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	National Bank Investments (Organization)
Decision number (file number)	P2017-ND-121 (File #003753)
Date notice received by OIPC	September 13, 2016
Date Organization last provided information	March 30, 2017
Date of decision	August 11, 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 is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • account number, and • transaction amount. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the information concerns residents of Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization reported "The incident resulted in a breach of our electronic files and a number of files being accessed on September 6 [2016] by an unauthorized party outside our organization." • The incident was discovered on September 7, 2016.

Affected individuals	The incident affected 106 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Validated the unauthorized third party no longer had access to documents and secured the environments. • Shared potential client impact with other constituents, such as Financial Institutions, Public Entities and Regulators and Payment Networks. • Tightened authentication procedures and other preventive security measures. • Notified affected individuals in writing and were advised to remain vigilant, review and monitor their account statements for suspicious activity. • Reviewed internal protocols to ensure proper access restrictions are in place. • Notified RCMP September 9, 2016.
Steps taken to notify individuals of the incident	Notified clients and intermediary dealers (if applicable) starting September 12, 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 reported "Given the actions taken and the nature of the information (no SIN, no credit card information, no email address), we assess that there is no real risk of significant harm. Furthermore, we have no indication to the effect that the information has been misused." The Organization later reported that "six months since the breach, it has not been informed of any harms or losses." In my view, the financial information at issue could be used to cause identity theft, fraud, and financial loss. 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.	As noted, the Organization reported "…we assess that there is no real risk of significant harm. Furthermore, we have no indication to the effect that the information has been misused." The Organization also said "Taking into consideration the measures put in place, we believe the likelihood of harm was very remote. It could not have been significant. By adding security notes in our internal systems in order to tighten our authentication procedures, our staff is required to take additional precautions in order to make sure the transaction is initiated by the concerned client."

	In my view, the likelihood of harm in this case is increased because the incident appears to be the result of malicious intent (access to files by an unauthorized party). Although the Organization has put additional precautions in place to ensure transactions are initiated by the client, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from the Organization's systems were to be used for fraudulent purposes, for example.

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 financial information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. The likelihood of harm in this case is increased because the incident appears to be the result of malicious intent (access to files by an unauthorized party). Although the Organization has put additional precautions in place to ensure transactions are initiated by the client, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed from the Organization's systems were to be used for fraudulent purposes, for example.

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 the Organization notified affected individuals in Alberta starting on September 12, 2016. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner