UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK

In re:	Chapter 11
Genesis Global Holdco, LLC, *et al*.,[1]	Case No.: 23-10063 (SHL)
Debtors.	Jointly Administered

NOTICE OF COMMUNICATION TO CLAIMANTS

PLEASE TAKE NOTICE THAT on August 25, 2023, Kroll Restructuring Administration LLC ("*Kroll*") announced a security incident involving the personal information of bankruptcy claimants in the above-captioned case ("*Genesis*").

PLEASE TAKE FURTHER NOTICE THAT upon continued investigation of this incident, Kroll has determined that it may have involved personal data related to additional *Genesis* claimants (the "*Additional Claimants*").

PLEASE TAKE FURTHER NOTICE THAT on November 16, 2023, Kroll provided email notice, in the form attached hereto as Exhibit A, to the Additional Claimants. On November 29, 2023, Kroll provided notice via USPS first class mail, in the form attached hereto as Exhibit B, to the Additional Claimants with undeliverable email addresses.

[1] The Debtors in these Chapter 11 Cases, along with the last four digits of each Debtor's tax identification number (or equivalent identifier), are: Genesis Global Holdco, LLC (8219); Genesis Global Capital, LLC (8564); and Genesis Asia Pacific Pte. Ltd.. (2164R). For the purpose of these Chapter 11 Cases, the service address for the Debtors is 250 Park Avenue South, 5th Floor, New York, NY 10003.

Dated: November 30, 2023
New York, New York

Kroll Restructuring Administration LLC

/s/ Adam M. Adler

Adam M. Adler
55 East 52nd Street, 17th Floor
New York, NY 10055
Phone: (212) 257-5450
adam.adler@kroll.com

Claims and Noticing Agent to the Debtors

Exhibit A: November 16, 2023, Email from Kroll to Certain Genesis Claimants

From: Kroll Noticing <noticing@ra.kroll.com>
Sent: Thursday, November 16, 2023
To:
Subject: IMPORTANT – Notice of Data Breach/Steps to Protect Your Cryptocurrency and Genesis Claim

In re: Genesis Global Holdco, LLC, Case No. 23-10063
United States Bankruptcy Court for the Southern District of New York

As you may know, on August 25, 2023, Kroll Restructuring Administration LLC ("Kroll"), the claims and noticing agent for the Genesis bankruptcy proceeding, announced a security incident involving the personal data of certain bankruptcy claimants in the matters of three cryptocurrency companies, including Genesis.

This email is to inform you that our ongoing investigation has determined that additional personal data may have been impacted by this incident, including personal data associated with the email address to which this notice is being sent.

We encourage you to read this email carefully, as it provides important information that can help protect you and your digital assets against misuse of your personal data.

What happened? On or about Saturday, August 19, 2023, an unauthorized third party gained control of a mobile phone number belonging to an employee of Kroll. As a result, the unauthorized third party accessed Kroll's cloud-based systems containing information about certain Genesis claimants. When Kroll became aware of the incident, it acted quickly to secure the impacted Kroll account and launched an investigation. This incident did not affect any Genesis systems or Genesis digital assets. Further, Kroll does not maintain passwords to Genesis accounts.

As part of Kroll's ongoing investigation, we have determined that data related to additional Genesis claimants or customers may have been accessed by the unauthorized third party in connection with this incident. The files and data that may have been accessed during the incident included personal data that you, your representative, or Genesis provided to Kroll in connection with the Genesis bankruptcy proceeding.

What information was involved? The information that the unauthorized third party may have accessed included the email address to which this notice is being sent, and may have also included your name, your phone number, your address, the number or unique identifier of your claim, the amount of your claim, information about your Genesis coin holdings and balances, and/or a copy of your proof of claim form.

Important Information for Genesis Claimants. Kroll recommends that you always remain vigilant and exercise caution to protect your accounts and digital assets. You should be alert for scams, whether by phishing email, text message, social media, or other communications channels, that try to trick you into giving up control over your cryptocurrency accounts, wallets, or other digital assets.

You can help maintain the security of your accounts and digital assets by remaining vigilant and taking certain steps, including the following:

- Never share your passwords, seed phrases, private keys, and other secret information with untrusted individuals, applications, websites or devices.
- Never presume an email or other communication is legitimate because it contains information about your claim or your Genesis account.
- Verify information that you receive about the *Genesis* bankruptcy case or your claim, including emails purporting to be from Kroll or Genesis, by visiting the website of the Claims Agent, Kroll Restructuring Administration LLC: https://restructuring.ra.kroll.com/genesis or contacting Kroll Restructuring Administration at genesisquestions@kroll.com.

The Court presiding over the Genesis bankruptcy case (the United States Bankruptcy Court for the Southern District of New York, the "Bankruptcy Court"), Kroll, and Genesis will never ask or require you to do any of the following in connection with the processing of bankruptcy claims or the distribution of Genesis assets:

- Link a cryptocurrency wallet to a website or application
- Provide your seed phrase or private keys
- Download any software or use a particular wallet application
- Provide your password over email, text message, or over the phone
- Provide personal identifying information, such as your birthday or Social Security number, over email, social media or in any manner other than as described in a Court-approved process posted to Kroll Restructuring Administration's case website or the Bankruptcy Court's docket

Please know that any distribution of Genesis assets will only be at the time and in the manner established by the Bankruptcy Court. Information about the Bankruptcy Court's orders can be found at the website of the Claims Agent, Kroll Restructuring Administration LLC: https://restructuring.ra.kroll.com/genesis.

If you have any questions, receive suspicious communications, or wish to verify the authenticity of communications that are purported to be from individuals associated with the Genesis bankruptcy

case, please contact: genesisquestions@kroll.com.

Protect Your Online Accounts and Cryptocurrency against "SIM swap" attacks. Although we are not currently aware of any SIM swapping attacks on Genesis customers in connection with the incident, Kroll recommends that all owners of cryptocurrency and digital assets always take extra caution to protect their accounts.

SIM swapping attacks are designed to get your mobile carrier to transfer your phone number to a device controlled by the attacker, so the first line of defense is following the advice of your carrier to protect your mobile phone account. Owners of cryptocurrency and digital assets should consider additional layered protections against SIM swapping, including the following:

1. **Your mobile service provider can help you set up a "SIM lock."** Contact your mobile carrier and request to put a SIM lock on your phone number so that you must appear in person with an ID to make changes. Your mobile service provider may also allow you to set a secure pin or password that must be provided before a number can be ported. Choose a unique pin or password and store it in a secure, offline location.
2. **In your mobile device settings, set up a private PIN for SIM Lock.** In addition to having your mobile service provider placing a SIM lock on your number, you can set up a SIM lock on your Android and iPhone devices through the device settings. Locking your mobile device's SIM card adds yet another layer of security, meaning that even if someone can get into your phone, they still can't use it to call, text, or access your data plan.
3. **Consider using a Secure Mobile Service.** There are several Secure Mobile Service options that can be used proactively to defend against SIM swapping. These range in choice of service, hardware and device depending upon your preference. Some examples to consider include Efani, Silent Phone, Cloudflare Zero Trust SIM, Silent Link, and 4Freedom Mobile Silent Phone.
4. **Use a separate phone.** A popular and effective low-tech alternative is getting a separate phone and number to be used exclusively for bank and financial applications. Do not give this number to anyone else.
5. **Additional authentication.** Many people choose to use options for multi-factor security such as authenticator applications. Google, Microsoft and Duo offer free and easy to use applications that are available in both the Apple App Store and Google Play Store. For additional security, these apps can be installed on a separate phone.
6. **Hardware options.** Physical tokens for multi-factor authentication are simple and secure. If you prefer using a USB hardware authentication device, one of the most popular and practical options is YubiKey.
7. **Do not use crypto or online broker/exchange phone apps.** Cyber attackers target cryptocurrency and exchange accounts, so consider only accessing these accounts with an air-gapped computer protected with a hardware multi-factor authentication device. If you do, be sure to safely store backup keys.

8. **Archive and back-up sensitive data.** Protect sensitive email contents by archiving and backing up email so it's not accessible to an intruder if a breach occurs.

Exhibit B: November 29, 2023, First Class Mail Letter from Kroll to Certain Genesis Claimants

In re: Genesis Global Holdco, LLC, Case No. 23-10063
United States Bankruptcy Court for the Southern District of New York

As you may know, on August 25, 2023, Kroll Restructuring Administration LLC ("Kroll"), the claims and noticing agent for the Genesis bankruptcy proceeding, announced a security incident involving the personal data of certain bankruptcy claimants in the matters of three cryptocurrency companies, including Genesis.

This letter is to inform you that our ongoing investigation has determined that additional personal data may have been impacted by this incident, including personal data associated with the name and address to which this notice is being sent.

We encourage you to read this notice carefully, as it provides important information that can help protect you and your digital assets against misuse of your personal data.

What happened? On or about Saturday, August 19, 2023, an unauthorized third party gained control of a mobile phone number belonging to an employee of Kroll. As a result, the unauthorized third party accessed Kroll's cloud-based systems containing information about certain Genesis claimants. When Kroll became aware of the incident, it acted quickly to secure the impacted Kroll account and launched an investigation. This incident did not affect any Genesis systems or Genesis digital assets. Further, Kroll does not maintain passwords to Genesis accounts.

As part of Kroll's ongoing investigation, we have determined that data related to additional Genesis claimants or customers may have been accessed by the unauthorized third party in connection with this incident. The files and data that may have been accessed during the incident included personal data that you, your representative, or Genesis provided to Kroll in connection with the *Genesis* bankruptcy proceeding.

What information was involved? The information that the unauthorized third party may have accessed included the name and address to which this notice is being sent, and may have also included your phone number, the number or unique identifier of your claim, the amount of your claim, information about your Genesis coin holdings and balances, and/or a copy of your proof of claim form.

Important Information for Genesis Claimants. Kroll recommends that you always remain vigilant and exercise caution to protect your accounts and digital assets. You should be alert for scams, whether by phishing email, text message, social media, or other communications channels, that try to trick you into giving up control over your cryptocurrency accounts, wallets, or other digital assets.

You can help maintain the security of your accounts and digital assets by remaining vigilant and taking certain steps, including the following:

- Never share your passwords, seed phrases, private keys, and other secret information with untrusted individuals, applications, websites or devices.
- Never presume an email or other communication is legitimate because it contains information about your claim or your Genesis account.
- Verify information that you receive about the *Genesis* bankruptcy case or your claim, including emails purporting to be from Kroll or Genesis, by visiting the website of the Claims Agent, Kroll Restructuring Administration LLC: https://restructuring.ra.kroll.com/genesis or contacting Kroll Restructuring Administration at genesisquestions@kroll.com.

The Court presiding over the Genesis bankruptcy case (the United States Bankruptcy Court for the Southern District of New York, the "Bankruptcy Court"), Kroll, and Genesis will never ask or require you to do any of the following in connection with the processing of bankruptcy claims or the distribution of Genesis assets:

- Link a cryptocurrency wallet to a website or application
- Provide your seed phrase or private keys
- Download any software or use a particular wallet application
- Provide your password over email, text message, or over the phone
- Provide personal identifying information, such as your birthday or Social Security number, over email, social media or in any manner other than as described in a Court-approved process posted to Kroll Restructuring Administration's case website or the Bankruptcy Court's docket

Please know that any distribution of Genesis assets will only be at the time and in the manner established by the Bankruptcy Court. Information about the Bankruptcy Court's orders can be found at the website of the Claims Agent, Kroll Restructuring Administration LLC: https://restructuring.ra.kroll.com/genesis.

If you have any questions, receive suspicious communications, or wish to verify the authenticity of communications that are purported to be from individuals associated with the *Genesis* bankruptcy case, please contact: genesisquestions@kroll.com.

Protect Your Online Accounts and Cryptocurrency against "SIM swap" attacks. Although we are not currently aware of any SIM swapping attacks on Genesis customers in connection with the incident, Kroll recommends that all owners of cryptocurrency and digital assets always take extra caution to protect their accounts.

SIM swapping attacks are designed to get your mobile carrier to transfer your phone number to a device controlled by the attacker, so the first line of defense is following the advice of your carrier to protect your mobile phone account. Owners of cryptocurrency and digital assets should consider additional layered protections against SIM swapping, including the following:

1. **Your mobile service provider can help you set up a "SIM lock."** Contact your mobile carrier and request to put a SIM lock on your phone number so that you must appear in person with an ID to make changes. Your mobile service provider may also allow you to set a secure pin or password that must be provided before a number can be ported. Choose a unique pin or password and store it in a secure, offline location.
2. **In your mobile device settings, set up a private PIN for SIM Lock.** In addition to having your mobile service provider placing a SIM lock on your number, you can set up a SIM lock on your Android and iPhone devices through the device settings. Locking your mobile

device's SIM card adds yet another layer of security, meaning that even if someone can get into your phone, they still can't use it to call, text, or access your data plan.

3. **Consider using a Secure Mobile Service.** There are several Secure Mobile Service options that can be used proactively to defend against SIM swapping. These range in choice of service, hardware and device depending upon your preference. Some examples to consider include Efani, Silent Phone, Cloudflare Zero Trust SIM, Silent Link, and 4Freedom Mobile Silent Phone.
4. **Use a separate phone.** A popular and effective low-tech alternative is getting a separate phone and number to be used exclusively for bank and financial applications. Do not give this number to anyone else.
5. **Additional authentication.** Many people choose to use options for multi-factor security such as authenticator applications. Google, Microsoft and Duo offer free and easy to use applications that are available in both the Apple App Store and Google Play Store. For additional security, these apps can be installed on a separate phone.
6. **Hardware options.** Physical tokens for multi-factor authentication are simple and secure. If you prefer using a USB hardware authentication device, one of the most popular and practical options is YubiKey.
7. **Do not use crypto or online broker/exchange phone apps.** Cyber attackers target cryptocurrency and exchange accounts, so consider only accessing these accounts with an air-gapped computer protected with a hardware multi-factor authentication device. If you do, be sure to safely store backup keys.
8. **Archive and back-up sensitive data.** Protect sensitive email contents by archiving and backing up email so it's not accessible to an intruder if a breach occurs.