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	Audio Visual Services Group, LLC d/b/a PSAV (Organization)
Decision number (file number)	P2020-ND-189 (File #016394)
Date notice received by OIPC	July 8, 2020
Date Organization last provided information	July 8, 2020
Date of decision	December 16, 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 the 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 a full-service global event production company 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: <u>Individual 1</u> • name, • credit card number and expiry date. The Organization reported that it "…believes that the credit card number is associated with a corporate card, as the card was used to pay for services…provided to its customer". To the extent this is the case, this information is not about an identifiable individual and is not "personal information" as defined in section 1(1)(k) of PIPA. <u>Individual 2</u> • name, • resume (name, address, email address, telephone number, and work/education history), • social insurance number, • driver's license number, • signature, • bank account and routing numbers, and

	• tax forms TD1 and TD1AB. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On or about January 15, 2020, the Organization learned that an unauthorized party had gained remote access to certain employees' business email mailboxes. • The unauthorized activity was part of an apparent attempt to use email accounts to re-route wire transfer payments from vendors to bank accounts under the control of the unauthorized party. • The Organization's investigation found the unauthorized access began on or before October 22, 2019 and ended on or about February 5, 2020.
Affected individuals	The incident affected two (2) residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Conducted a detailed analysis of the affected email accounts and identified personal information in those accounts. • Terminated the unauthorized access and began an investigation of the incident. • Hired outside cybersecurity experts to assist with the investigation. • Reviewing security protocols and taking steps to enhance security. • Implemented multi-factor authentication for all employee business email accounts. • Reset password for impacted accounts. • Arranged for affected individuals to receive a two-year complimentary identity theft protection service. • Provided a guidance document on steps affected individuals can take to protect themselves.
Steps taken to notify individuals of the incident	The affected individual in Alberta was notified by letter on July 8, 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 did not specifically identify harm(s) that might result from this incident, but reported it "…has arranged for affected individuals to receive a complimentary two-year membership of the Equifax Complete Premier plan, which helps detect misuse of personal information and provides affected individuals with identity protection focused on identification and resolution of identity theft". In my view, a reasonable person would consider that the contact, identity, financial, tax, employment and education information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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 did not specifically assess the likelihood that significant harm would result from this incident. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion into an employee's email account). Further, the information may have been exposed for approximately three and a half (3 ½) months.

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, financial, tax, employment and education information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion into an employee's email account). Further, the information may have been exposed for approximately three and a half (3 ½) months.

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 the affected individuals by letter on July 8, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner