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	BlockFi, Inc. (the Organization)
Decision number (file number)	P2021-ND-047 (File #015910)
Date notice received by OIPC	May 23, 2020
Date Organization last provided information	December 16, 2020
Date of decision	March 2, 2021
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's head office is in Jersey City, New Jersey, USA. 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: • first and last name, • telephone number, • email address, • physical address, • date of birth, and • customer account and activity 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	• On May 14, 2020, an employee of the Organization detected a possible phishing attack and investigated.

	• The Organization discovered that an employee's smartphone SIM card had been ported to a new carrier by unknown external actor(s) who used the SIM to access the employee's Google account, and then the Organization's systems through Google's single sign-on interface, and to download a database of customer information. • The accounts of at least 11 customers were accessed and the designated email addresses for these customers were changed. However, the perpetrators were not able to effect cryptocurrency withdrawals from any of the accounts.
Affected individuals	The incident affected 1,327 Canadians, including 161 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Disabled the employee's software accounts. • Disabled customer trading that same day, in order to prevent any further unauthorized withdrawal attempts using customer accounts. • Concluded that no customer funds were lost or misappropriated, and that no customer account passwords or credentials were accessed in the course of the incident, and none of the foregoing are at immediate risk of loss because of the incident. • Notified all customers whose accounts were accessed by the external actor(s), and all other customers whose information was accessed. • Implemented or looking to implement additional measures to enhance security policies and programs.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on May 19, 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: *Affected individuals could potentially be contacted at the telephone number, email address, and/or physical addresses they provided in connection with their …account. However, given that no information that would enable the actor(s) to access or misappropriate customers' funds was accessed, we do not foresee any financial harm resulting from the breach.* In my view, a reasonable person would consider that the contact, identity, and account information at issue could be used to cause the harms of fraud, identity theft and financial loss. Email addresses could be used for the purposes of phishing, increasing

	the 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 reported, *We do not anticipate serious harm as likely as no funds were misappropriated and no information that could access funds was compromised.* In my view, a reasonable person would consider the likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to a deliberate, unauthorized access and downloading of the Organization's customer database by an unknown external actor.

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 account information at issue could be used to cause the harms of fraud, identity theft and financial loss. Email addresses could be used for the purposes of phishing, increasing the vulnerability to identity theft and fraud. These are all significant harms. The likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to a deliberate, unauthorized access and downloading of the Organization's customer database by an unknown external actor.

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 email on May 19, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner