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)	P2020-ND-006 (File #013754)
Date notice received by OIPC	October 25, 2019
Date Organization last provided information	October 25, 2019
Date of decision	February 11, 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 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 "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • telephone number, • email address, • account number, and • arrears 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 September 13, 2019, an employee was conversing by email with a customer, and inadvertently used the ongoing email string in an email to a different customer.

	• The incident was discovered on October 21, 2019 when it was reported by the unintended recipient, who also provided a copy of the email at issue to the Organization.
Affected individuals	The incident affected one (1) individual.
Steps taken to reduce risk of harm to individuals	Reviewed Privacy guidelines with the employee and provided additional training.
Steps taken to notify individuals of the incident	The affected individual was notified by letter on October 25, 2019.
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 [sic] that a third party is aware of personal struggles." In my view, a reasonable person would consider that the financial information at issue (account number and arrears balance) could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud.
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 "Harm is unlikely as the third party has had the information for over a month and has done nothing with the information". In my view, the likelihood of harm resulting from this incident is decreased because the incident was not the result of malicious action but rather human error, and the incident was reported by the unintended recipient. 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. Lastly, it is not clear why the unintended recipient took over a month to report the incident to the Organization.
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 financial information at issue (account number and arrears balance) could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation and embarrassment. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud.

The likelihood of harm resulting from this incident is decreased because the incident was not the result of malicious action but rather human error, and the incident was reported by the unintended recipient. 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. Lastly, it is not clear why the unintended recipient took over a month to report the incident to the Organization.

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 letter on October 25, 2019. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner