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	SalonBiz (Organization)
Decision number (file number)	P2020-ND-185 (File #017236)
Date notice received by OIPC	September 9, 2020
Date Organization last provided information	November 4, 2020
Date of decision	December 8, 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 all or some of the following information: • name, • address, • date of birth, • online credentials, • driver's licence number, • payment card information, and • financial account number or routing number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
u**Description of incident**	• On May 29, 2020, the Organization detected unusual activity within an employee's email account.

	• The Organization secured the account and launched an investigation. • An independent forensics firm determined that one employee email account was accessed without authorization. On August 7, 2020, the Organization learned the email account contained personal information which may have been accessed by an unauthorized actor.
Affected individuals	The incident affected 4 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged an independent forensics firm to determine what happened. • Notified the Federal Bureau of Investigation (FBI). • Changed account passwords and strengthened the email environment.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on September 9, 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 potential harm(s) that might result from the incident were "Low risk of financial theft". In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Online credentials could be used to compromise other online accounts. These are all 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 its assessment there is a "low likelihood" of harm resulting fro this 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 (phishing) and allowed an unauthorized party to gain access to email accounts.
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 contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Online credentials could be used to compromise other online accounts. These are all significant harms.	

The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing) and allowed an unauthorized party to gain access to email accounts.

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 Organization notified affected individuals in a letter dated September 9, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner