2021
Date of decision	December 1, 2021
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 whose personal information was collected in Alberta 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 the following information: • name, • address, • telephone number, • mobile telephone number, • email address, and • information about the customer's purchases and the amount of rebate they received from the Organization in 2020. The information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	• A document containing personal information about customers was intended to be placed in a password-protected secure folder that could only be viewed within the Organization by those with access to it via password. • Inadvertently, the document was placed in a different folder that was not password-protected and whose contents could be viewed online outside of the Organization. • The breach was discovered on February 10, 2021, when a member of the public notified the Organization that he had come across the document while searching for his own email address online. • The Organization immediately investigated the matter, located the document, and took it down on that same date.
Affected individuals	The incident affected approximately 1,626-1,688 individuals, including five (5) individuals whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Took the document down immediately. • Requested immediate removal of the document from Google's search index. • Disabled search engine indexing on any Office-type files and disabled server indexing so that directory-style listing on the web server will be denied. • Notified affected individuals and encouraged them to remain alert for any communications from third parties that reference their relationship with the Organization. • Shifting to using secure file transfer platforms for sharing this type of document, rather than making the document available through a password-protected folder. • Notified the Office of the Privacy Commissioner of Canada
Steps taken to notify individuals of the incident	Affected individuals were notified by letter between February 23, 2021 and February 26, 2021.
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, *There is no indication of any actual or attempted misuse of any of the information contained in the document. Nor does [the Organization] have any information to suggest that anyone other than the individual who notified [the Organization] about this matter has viewed the document. That individual has confirmed that he did not copy the document.*

	Based on the nature of the incident, the possible harms that might occur as a result of the incident could include fraud/phishing emails. In my view, a reasonable person would consider that the contact information, along with email address and information about the individual's transactions with the Organization, could be used to for phishing purposes, increasing vulnerability to identity theft and fraud.
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, *In light of the circumstances discussed above, [the Organization] does not believe that this incident gives rise to a reasonable risk of significant harm to the individuals whose information is contained in the document, and accordingly does not consider this incident to constitute a "breach" as defined in the Alberta Personal Information Protection Act. Nonetheless, [the Organization] is committed to transparency and is serious about protecting its customers' personal information. We are therefore informing the Alberta IPC of this incident and notifying all individuals as a courtesy.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is decreased because the incident did not result from malicious intent. However, the likelihood of harm resulting is increased because the Organization does not know how long the information was exposed publicly and did not confirm the information was not accessed (such as through a review of audit logs). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach.

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.

A reasonable person would consider that the contact information, along with email address and information about the individual's transactions with the Organization, could be used to for phishing purposes, increasing vulnerability to identity theft and fraud.

The likelihood of harm resulting from this incident is decreased because the incident did not result from malicious intent. However, the likelihood of harm resulting is increased because the Organization does not know how long the information was exposed publicly and did not confirm the information was not accessed (such as through a review of audit logs). The lack of reported incidents

resulting from this breach to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach.

I require the Organization to notify the affected individuals whose personal information was collected 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 between February 23, 2021 and February 26, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner