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	GoldSilver, LLC (Organization)
Decision number (file number)	P2019-ND-051 (File #011277)
Date notice received by OIPC	December 21, 2018
Date Organization last provided information	December 21, 2018
Date of decision	May 2, 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 whose personal information was collected in Alberta, 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, • financial account information, and • passport number (for 2 Alberta residents). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On November 20, 2018, the Organization was alerted to a potential security incident in which an attacker demanded an extortion payment or he would release certain customer information obtained from the Organization's systems. • The investigation determined that an unauthorized person obtained access to a database containing certain customer records between September 28, 2018 and November 20, 2018.

Affected individuals	The incident affected 13,248 individuals, including 15 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Took steps to secure the system, investigate the credibility of the claim, and engaged a forensic computer security firm to assist in the investigation. • Requested assistance from the FBI. • Deactivated the individuals' account credentials and prompted the individuals to create a new password when they log in. • Implementing additional procedures to further expand and strengthen the security of their system.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent December 19, 2018.
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 "Unauthorized charges may be made an an [sic] individuals' account. The risk for harm is minimized because the database did not include routing numbers for the financial accounts". I accept the Organization's assessment. A reasonable person would consider that the financial information and identity information (for 2 resident of Alberta) at issue could be used to cause the significant harms of identity theft, fraud and financial loss (including making unauthorized charges on an account).
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 "Unauthorized charges to an account require information beyond the individuals' name and account number. [The Organization] has provided notice to the individuals and advised them to review their financial statements and credit reports for any unauthorized activity, and to immediately report any unauthorized charges to their financial institution. Thus, potential harm is not likely to be significant." In my view, a reasonable person would consider the likelihood of harm resulting in this case to be increased as the personal information was compromised due to malicious action that resulted in an extortion demand. The information may have been exposed for almost 2 months. The Organization did not report that the information was recovered, nor any information concerning whether the information may have been used or further disclosed.
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 financial information and identity information (for 2 resident of Alberta) at issue could be used to cause the significant harms of identity theft, fraud and financial loss (including making unauthorized charges on an account). The likelihood of harm resulting in this case is increased as the personal information was compromised due to malicious action that resulted in an extortion demand. The information may have been exposed for almost 2 months. The Organization did not report that the information was recovered, nor any information concerning whether the information may have been used or further disclosed.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individuals were notified by letter sent December 19, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner