On May 14th 2020, BlockFi experienced a temporary data breach that exposed some BlockFi client data. We promptly discovered the root cause and stopped the unauthorized intrusion into our systems. We wanted to provide a deeper look at what happened and what we have done to prevent this type of incident going forward. We are committed to always providing transparent and clear communication.

5/14 Incident

From approximately 07:17 UTC to 08:43 UTC on May 14, 2020, a BlockFi employee's phone number was breached and utilized by an unauthorized third party to access a portion of BlockFi's encrypted back office system. This type of breach is commonly referred to as a SIM port. The unauthorized third party was able to do this by obtaining unauthorized access to the employee's phone and email via a cell phone network vulnerability. Based on the unauthorized third party's actions, it appears that the perpetrator attempted to make unauthorized withdrawals of client funds using the BlockFi platform, but was unsuccessful in doing so. However, the unauthorized third party was able to access BlockFi client information typically used by BlockFi for retail marketing purposes throughout the duration of this incident.

Every action the unauthorized third party took with respect to our systems was logged, and BlockFi was able to confirm that **no funds, passwords, social security numbers, tax identification numbers, passports, licenses, bank account information, nor similar non-public identification information was exposed as a result of this incident.**

The unauthorized third party was able to access information that BlockFi typically uses for retail marketing purposes. The information accessed is listed below:

1. Name as listed on the account
2. Email address
3. Date of birth
4. Physical address as listed on the account
5. Activity history

The incident was detected and triggered our Incident Response Protocol. The team took the following actions:

1. Locked the affected employee's credentials
2. Suspended the affected employee's access to all BlockFi systems
3. Triggered additional identity controls for all BlockFi employees to immediately confirm full control of their accounts
4. Audited the scope of attack
5. Prevented a second attempted attack from the unauthorized third party

Response

In response to the incident, BlockFi took the following actions to eliminate this vulnerability:

1. Security updates to BlockFi systems which enable us to further limit employee access to information used for retail marketing purposes
2. Security updates to employee mobile phones to further prevent risk of hacking (we detail some of the steps that you can take to protect yourself from this type of hack at the bottom of this report)
3. Enhanced security audits and penetration testing
4. Upgrades to our Incident Response Protocol trigger faster lockdown times in the event of a breach

What's Next

Due to the nature of the information that was leaked, we do not believe there is any immediate risk to BlockFi clients or company funds. Your account funds, passwords, and non-public identification information are secure and no BlockFi client or company funds were impacted as a result of this incident.

Over the next few weeks, you may experience an increased quantity of security checks in the withdrawal process from our platform due to extra precautions.

Throughout the pandemic, we have seen an increase in hacking and phishing attempts aimed both at companies and individuals. We recommend that you take the following steps to help secure your personal accounts from this type of vulnerability:

1. **Turn 2FA on** both for your BlockFi accounts and your personal devices. We have instructions here. For Gmail, we recommend removing personal emails and cell phone numbers for device confirmation. Instead, use an authenticator app or push notifications, which are much more secure.
2. **Turn Whitelisting on** at BlockFi. We have instructions here. We recommend this action even if you do not have a whitelisted address. Any time you wish to withdraw, you will have to add a new whitelisted address, which will trigger a 72-hour hold. This means that all withdrawals will be subject to a 72-hour hold, in addition to our standard 1 business day security hold. This significantly reduces the risk of being impacted by a bad actor.

Over the coming days, we will be focused on answering your questions and continuing to provide clear and transparent communication.

How do I reach you?

Our security team is ready to answer any questions you may have as a result of this incident. You can reach them at communications@blockfi.com. Response times may be slower than our typical Support desk times.

Here are links to BlockFi's Vulnerability Disclosure Policy and Bug Bounty Program.

FAQ

Why do you believe there is no immediate risk to my BlockFi funds? And what about credit cards and bank accounts?

Typically, perpetrators need access to a certain combination of personally identifiable information (PII) that would allow them to open credit cards in your name or misappropriate your funds including the following:

- Social security number
- Driver's license number or non-driver identification card number
- Account number, credit, or debit card number in combination with other identifiable data
- Biometric information such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation
- Username or email address *in combination* with a password or security question

None of this information has been exposed. The information that has been exposed about you would not typically allow a perpetrator to open a bank account on your behalf or take out credit on your behalf. In general, banks require social security numbers and/or driver's license information in order to open accounts - this information was not accessed by the intruder during the breach.

This incident likely differs from other data breaches that you may have read about in the news, because of the limited amount of information the perpetrator was able to access.

In any case, 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

How do you know exactly what actions the intruder took with respect to your systems?

Our system monitors and logs all activity.

Is there anything I need to do?

While you are not strictly required to do so, given the heightened amounts of phishing and hacking attempts over the past few weeks, we recommend you turn 2FA on for all of your devices and do not recommend using SMS texting as a two-factor method.

We also recommend activating Whitelisting on your BlockFi accounts, even if there is no whitelisted address associated with your account. This adds an automatic 72-hour hold to any withdrawals, in addition to our standard 1 business day security hold.

What steps has BlockFi taken to help prevent such an incident from happening again?

In response to the incident, BlockFi immediately took the following actions to eliminate this vulnerability:

1. Security updates to BlockFi systems which enable us to further limit employee access to information used for retail marketing purposes
2. Security updates to employee mobile phones to further prevent risk of hacking (we detail some of the steps that you can take to protect yourself from this type of hack at the bottom of this report)
3. Enhanced security audits and penetration testing
4. Upgrades to our Incident Response team triggers to promote faster lockdown times in the event of a breach

How do you know SSN and other information wasn't exposed?

Every action the unauthorized third party took with respect to our systems was logged, and we were able to verify the full extent of the attack as well confirm that no funds, passwords, social security numbers, tax identification numbers, passports, licenses, bank account information, nor similar non-public identification information were exposed as a result of this incident.

Are my funds safe?

Your funds were not misappropriated during the breach. No funds, passwords, social security numbers, tax identification numbers, passports, licenses, bank account information, nor non-public identification information were exposed as a result of this incident.

What information was compromised?

The unauthorized third party was able to access information that BlockFi typically uses for retail marketing purposes. The information accessed is listed below:

1. Name as listed on the account
2. Email address
3. Date of birth
4. Physical address as listed on the account
5. Activity history

What can I do to protect myself?

In general we recommend the following to help keep your account secure:

1. Frequently update your password
2. Enable 2FA
3. Enable Whitelisting

In addition, you may also want to update the email address associated with your account. In order to proceed with this request, please complete the attached form here.

Delete My Account - but had previous history / used our services

As a registered MSB, BlockFi is subject to record keeping requirements under the Bank Secrecy Act. Because of that, we're unable to delete your account at this time.

Update my Email Address ASAP!

In order to proceed with this request, please complete the attached form here.

Why should I turn 2FA on my personal email? What additional security items outside my BlockFi account should I take?

You should always be using 2FA to secure your personal accounts. Once an outside party has access to your email, they can gain control of your other accounts by attempting to log in and clicking the “forgot password” button. Once they do this, if you do not have 2FA turned on, they can use your email to submit withdrawal requests. The unauthorized third party will then delete the entire email history they created, so the hacked user will never become aware of the fraudulent withdrawals or email activity.

You can prevent this from happening by turning 2FA on your personal email and BlockFi accounts *and* ensuring that the type of 2FA is either the authenticator app or a push notification.

Types of 2FA that we do not consider secure for your personal email are backup phone numbers and recovery emails.