June 25, 2020

Via Email

Attorney General Bob Ferguson
Attorney General's Office
Consumer Resource Center
800 Fifth Avenue, Suite 2000
Seattle, WA 98104
SecurityBreach@atg.wa.gov

Re: Data Incident

Dear General Ferguson:

On May 14, 2020, at or around 4:26 AM UTC, BlockFi, Inc. ("BlockFi") detected a possible intrusion into its technical infrastructure and began to investigate the incident. BlockFi discovered that an employee's smartphone SIM card had been ported to a new carrier by unknown external actor(s).

BlockFi disabled the affected employee's relevant software accounts as it continued its investigation of the incident. BlockFi discovered that external actor(s) used the employee's SIM toaccess the employee's Google account. This allowed the external actor(s) to access BlockFi's systems through Google's single sign-on interface and download a database of BlockFi customer information that included first and last name, phone number, email address, physical address, date of birth, and BlockFi customer account and activity information. No governmental identification numbers, passwords or account credentials, bank account or credit card number, or passport information was compromised, and no information that would enable the actor(s) to access or misappropriate customers' funds was accessed. BlockFi discovered that the accounts of at least 11 customers were accessed by the external actor(s), who changed the designated email addresses for these customers, but were not able to effect cryptocurrency withdrawals from any of these accounts.

Based on BlockFi's investigation to date, we believe that the personal data of approximately 696 Washington residents were accessed by external actors.

BlockFi disabled customer trading that same day as it continued to investigate the incident, in order to prevent any further unauthorized withdrawal attempts using customer accounts. BlockFi's investigation is continuing, but has thus far 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 as a result of the incident. BlockFi promptly notified all customers whose accounts were accessed by the external actor(s), and all other customers whose information was accessed. A sample notification is attached here as Exhibit A.

BlockFi is additionally implementing the following additional measures to its security policies and programs, many of which are already in progress:

- security updates to BlockFi's systems;

- security updates to employee mobile phones to further prevent risk of hacking;

- enhanced security audits and penetration testing effective immediately;

- at the first indication of account compromise, disable all potentially affected customer accounts, and enable them only after telephone or in person communication with affected customers;

- implementing VictorOps for BlockFi's incident response team, to help ensure potential incidents are addressed as quickly as possible regardless across multiple time zones;

- requiring employees to continue their report of any security incidents until receiving affirmative receipt from the BlockFi's incident response team;

- segregating dedicated critical hardware for personnel with access to and control over customer transactions;

- analyzing and further limit permissions and privileges among personnel;

- Remove critical people from critical roles;

- analyzing access logs to all services (including without limitation Slack and G Suite), and determine which resources are most vulnerable to be compromised and utilized in future attacks;

- encouraging all customers to adopt the two-step verification process made available to them by BlockFi for their accounts; and

- encouraging all customers to 'whitelist' their BlockFi account and thus require 72 hours to pass before new withdrawal addresses may be added to their accounts, and place an automatic 72-hour holding period on any future withdrawals to addresses not previously designated by customer.

If you have any questions please contact us at privacy@blockfi.com or 646-779-9688.

Sincerely,

DocuSigned by:
Matthew Young
FDC6632992DB46E...

Matthew Young
Corporate Counsel

Exhibit A

Customer Notification

Subject line:
Important Information about your BlockFi Account

Dear valued BlockFi client,

On May 14th, there was a data incident at BlockFi that exposed certain client account information for a brief period of time. While no information was accessed that would enable the intruder to access your account or your funds, we believe it is in the interest of transparency to share the following details with you, and all of our other clients who were potentially affected.

Your funds, passwords, and non-public identification information are secure and no BlockFi client or company funds were impacted or at risk. No action is required by you.

This email contains:

1. A summary of what happened
2. What it means for you and our recommended next steps
3. The actions we took and our next steps

What happened:

Unauthorized activity occurred in our system for about an hour on May 14th.

- *Account Information in your BlockFi account that was accessed during the incident is data we typically use for marketing purposes: Name, Email Address, Date of Birth, Postal Address, Activity History*

- *Account Information in your BlockFi account that was **NOT** accessed: Social Security Number, Tax Identification Numbers, Passports, Licenses, Passwords, Bank Account Information, Account Preferences, Photos uploaded for identification purposes*

What this means for you

Your BlockFi account, funds, and ability to take action in our system remain fully available. **No funds were lost or at risk** and **no action is required by you**.

However, we strongly recommend using best practices to secure your account including enabling two factor authentication (2FA) and whitelisting in your profile settings. Read more about how to set up these security features here.

The actions we took and our next steps

We quickly terminated the intruder's access to BlockFi's internal system and are taking the following steps to prevent such incidents from happening again:

- Released immediate security updates to BlockFi's systems, aimed at further securing marketing-related data
- Implemented security updates to employee cell phones to further prevent risk of cell phone network vulnerabilities

While there was no risk to account access or to your funds, we believe that communicating with you is the right thing to do. One of our company values is "Transparency Builds Trust" and in the interest of disclosing as much information as we can we have published a more detailed incident report available here.

We are constantly reviewing and improving our systems and security processes and will be accelerating efforts in a number of areas as a result of this activity. Unfortunately, data incidents are a constant concern for companies across all industries and, with its growth, the cryptocurrency sector is increasingly targeted. In addition to ongoing development of our systems, we are actively researching options for us to contribute to the cybersecurity efforts of the cryptocurrency industry more broadly.

We are available to answer any questions that you may have related to this incident at **communications@blockfi.com**. Thank you for your continued support.

Sincerely,
The BlockFi Team

Notice for Residents of Washington

BlockFi does not report to credit bureaus. No BlockFi activity impacts your credit score. The State of Washington recommends that we include the following information on notices, in the event that you are interested in learning more about your credit reports.

If you wish, you may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, or by calling toll-free 877-322-8228. You can also elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

TransUnion	P.O. Box 1000 Chester, PA 19022	1-800-916-8800
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241	1-800-685-1111
Experian	P.O. Box 2104 Allen, TX 75013-0949	1-888-397-3742

Subject line:
Important Information about your BlockFi Account