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	Raintree Financial Solutions (Organization)
Decision number (file number)	P2016-ND-52 (File #002907)
Date notice received by OIPC	May 11, 2016
Date Organization last provided information	June 1, 2016
Date of decision	August 25, 2016
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 is incorporated and licenced under the Alberta *Insurance Act* to carry on business 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 following information is involved: • email address, • general correspondence. Some or all of the following information may be involved: • Social Insurance Number, • driver's license number, and • credit card information. This information is about identifiable individuals 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 14, 2016, an employee's email account was breached and a phishing based email was sent to the employee's contact list, encouraging recipients to enter their email account log in information. • A number of recipients immediately contacted the Organization to report the suspicious activity.
Affected individuals	Approximately 150-200 residents of Alberta were affected.
Steps taken to reduce risk of harm to individuals	• The breached email account was reset within one hour of the breach occurring. • All other account holders also had their accounts reset within 24 hours of the incident.
Steps taken to notify individuals of the incident	Notification sent by email to suspected affected individuals on March 14 and 15, 2016.
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 recognized the affected individuals may be at risk for phishing. I agree with the Organization's assessment. The compromised email addresses could be used for phishing purposes. In addition, if sensitive identity and financial information was compromised, it could be used to cause the harms of 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 did not specifically assess the likelihood of harm resulting from the breach but noted the employee's contacts could be "vulnerable to the same attack." In my view, the likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate unauthorized access) and the compromised information was used to send phishing emails.

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 compromised email addresses could be used for phishing purposes. In addition, if sensitive identity and financial information was compromised, it could be used to cause the harms of identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate unauthorized access) and the compromised information was used to send phishing emails. I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified the affected individuals via email on March 14 and 15, 2016, in accordance with the Regulation. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner