



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Financial Strategies Group (Organization)
Decision number (file number)	P2022-ND-076 (File #023131)
Date notice received by OIPC	June 30, 2021
Date Organization last provided information	June 22, 2022
Date of decision	January 10, 2023
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 whose personal information was collected in Alberta pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (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”	<p>The incident involved some or all of the following information:</p> <ul style="list-style-type: none">• name,• address,• phone number,• personal identification,• banking information, and• life insurance policy information and applications. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p>
DESCRIPTION OF INCIDENT	
<input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On June 16, 2021, the Organization’s office was broken into.• Staff discovered the incident when they arrived to the office on June 17, 2021.• Several paper life insurance files were stolen.• The desktop computer was stolen. It was password-protected.

	<ul style="list-style-type: none"> • The technology systems are encrypted. • Only one stolen cheque was recovered. • There is a potential that the thieves were able to view personal information in the stolen files.
Affected individuals	The incident affected 11 individuals.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Reported the incident to the police. • Contacted MFDA dealer, MGA life insurance dealer, and various insurers. • Changed passwords to online accounts. • Upgraded security system. Doors repaired and rekeyed. Improved security systems on office technology (server, computers), changed passwords on devices and online accounts.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally between June 17, 2021 and June 23, 2021.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>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.</p>	<p>The Organization reported the possible harms that may occur as a result of the breach are “Identity theft or financial fraud possibly.”</p> <p>I agree with the Organization’s assessment. A reasonable person would consider the contact, identity and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. These are significant harms.</p>
<p>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.</p>	<p>The Organization reported the likelihood that the harm will result is “Unknown.”</p> <p>In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased, as it was the result of malicious intent (break-in). The laptop was password protected, but the Organization did not report that it was encrypted. Only one stolen cheque was recovered. The desktop computer and the life insurance files have not been recovered.</p>
DECISION UNDER SECTION 37.1(1) OF PIPA	
<p>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.</p> <p>Contact, identity and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. These are significant harms.</p>	

The likelihood of harm resulting from this incident is increased, as it was the result of malicious intent (break-in). The laptop was password protected, but the Organization did not report that it was encrypted. Only one stolen cheque was recovered. The desktop computer and the life insurance files have not been recovered.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individuals were notified verbally between June 21, 2021 and June 23, 2021. The Organization is not required to notify the individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance