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	Investors Group Financial Services Inc. (Organization)
Decision number (file number)	P2020-ND-058 (File #014931)
Date notice received by OIPC	January 22, 2020
Date Organization last provided information	January 22, 2020
Date of decision	May 29, 2020
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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • age, • date of birth, • account number, and • investment holdings. 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 December 16, 2019, while the Organization's clients were on vacation, a hacker gained access to the clients' (husband and wife) email account and then proceeded to pose as the wife and called the Organization's consultant to request the clients' statements.

	• Upon receiving this request, the Consultant provided a copy of the statements (one for the husband's account, and one for the wife's account) to the hacker. • On December 17, 2019, the hacker emailed the consultant asking for information on how to redeem some assets from the account. • Between December 17, 2019 and January 6, 2020, the consultant and the hacker exchanged emails. The consultant informed the hacker that validation of identity was required and to confirm the instructions. • The consultant made several attempts to confirm the identities of the clients, and was concerned with his inability to speak with them directly. • The consultant decided to check Facebook and saw that the clients were on vacation. • The advisor messaged the husband through Facebook where the husband confirmed they had not contacted the consultant nor did they ask for a redemption by email. • The consultant informed the clients of the requests he received by email and that their email account was compromised.
Affected individuals	Two individuals were affected by the incident.
Steps taken to reduce risk of harm to individuals	• Notified clients of the incident. • Created new accounts with new account numbers. • Flagged the account. • Informed clients to inform their email provider to lock their compromised email account and to contact their financial institutions. • Will verify requests to share information by telephone with the clients.
Steps taken to notify individuals of the incident	Affected individuals were notified by Facebook messages on January 6, 2020 and formally via a new email address on January 21, 2020.
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: *There is a limited possibility that the hacker may utilize the information in the statement in conjunction with any other information that they may have found within the clients' email account to contact other financial institutions that service the clients.*

	In my view, a reasonable person would consider that the identity and financial information at issue could be used for identity theft, fraud, or 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.	The Organization reported that, *Since new accounts and account numbers were established and flags were immediately placed on the new accounts to mitigate the risk of being improperly accessed, there is very limited likelihood that harm will occur as a result of the statements being disclosed. The impacted individuals have not suffered any financial losses to their [Organization] accounts and are unlikely to suffer financial losses to their [Organization] accounts as a result of the actions taken by the Consultant and the firm in response to the incident.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate actions by a third party). Although the Organization has put additional safeguards in place, 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. The fact no financial loss has been reported to date is not a mitigating factor, as identity theft can happen months and even years after a data breach.

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 the identity and financial information at issue could be used for identity theft, fraud, or financial loss. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate actions by a third party). Although the Organization has put additional safeguards in place, 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. The fact no financial loss has been reported to date is not a mitigating factor, as identity theft can happen months and even years after a data breach.

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 the affected individuals by Facebook messages on January 6, 2020 and formally via a new email address on January 21, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner