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	Luxottica of America Inc. (Organization)
Decision number (file number)	P2021-ND-117 (File #017942)
Date notice received by OIPC	October 29, 2020
Date Organization last provided information	October 29, 2020
Date of decision	April 27, 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 eyewear and eye care corporation that owns optical retail locations across the country, including in Alberta. The Organization also acts as a service provider to other eye care practices in various provinces. 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: • full name, • appointment information, • contact information, and • notes from a health care professional (medical diagnoses or conditions relating to eye care). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On August 9, 2020, an automated attack was carried out against the Organization's appointment scheduling application using an account that was created on August 5, 2020. • The Organization investigated to determine the extent and nature of the incident and to confirm whether patient records had been accessed and/or acquired. • On August 28, 2020, the Organization preliminarily concluded that the unauthorized person might have accessed and acquired personal information from the appointment scheduling application.
Affected individuals	The incident affected 4,898 individuals residing in Alberta
Steps taken to reduce risk of harm to individuals	• Investigated and took the scheduling application offline to remediate the issue and ensure the security of systems. • Worked with third-party cybersecurity specialists to determine the full nature and scope of the event. • Took measures to enhance security controls and prevent similar incidents, including implementing additional access restrictions on the appointment-scheduling platform. • Notified U.S. federal law enforcement.
Steps taken to notify individuals of the incident	The Organization notified affected individuals by mail and email, beginning October 27, 2020. On September 28, 2020, the Organization provided notice to impacted practices for whom it acts as a service provider. Additionally, the Organization provided conspicuous notice via newspaper publications.
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: *We do not believe this incident poses a significant risk of harm to individuals. Our conclusion is based on: the types of information accessed by the attacker; no evidence of misuse of personal information or harm to patients as a result of this incident; the low likelihood that the incident will adversely affect the provision of health services to the impacted individuals; the low likelihood of identity theft and fraud; and the low likelihood of embarrassment, physical, mental or financial harm or damage impacting individuals' reputations.* The Organization's notice to affected individuals said: *You should always remain vigilant, including by regularly reviewing your account statements. If you discover any suspicious or unusual activity on your accounts or if you suspect*

	identity theft or fraud, be sure to report it immediately to your health plan or insurer In my view, a reasonable person would consider that the contact information, if it includes email addresses, could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Medical information could be used to cause embarrassment and humiliation. These are 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 between the incident and the possible harm.	The Organization reported that it has "…no evidence of misuse of personal information or harm to patients as a result of this incident". In my view, a reasonable person would consider 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 lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing, identity theft, fraud and embarrassment 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, if it includes email addresses, could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Medical information could be used to cause embarrassment and humiliation. These are significant harms. 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 lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing, identity theft, fraud and embarrassment can occur months and even years after a data breach.

I require the Organization to notify the affected individuals whose 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 mail and email, beginning October 27, 2020 and also provided conspicuous notice via newspaper publications. On September 28, 2020, the Organization provided notice to impacted practices for whom it acts as a service provider. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner