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	8159181 Canada Inc. d/b/a Canadian Bitcoins (Organization)
Decision number (file number)	P2021-ND-282 (File #024095)
Date notice received by OIPC	December 1, 2021
Date Organization last provided information	December 1, 2021
Date of decision	February 21, 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 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 headquartered in Ottawa, Ontario, 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:
	• name,
	• date of birth,
	• contact information including:
	• telephone number,
	• current address,
	• time at current address,
	• email address,
	• user identification number,
	• two-factor authentication code,
	• IP address used for account creation,
	• organization's notes about a user,
	• status of a user account, including:
	  ○ verification status,
	  ○ risk level,
	  ○ transaction threshold,
	  ○ account balance,
	  ○ affiliate or merchant program participation,
	  ○ VIP status,
	  ○ account monitoring status,

	• information associated with reports to regulators, including:
	  ○ type of report,
	  ○ number of report,
	  ○ transaction date,
	  ○ transaction number,
	  ○ transaction description,
	  ○ IP address used for a transaction,
	  ○ user identification number,
	  ○ organization's opinion about the user,
	• banking information (institution, transit, and account numbers),
	• partial payment card information (type, expiry, last four digits),
	• "randomized user and card identification numbers and payment tokens associated with third party payment processors",
	• crypto wallet address,
	• account verification information, including:
	  ○ previous addresses,
	  ○ web browser and operating system used during verification,
	• identification information, including:
	  ○ type of identification,
	  ○ identification number,
	  ○ expiry date,
	  ○ copies/scans of the identification, and
	• transaction information.
	
	This information is about identifiable individuals 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	• Between October 9 and 11, 2021, a database under the control of the Organization was accessed without authorization. • The Organization reported that it "...initially became aware of unusual activity on its website on October 11, 2021, when its system automatically generated an error email." At that time, the Organization disabled its website, investigated, and quarantined suspicious files. • On October 21, 2021, the Organization "received an email from an anonymous perpetrator alleging that he/she had downloaded the Company's database and user documents."

	• An investigation determined that a vulnerability in certain website functionality was exploited, enabling the threat actor to upload and execute a malicious file.
Affected individuals	The incident affected 86,384 individuals, including 4,271 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Analyzed new transactions for anomalies. • Analyzed user IP and wallet addresses for anomalies. • Making outbound phone calls to confirm user transactions. • Monitoring login and login failure activities. • Searched for, and determined that other similar website functionality was not susceptible to the vulnerability. • Implemented a file upload sanitization process. • Added safeguards against unauthorized file execution. • Obfuscated file paths for certain types of uploads. • Reported the incident to the Canadian Anti-Fraud Centre. • Reported the incident to law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by email or telephone on December 1, 2021.
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 the possible harms of "Phishing, identity theft, fraud, embarrassment". I agree with the Organization's assessment. A reasonable person would consider that the contact, identity (date of birth, identification), and financial (banking, payment card, crypto wallet address, account balance) information, in addition to account monitoring status, and the Organization's notes and/or opinions about a user could be used to cause the harms of identity theft, fraud, financial loss, damage to reputation, and embarrassment, hurt or humiliation. Contact (email, telephone), location (physical address, IP address), and financial (crypto wallet address, account balance) information could be used to cause bodily harm, financial loss, damage to or loss of property, or extortion. Email addresses could be used for phishing or spear-phishing, increasing affected individuals' vulnerability to the above. 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: *Based on the nature of the incident, there could be a risk of phishing attempts, theft or fraud for some affected individuals where the information contained in the affected database would allow for such harms.* *Individuals whose personal information is included in the Company's user notes and/or mandatory reports to regulators may experience some embarrassment depending on the content of the notes and/or reports.* 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 unauthorized third party (deliberate intrusion, accessing personal information without authorization). The Organization did not report whether the records were recovered, nor did it report whether the information was published online. Despite this, the "perpetrator" alleged in an email to the Organization that they had downloaded the records, leaving open the possibility that the personal information may be misused in the future.

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 (date of birth, identification), financial (banking, payment card, crypto wallet address, account balance) information, in addition to account monitoring status, and the Organization's notes and/or opinions about a user could be used to cause the harms of identity theft, fraud, financial loss, damage to reputation, and embarrassment, hurt or humiliation.

Contact (email, telephone), location (physical address, IP address), and financial (crypto wallet address, account balance) information could be used to cause bodily harm, financial loss, damage to or loss of property, or extortion.

Email addresses could be used for phishing or spear-phishing, increasing affected individuals' vulnerability to the above. 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 unauthorized third party (deliberate intrusion, accessing personal information without authorization). The Organization did not report whether the records were recovered, nor did it report whether the information was published online. Despite this, the "perpetrator" alleged in an email to the Organization that they downloaded records, leaving open the possibility that the personal information may be misused in the future.

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 or telephone on December 1, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner