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)	P2018-ND-115 (File # 007361)
Date notice received by OIPC	December 20, 2017
Date Organization last provided information	February 23, 2018
Date of decision	August 13, 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 is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • social insurance number, • date of birth, • estimation of financial worth, • account holdings, • void cheques, • old client application forms, and • personal financial reviews. 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 1, 2017, the Organization was broken into. Several employee laptops and one paper file in a briefcase were stolen. • The thieves broke into a fireman's access box located on the outside of the building and used the contents from the access box to get into the building. The firebox belonged to the landlord of the building. • The incident was discovered by staff upon arriving for work. • The Organization said the stolen laptops were protected by encryption and strong password requirements.
Affected individuals	The incident affected 2 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Notified clients whose client file was stolen. • Offered reimbursement for credit monitoring services. • Tagged client accounts with confidentiality alerts. • The landlord replaced and upgraded the lock box on the exterior of the building.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on December 13, 2017.
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 "one potentially [sic] type of harm that could result is identity theft for the clients whose personal information was stolen in paper format from the client file" and "We consider the potential harm to be significant because the personal information could be used to commit identity theft (e.g. applying for a credit card in the name of the clients)." Further, the Organization reported that "The laptops themselves however were protected by encryption and strong password requirements so we don't consider this to be a potential harm to our clients." I agree with the Organization's assessment. The identity and financial information contained within the paper file could be used to cause the significant harms of identity theft and fraud. Because the laptops were encrypted and had strong password protection, in my view, any personal information on the laptops could not be used to cause harm to the affected individuals.

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 "We do not consider it likely that harm will result. This is because the targets of the theft were laptops that could be easily erased and sold for a quick profit by the thieves (although we are only guessing at their motive). These laptops were protected by encryption and strong password requirements. We also do not consider it likely that harm will result because other client files within the office were untouched by the thieves and no other client files were noticed missing after the incident was discovered and after the office was searched." In my view, the likelihood of harm resulting from this incident is increased because the personal information in the briefcase was compromised due to the malicious action of an unknown third party (stolen along with the laptop). Further, the information has not been recovered. Although the Organization does not believe the information was the target of the theft, it is impossible to know this for sure.

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 identity and financial information contained within the paper file could be used to cause the significant harms of identity theft and fraud. Because the laptops were encrypted and had strong password protection, any personal information on the laptops could not be used to cause harm to the affected individuals. The likelihood of harm resulting from this incident is increased because the personal information in the briefcase was compromised due to the malicious action of an unknown third party (stolen along with the laptop). Further, the information has not been recovered. Although the Organization does not believe the information was the target of the theft, it is impossible to know this for sure.

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 a letter dated December 13, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner