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	Kinsted Wealth (Organization)
Decision number (file number)	P2019-ND-074 (File #012050)
Date notice received by OIPC	February 15, 2019
Date Organization last provided information	February 15, 2019
Date of decision	June 4, 2019
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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following types of information may be at issue for 409 clients: • name, • social insurance number, • date of birth, • contact information, • Organization custody account number and assets under management. The following types of information may be at issue for 386 clients: • contact information, • Organization custody account number and assets under management. 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 January 23, 2019, a phishing email was sent to the Organization's employees. • One employee opened the email and, as a result, the attacker gained access to client information in that employee's email contact file. • The attacker then sent out phishing emails to a limited number of clients from the employee's contact list.
Affected individuals	The incident affected 767 Canadians, including 719 in Alberta.
Steps taken to reduce risk of harm to individuals	• Contacted IT support and sent a message to all employees advising against opening any suspicious emails. • Notified all affected clients about the phishing email and warned them not to open it. • Initiated an investigation to identify and assist affected individuals. Retained IT consulting firm and an IT forensic firm to assist in the investigation. • Providing affected individuals with access to credit monitoring services for 2 years. • Notifying relevant Privacy Commissioners.
Steps taken to notify individuals of the incident	All affected individuals were notified by letter dated February 13, 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 that "The most pressing risk of harm is with respect to identify theft" and "Affected individuals have further been counselled to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports". In my view, a reasonable person would consider that contact, identity and financial information, could be used to cause the significant harms of fraud and identity theft. To the extent contact information includes email addresses, this information 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 that "While we view the risk to be relatively low, namely because we have engaged two IT firms (one of the firms being a forensic firm) and we have uncovered no evidence of accessing the data at issue, we have provided the affected individuals with information and resources to help them protect and monitor their information for any potential unauthorized activity".

	In my view, a reasonable person would consider that the likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (deliberate action by unknown and unauthorized third party) and additional phishing emails were sent. The information has not been recovered.

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.

A reasonable person would consider that contact, identity and financial information, could be used to cause the significant harms of fraud and identity theft. To the extent contact information includes email addresses, this information could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (deliberate action by unknown and unauthorized third party) and additional phishing emails were sent. The information has not been recovered.

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 were notified by letter dated February 13, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner