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	Investia Financial Services Inc. (Organization)
Decision number (file number)	P2018-ND-070 (File #008698)
Date notice received by OIPC	May 17, 2018
Date Organization last provided information	May 17, 2018
Date of decision	July 4, 2018
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"	For the 2 affected clients in Alberta, the redirected emails contained the following information: • name (first and last), • address, • email address, • telephone number, • investment companies, type, account number, history and balance of investments, • bank account information, and • signature. 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 April 19, 2018, the Organization was made aware that the email address used by an employee of two mutual fund representatives was compromised by malware and emails exchanged with 22 individuals (18 client accounts) were redirected to two unknown email addresses. • The representatives discovered the incident on April 6, 2018 when an owner of the company was informed that an employee was not receiving emails on her desktop and on her Office 365 account. That same day, an investigation was conducted and the unknown email address was identified. • The cause of the incident remains unclear; it is suspected that the employee clicked on a phishing email with a malicious link or attachment, or on a malicious link within a Google Chrome browser window. • The emails were redirected between March 26, 2018 and April 6, 2018.
Affected individuals	The incident affected 20 clients located in British Columbia and 2 who are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Contacted the affected clients to inform them and to make sure that they monitor their accounts with other financial institutions to detect potential unusual activities. • Modified client account numbers and implemented security measures to monitor unusual transactions. • Notified fund companies to prevent direct trading, implement enhanced identification verification and ensure that any request to modify banking information or redeem mutual fund shares or units is confirmed prior to proceeding. • Flagged client files to ensure proper client identification and security questions are confirmed with clients prior to discussing or reviewing account information. • Offered affected individuals credit monitoring service. • Cleaned and reformatted the affected computer and secured the impacted email account. • Enhanced authentication. • Providing staff training on the measures to take in order to protect the privacy of their clients. • Will review privacy and IT security procedures to determine where improvements can be made.
Steps taken to notify individuals of the incident	Affected individuals were contacted by telephone and letters were sent on or around May 3, 2018

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 following types of harm could result from the breach: *- Fraud* *- Identity Theft* *- Credit record* *- Stress and time consuming effects* The Organization also said the information "…could be used to identify the Affected clients … and create financial prejudice". Further, "The personal information that was compromised could result in significant harm as it might be used to conduct criminal activies [sic] such as fraud and identity theft by the third party to whom the malware was directing emails". I agree with the Organization's assessment. The contact and financial information could be used to cause the significant harms of identity theft, fraud and negative effects on a credit record. Email addresses could be used to cause the significant harm of phishing.
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 its assessment of the likelihood of harm resulting from this incident, the Organization identified the following: *a. An unauthorized third party obtained access to the information contained in the emails.* *b. The computer of the employee was encrypted and pasword-protected [sic].* *c. The information is highly sensitive (DOB, SIN, Residential addresses, banking and financial informations).* *d. There are evidence of malicious intent (malware).* *e. The information may be used for criminal purposes, such as identity theft or fraud.* *f. The emails that were redirected are still in possession of the unauthorized third party.* *g. Eighteen (18) …client accounts were affected by the breach of privacy; two (2) of which were residents of Alberta.* In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and misdirection of email), and 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 as a result of this incident.	

The contact and financial information could be used to cause the significant harms of identity theft, fraud and negative effects on a credit record. Email addresses could be used to cause the significant harm of phishing. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and misdirection of email), and 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 contacted by telephone and letters were sent on or around May 3, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner