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 (Organization)
Decision number (file number)	P2021-ND-046 (File #17458)
Date notice received by OIPC	April 14, 2020
Date Organization last provided information	April 14, 2020
Date of decision	March 2, 2021
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 operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported the incident involved the following information: • name, • cell phone number, • email address, and • account number. The Organization's report of the breach also says the information disclosed in error includes that the customer account "is in collections". 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 April 3, 2020, an employee was conversing by email with a customer but inadvertently used the ongoing email thread in an email to a different customer. • The employee who made the error reported it to a supervisor. • The customer who received the information in error was contacted and agreed to delete the email. • The breach was discovered on April 4, 2020.
Affected individuals	The incident affected one resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Reported the error to a supervisor. • Contacted the customer who received the information in error; the customer agreed to delete the email.
Steps taken to notify individuals of the incident	The affected individual was notified by email on April 14, 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 "The information shared is insufficient to allow for identity theft or financial fraud. The customer may feel personal embarassment that a third party is aware of the account is in collections". In my view, a reasonable person would consider the financial information (account number and that the account is in arrears) could be used to cause the harms of embarrassment and damage to reputation if the affected individual and the unauthorized recipient are known to each other. 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, the likelihood of harm resulting from this incident is decreased because the incident resulted from human error and not malicious intent and because the unauthorized recipient agreed to delete the information. However, it is not known if the unauthorized recipient and the affected individual are known to each other; further, the fact the unauthorized recipient is "demanding compensation" suggests the individual may not have deleted the information and may use it for some harmful purpose.

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 the financial information (account number and that the account is in arrears) could be used to cause the harms of embarrassment and damage to reputation if the affected individual and the unauthorized recipient are known to each other. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is decreased because the incident resulted from human error and not malicious intent and because the unauthorized recipient agreed to delete the information. However, it is not known if the unauthorized recipient and the affected individual are known to each other; further, the fact the unauthorized recipient is "demanding compensation" suggests the individual may not have deleted the information and may use it for some harmful purpose. 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 dated April 14, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner