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	LiveAuctioneers, LCC (Organization)
Decision number (file number)	P2020-ND-165 (File #017309)
Date notice received by OIPC	September 17, 2020
Date Organization last provided information	October 2, 2020
Date of decision	November 24, 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 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 all or some of the following information: • name, • email address, • password, • physical address, • telephone number, and • IP address. 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	

Description of incident	• On June 19, 2020, one of the Organization's technology service providers was subject to a cyber attack. • The attackers gained access to several of the Organization's environments, including Github and Amazon Web Services (AWS). The attackers obtained internal user credentials which were used to access and download a database containing the information at issue. • On July 2, 2020, the Organization was notified by its service provider that the systems had been compromised. • On July 11, 2020, the service provider advised the Organization that its data was involved in the incident and records were posted for sale on the dark web. On the same day, the Organization disabled or expired user passwords and began notifying impacted individuals. • On October 2, 2020, the Organization reported that law enforcement removed the user records from the attacker's forum on the dark web.
Affected individuals	The incident affected 3,463,544 individuals, of which 20,661 were residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Terminated relationship with the service provider. • Disabled unauthorized access to user account information and disabled passwords created before July 11, 2020. • Retired all 3.4M user account passwords. • Expired all security and access tokens on internal environments. • Reverted unauthorized changes such as firewall modifications and disabled a rogue server established by the attackers. • Engaged cyber security experts to further secure systems and perform vulnerability and penetration testing. • Implemented additional back-end protections such as multi-factor authentication, and other technical upgrades. • Contacted government authorities, law enforcement, and engaged with a forensics firm. • Will continue to review and assess privacy and cybersecurity policies to ensure adequate data protection safeguards are in place.
Steps taken to notify individuals of the incident	Affected individuals were notified by email between July 11 and August 10, 2020. A notice is also published on the Organization's website.

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.	In assessing the harm that might result from this incident, the Organization reported that "If an unauthorized third party has the login credentials … these could be used to login…, register for an auction, place bids, and charge winning items to the payment card on file", and "There is also a risk that the compromised information could be used for the purposes of identity theft or fraud". Further, "…exposure of the … credentials could affect other online accounts individuals hold" and "[users] could also be exposed to impersonation and phishing attempts." I agree with the Organization's assessment. A reasonable person would consider that the contact information at issue, including email addresses, could be used for the purposes of phishing. Credential pairings (email and password) could be used for the purposes of fraud, to gain unauthorized access to other services, or to obtain additional personal details for the purposes of identity theft. These are 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 that it "…is not aware of any incidences of fraud, identity theft or other harm to any individual data subject associated with the incident." In my view, a reasonable person would consider the likelihood of harm is increased as the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The records may have been exposed for 23 days between June 19 and July 11, before notification was provided to users. Further, the affected records may have been available for purchase on the dark web prior to removal by law enforcement.

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 information at issue, including email addresses, could be used for the purposes of phishing. Credential pairings (email and password) could be used for the purposes of fraud, to gain unauthorized access to other services, or to obtain additional personal details for the purposes of identity theft. These are significant harms.

The likelihood of harm is increased as the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The records may have been exposed for 23 days between June 19 and July 11, before notification was provided to users. Further, the affected records may have been available for purchase on the dark web prior to removal by law enforcement.

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 by email between July 11 and August 10, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner