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.