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	Quality Credit Services Limited (doing business as "Quality Credit Reporting") (Organization)
Decision number (file number)	P2018-ND-126 (File #009638)
Date notice received by OIPC	September 6, 2018
Date Organization last provided information	September 6, 2018
Date of decision	September 26, 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 affected individuals 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 licensed to do business in Alberta and the affected individuals are located in Alberta. 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: • contact information, • date of birth, • Social Insurance Number, and • financial information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The individuals affected by this incident are located in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• The affected individuals are prospective franchisees of a franchisor who retained the Organization to provide credit reports in connection with the credit applications of those prospective franchisees. The prospective franchisees are spouses.

	• On August 28, 2018, an employee of the Organization emailed the prospective franchisees to advise that the franchise credit applications had been received and that the credit report process was underway. • The employee attached the prospective franchisees' credit applications to the email. Even though the information in the credit applications was provided by the franchisees, sending the information back to the franchisees is not an approved procedure. • The mistake was compounded because the employee who sent the email mistyped the email address of one of the prospective franchisees. As a result, the information in the credit applications was misdirected with the potential for unauthorized disclosure if the misdirected email was received and opened. • The incident was discovered when it was reported to the Organization by one of the prospective franchisees on August 29, 2018.
Affected individuals	The incident affected 2 individuals.
Steps taken to reduce risk of harm to individuals	• Attempted to recall the email containing the credit reports. • Investigated to determine whether the email may have "bounced back" due to the incorrect email address. Unfortunately, the email appears to have been delivered. • Sent another email to the incorrect email address to instruct that the information should be deleted. Unfortunately, there has been no response. • Interviewed the employee to determine what occurred and to provide reinstruction on appropriate practices. • Obtained internal approval to provide credit monitoring and identity theft protection products. • Initiated a policy review, including employee re-education, in order to implement lessons learned from this incident. • Advised the affected individuals that the Organization intended to cover the costs of one-year of credit monitoring and identity theft.
Steps taken to notify individuals of the incident	Notified one of the affected individuals orally on August 30, 2018 and made a written individual breach notification report to each of the prospective franchisees separately on September 4, 2018.

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 "The information at issue is sensitive and could be used for phishing or identity theft purposes if obtained by a criminal actor." I agree with the Organization's assessment. The contact, identity and financial information at issue could be used to cause the significant harms of fraud, identity theft, and phishing.
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 "The potential unauthorized disclosure of personal information was the result of inadvertence and failure to follow company procedures. [The Organization] was not able to confirm that the email was received or opened. Although the risk of misuse appears to be low, it is not possible to rule out all risk." I agree with the Organization that the likelihood of harm resulting from this incident is reduced because the breach was the result of human error and not malicious activity. However, the Organization does not know to whom the information was disclosed and was not able to recover it or obtain an undertaking from the unauthorized recipient confirming the information was not viewed, used, or further disclosed.

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, identity and financial information at issue could be used to cause the significant harms of fraud, identity theft, and phishing. The likelihood of harm resulting from this incident is reduced because the breach was the result of human error and not malicious activity. However, the Organization does not know to whom the information was disclosed and was not able to recover it or obtain an undertaking from the unauthorized recipient confirming the information was not viewed, used, or further disclosed.

The Organization is required 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 that the Organization notified one of the affected individuals orally on August 30, 2018 and made a written individual breach notification report to each of the prospective franchisees separately on September 4, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner