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	New England College of Optometry (Organization)
Decision number (file number)	P2017-ND-13 (File #000995)
Date notice received by OIPC	June 16, 2015
Date Organization last provided information	June 16, 2015
Date of decision	January 9, 2017
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	This incident involves the following information: • name, • credit card number, expiry date, and security code (CVV). This information is about an identifiable individual 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 or around May 11, 2015, the Organization learned that a recently departed employee hired through a staffing agency stole and used some credit card numbers without authorization. • The Organization believes the individual may have had access to credit card information between October 2014 and May 2015, and may have physically written down or copied credit card information.

	• The Organization does not believe its computer systems, point of sale systems, or any electronic systems were breached or subject to any unauthorized access.
Affected individuals	The incident affected one (1) resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Initiated internal investigation. • Reviewed data security practices and put additional protections in place to ensure the security of all personal information collected. • Notified law enforce enforcement, Massachusetts Attorney General's office and other regulators.
Steps taken to notify individuals of the incident	Written notice of the incident was mailed to the affected individual on June 9, 2015.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 its report of the breach, the Organization did not specifically identify any potential harm that might result to from the incident. However, the Organization did advise that it would be "providing each individual with further information on how to protect against identity theft and fraud." In my view, the information at issue could be used to cause the harms of identity theft and fraud. 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 did not assess the likelihood of harm resulting from this incident. In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (theft of credit card information) and the information was exposed for approximately 7 months.
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 as a result of this incident. The information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (theft of credit card information) and the information was exposed for approximately 7 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 that written notice of the incident, in compliance with the Regulation, was mailed to the affected individual on June 9, 2015. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner