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	Silverberg & Associates Inc. (Organization)
Decision number (file number)	P2021-ND-289 (File #006835)
Date notice received by OIPC	October 11, 2017
Date Organization last provided information	December 9, 2017
Date of decision	February 25, 2022
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the 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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information of an employee and his family: • name and address, • social insurance number, • Nexus information (passport numbers, date of birth and contact information), • banking information (for the employee). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization also reported that personal information of employees of some corporate clients may have been at issue (name, salary, medical information for one individual); however, in respect of this information, the Organization is a service provider to its corporate clients and is not the organization with the responsibility to report this incident under section 34.1 of PIPA, or to notify affected individuals.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On October 4, 2017, an employee of the Organization noticed that a suspicious email seemed to have originated from his email account. • The employee opened his email account from his desktop and noticed that someone else seemed to have control of his computer. • The perpetrator deleted some of the employee's contacts, and sent and deleted folders, and also sent a phishing email to the employee's contacts. • The email account was secured on October 4, 2017. Although emails were deleted, it is not known if they were viewed or copied.
Affected individuals	The Organization reported that 4 individuals in Alberta were affected (1 employee and his 3 family members).
Steps taken to reduce risk of harm to individuals	• Terminated the intruder's administrator-level access to the employee's computer. • Computer systems were isolated and all potentially compromised passwords were changed. • All computers were scanned for malware and none was found. • IT consultants were used to stop the attack and scan all systems for possible malware.
Steps taken to notify individuals of the incident	The Organization reported that the incident was discovered by the affected individual, who was fully aware of the incident.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to those 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 harms that might result to the affected individual include "Finncial loss [sic].... and identity theft". 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 significant harms of identity theft and fraud. Email addresses could be used for phishing purposes.

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 it does "... not believe the harm is significant for anyone except [the employee] as a result of his prsonal [sic] information possiblely [sic] being accessed." In my view, a reasonable person would consider the risk of harm is increased as the incident resulted from malicious intent (deliberate action to takeover the email account), and because phishing emails were sent.

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 individual and his family members.

A reasonable person would consider the contact, identity and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing purposes. The risk of harm is increased as the incident resulted from malicious intent (deliberate action to takeover the email account), and because phishing emails were sent from the compromised account.

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 incident was discovered by the affected individual who is fully aware of the incident. Given the circumstances, the Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner