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	Rifco National Auto Finance Corporation (Organization)
Decision number (file number)	P2020-ND-184 (File #016778)
Date notice received by OIPC	March 20, 2020
Date Organization last provided information	March 20, 2020
Date of decision	December 8, 2020
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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • email address, • loan account number, and • outstanding loan balance. This information is about an identifiable individual 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 March 11, 2020, an employee of the Organization was corresponding with a customer by email and inadvertently used an email string that contained another customer's personal information. • On March 13, 2020, the customer who received the information in error alerted the Organization and provided a copy of the email she had received.

Affected individuals	The incident affected one individual.
Steps taken to reduce risk of harm to individuals	• Notified the affected individual. • Reviewed privacy guidelines with the employee and provided additional training.
Steps taken to notify individuals of the incident	The affected individual was notified by email on March 20, 2020.
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 information shared is insufficient to allow for identity theft or financial fraud. The customer may feel personal embarassment [sic] that a third party is aware of personal struggles". In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft and fraud, as well as potentially hurt, humiliation and embarrassment. Email address could be used for phishing purposes, increasing vulnerability to 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 reported that "Harm is unlikely as the third party has done nothing with the actual information but is demanding compensation from [the Organization]". In my view, a reasonable person would consider the likelihood of harm resulting in this case is reduced as the incident did not result from malicious intent, but rather human error, and the unintended recipient reported the error. However, the Organization did not report on efforts to ensure that the information was destroyed and not used or further disclosed, nor did it report whether there was any personal/professional relationships between the affected individual and the unintended recipient. Further, the fact the third party "is demanding compensation" increases the likelihood of harm resulting.
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 individual. A reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft and fraud, as well as potentially hurt, humiliation and embarrassment. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.	

The likelihood of harm resulting in this case is reduced as the incident did not result from malicious intent, but rather human error, and the unintended recipient reported the error. However, the Organization did not report on efforts to ensure that the information was destroyed and not used or further disclosed, nor did it report whether there was any personal/professional relationships between the affected individual and the unintended recipient. Further, the fact the third party "is demanding compensation" increases the likelihood of harm resulting.

I require the Organization to notify the affected individual, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual by email on March 20, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner