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 Finance Corporation (Organization)
Decision number (file number)	P2017-ND-80 (File #005787)
Date notice received by OIPC	June 2, 2017
Date Organization last provided information	June 2, 2017
Date of decision	June 19, 2017
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • email address, and • information that a loan payment had been missed. The information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The incident occurred in Alberta and affected residents of Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On May 31, 2017, an employee of the Organization sent an email message to the email addresses of approximately 300 customers. • The email informed customers that their account was in arrears and requested they contact the Organization immediately in order to resolve the missed payment.

	• The email addresses of all recipients were included in the "To" address line instead of the intended "BCC" address line, inadvertently disclosing the email addresses to all of the recipients. • The Organization learned of the incident the same day when it received a call from one of the email recipients. • Approximately 25 of the email messages were reported as undeliverable.
Affected individuals	The incident affected approximately 275 individuals.
Steps taken to reduce risk of harm to individuals	• Sent an Outlook recall request to all affected email addresses. • Suspended all batch email functions to customers and initiated re-training. • Followed up with the employee who sent the email. • Implementing new internal systems to prevent reoccurrence.
Steps taken to notify individuals of the incident	Affected individuals received an email notification and apology on May 31, 2017.
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 potential harm includes the possibility of customers receiving unsolicited emails. Individuals may be embarrassed that other individuals may know that they are 'behind on their account'. The limited and specific information in the email would make it very difficult for identity theft to occur." I agree with the Organization. Email addresses could be used to cause the harm of phishing. The profile information at issue (that customers were behind on their payments) could be used to cause the harms of hurt, humiliation and embarrassment. 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.	In assessing the likelihood of harm resulting from this incident the Organization noted that "The email was distributed to only people who were in the same position (so no 'outsiders' were sent the message); however customer email addresses and the corresponding message could be re-distributed." Further, the email messages "contained a confidentiality disclosure at the bottom of the message." The incident was the result of human error, rather than malicious intent and the Organization acted quickly in responding by implementing mechanisms to prevent reoccurrence and to notify affected individuals. In addition, the Organization reported "The "Recall" feature in Microsoft Outlook was utilized to delete unread copies of the email message."

	In my view, there is a real risk of harm resulting from this incident. Although the incident was not the result of malicious intent but rather human error, and the Organization acted quickly in responding, the information was nonetheless sent to approximately 300 unintended recipients increasing the likelihood that some professional or personal relationship exists between the affected individuals and the unintended recipients such that hurt, humiliation and embarrassment could result. The Organization was unable to recall all of the email messages. It is not possible for the Organization to ensure the personal information will not be further used or distributed.

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. Email addresses could be used to cause the harm of phishing. The profile information at issue (that customers were behind on their payments) could be used to cause the harms of hurt, humiliation and embarrassment. These are significant harms. Although the incident was not the result of malicious intent but rather human error, and the Organization acted quickly in responding, the information was nonetheless sent to approximately 300 unintended recipients increasing the likelihood that some professional or personal relationship exists between the affected individuals and the unintended recipients such that hurt, humiliation and embarrassment could result. The Organization was unable to recall all of the email messages. It is not possible for the Organization to ensure the personal information will not be further used or distributed.

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 affected individuals received an email notification and apology on May 31, 2017. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner