Joshua A. Sussberg, P.C.
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
601 Lexington Avenue
New York, New York 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)
Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)
Christopher S. Koenig
KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
333 West Wolf Point Plaza
Chicago, Illinois 60654
Telephone: (312) 862-2000
Facsimile: (312) 862-2200

Counsel to the Post-Effective Date Debtors

UNITED STATES BANKRUPTCY COURT
SOUTHERN DISTRICT OF NEW YORK

In re:	)	Chapter 11
CELSIUS NETWORK LLC, *et al.*,[1]	)	Case No. 22-10964 (MG)
Post-Effective Date Debtors.	)	(Jointly Administered)

NOTICE REGARDING COMPLETED DISTRIBUTION COMMUNICATIONS AND ONGOING PHISHING ATTEMPTS

PLEASE TAKE NOTICE that, contemporaneously herewith, the post-effective date debtors (collectively, the "Post-Effective Date Debtors" and, prior to the Effective Date, the "Debtors") began sending emails to creditors who have received all amounts they are eligible to receive under the Plan, and who are not eligible for future distributions, on account of their Claims (the "Fully Redeemed Claims") to try to prevent creditors with Fully Redeemed Claims from falling victim to ongoing phishing attempts and scams (as further detailed below).

PLEASE TAKE FURTHER NOTICE that this notice contains additional information regarding the Fully Redeemed Claims and known ongoing phishing attempts targeted at the Post-Effective Date Debtors' creditors. Please read this notice carefully for details.

[1] The Post-Effective Date Debtors in these chapter 11 cases, along with the last four digits of each Post-Effective Date Debtor's federal tax identification number, are: Celsius Network LLC (2148); Celsius KeyFi LLC (4414); Celsius Lending LLC (8417); Celsius Mining LLC (1387); Celsius Network Inc. (1219); Celsius Network Limited (8554); Celsius Networks Lending LLC (3390); Celsius US Holding LLC (7956); GK8 Ltd. (1209); GK8 UK Limited (0893); and GK8 USA LLC (9450). The location of Post-Effective Date Debtor Celsius Network LLC's principal place of business and the Post-Effective Date Debtors' service address in these chapter 11 cases is 50 Harrison Street, Suite 209F, Hoboken, New Jersey 07030.

Fully Redeemed Claims

On April 25, 2025, the Post-Effective Date Debtors began sending emails (each such email, the "Fully Redeemed Email"), the form of which is attached hereto as **Exhibit A**, to creditors who have Claims in Class 4 (Convenience Claims), Class 6A (General Custody Claims), or Class 6B (Withdrawable Custody Claims) who have fully redeemed their distributions under the Plan. Such email will be sent to approximately 200,000 creditors in total.

Unlike creditors who hold other Claims, creditors that hold Convenience Claims or Custody Claims are eligible for fixed distributions under the Plan and are not eligible for additional future distributions on account of Illiquid Recovery Rights. For example, creditors who have Convenience Claims received a one-time distribution in an amount that provides a 70% recovery on the Petition Date value of their Claims. Creditors who had either General Custody Claims or Withdrawable Custody Claims were eligible to withdraw the cryptocurrency held in their Custody account or, if they failed to do so on or before February 29, 2024, received bitcoin, ether, and/or Cash calculated in accordance with the Plan.[2] The only way creditors who hold these Claims would be eligible for future distributions is if they hold some other class of Claim against the Debtors (*e.g.*, a creditor held both a General Custody Claim and an Earn Claim).

The Fully Redeemed Email is intended to inform a creditor when it has received all distributions it is eligible to receive under the Plan. It also notifies a creditor that neither Celsius nor Stretto will send such creditor any further communications regarding such creditor's Claim(s). In sending the Fully Redeemed Email, the Post-Effective Date Debtors hope to provide creditors an update on their distribution status and assist in preventing creditors who have already received all eligible distributions under the Plan from falling victim to ongoing phishing attempts (further described below). As additional creditors receive their final distributions, the Post-Effective Date Debtors intend to send such creditors the Fully Redeemed Email.

Phishing Attempts

The Post-Effective Date Debtors are aware of continued phishing attempts purporting to be related to these Chapter 11 Cases. For example, creditors have reported emails purportedly from Celsius or Stretto asking them to log into a "claims portal" to provide their wallet information and receive their distribution. Many of these emails state that the distribution will be made in USDC or ether. These emails also include a one-time passcode or authorization code to access the "claims portal" or support ticket system.

For the avoidance of doubt, the second distribution will only be made in bitcoin or Cash. **Celsius is not making distributions directly to creditors' wallets** and also does not send a one-time passcode or authorization code as part of an email informing a creditor of their distribution status. Rather, the one-time passcode used to log in to the legitimate Celsius Claims Portal is sent when a creditor takes the affirmative action to log in to such portal by inputting its

[2] If a creditor failed to withdraw some or all of its Custody Assets on or before February 29, 2025, the Plan provided that any assets remaining in such creditor's Custody Account would be converted to bitcoin or ether (or Cash, if a creditor could not be serviced by a cryptocurrency Distribution Agent) based on the values in the Deactivation Date Cryptocurrency Conversion Table and distributed to such creditor.

email address at the login screen. Additionally, a creditor is not required to enter a code to submit a Celsius Distributions Support ticket.

Please proceed with caution and review the Post-Effective Date Debtors' Recommendations for Phishing Emails, attached hereto as **Exhibit B**.

Neither the Post-Effective Date Debtors nor their advisors will ***ever*** contact you by telephone call, social media, or text message to request account information or other personal information absent an (a) order by the Court or (b) on-the-record instruction from the Court. ***Please note that in connection with the KYC process noted above, the Post-Effective Date Debtors or Stretto will ONLY request an account holder's personally identifiable information and financial information through (i) an email from the domain "@celsius.network" (e.g., complianceteam@celsius.network), or (ii) an email from the domain "@stretto.com" (e.g., celsiusdistributions@stretto.com).*** In addition, the Post-Effective Date Debtors will not ask you to connect your wallet through a third-party to receive your distribution. Specifically, many phishing attempts request creditors to link an ERC-20 compatible non-custodial wallet to complete such creditor's distribution.

If you see any suspicious website domains or receive any uncorroborated email, text message, or telephone call purporting to be from the Post-Effective Date Debtors or their advisors claiming that withdrawals are available or requesting account information, personal information, or payment, we request that you please ***immediately*** contact the Debtors' counsel at CelsiusCreditorQuestions@kirkland.com or the Post-Effective Date Debtors' claims agent at CelsiusInquiries@stretto.com.

Copies of the pleadings filed in the above-captioned chapter 11 cases may be obtained free of charge by visiting the website of Stretto at http://www.cases.stretto.com/celsius. You may also obtain copies of any pleadings by visiting the Court's website at http://www.nysb.uscourts.gov in accordance with the procedures and fees set forth therein.

[*Remainder of page intentionally left blank.*]

New York, New York
Dated: April 25, 2025

/s/ Joshua A. Sussberg

KIRKLAND & ELLIS LLP
KIRKLAND & ELLIS INTERNATIONAL LLP
Joshua A. Sussberg, P.C.
601 Lexington Avenue
New York, New York 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900
Email: joshua.sussberg@kirkland.com

- and -

Patrick J. Nash, Jr., P.C. (admitted *pro hac vice*)
Ross M. Kwasteniet, P.C. (admitted *pro hac vice*)
Christopher S. Koenig
333 West Wolf Point Plaza
Chicago, Illinois 60654
Telephone: (312) 862-2000
Facsimile: (312) 862-2200
Email: patrick.nash@kirkland.com
ross.kwasteniet@kirkland.com
chris.koenig@kirkland.com

Counsel to the Post-Effective Date Debtors

Exhibit A

Fully Redeemed Email

Subject Line: Completion of Claim Distributions from Celsius Network

Dear [●],

You are receiving this email because you had either a Convenience Claim or a Custody Claim under the Plan of Reorganization of Celsius Network LLC and Its Debtor Affiliates. Creditors who held Convenience Claims were eligible to receive a one-time distribution equal to 70% of the petition date value of their Convenience Claim. Creditors who held Custody Claims were eligible to either withdraw their Custody assets from the Celsius Platform or, if such assets remained on the Celsius Platform after February 29, 2024, receive a one-time distribution of BTC, ETH, and/or US Dollars on account of such assets.

This is to inform you that you will not receive any future distributions because you have either (i) successfully received your distribution on account of your Convenience Claim and/or (ii) have withdrawn all eligible Custody assets from the Celsius Platform or otherwise received your distribution on account of your Custody Claim. Creditors who held Convenience Claims or Custody Claims did not receive Illiquid Recovery Rights under the Plan and are not eligible to receive future distributions. No further communications regarding this matter will be issued.

If you have any questions or require additional information, please open a ticket with Celsius Distributions Support. Please note that tickets opened by creditors with completed distributions will not be considered a priority and such requests may not receive a response.

For more information, visit our Knowledge Base
This resource is integrated with the support ticketing system and contains comprehensive information on distributions and answers to frequently asked questions. For court updates, visit cases.stretto.com/celsius.

Stay alert for phishing attempts
Celsius or its advisors will never (i) request that you connect your wallet to receive your distribution or (ii) contact you directly by phone, text message, or social media to request account or personal information absent an order or on-the-record instruction by the Court.

Celsius

Exhibit B

Post-Effective Date Debtors'
Recommendations for Phishing Emails

Post-Effective Date Debtors' Recommendations for Phishing Emails

Be aware of the sender's email address and URLs contained in their messages. Phishing emails will exploit your trust, expectations, and complacency with interacting with seemingly trusted sources. The first step is always to verify the Email Sender's Identity, and without clicking on the links in the email, confirm where they are directed to.

We recommend users proactively "whitelist" official emails by creating email filters/tags or automation that will only tag Stretto or Celsius emails from legitimate sources.

Review the below list of official websites and email addresses. You should disregard anything not coming from these email addresses or proceed with extreme caution.

Please refer to the below for a list of official email addresses:

- hello@celsius.network
- app@celsius.network
- claims@distributions.celsius.network
- do-not-reply@updates.celsius.network
- do-not-reply@claimsportal.celsius.network
- complianceteam@celsius.network
- no-reply@cases-cr.stretto-services.com
- celsiusdistribution@stretto.com
- ionicdigital@odysseytrust.com
- ionicdigitalinc@proxypush.com
- do.not.reply@hyperwallet.com
- do-not-reply@onfido.com
- CelsiusCreditorAnswers@kirkland.com
- CelsiusCreditorQuestions@kirkland.com
- CelsiusLitigationAdmin@m3-partners.com

Please refer to the below for a list of official websites:

- celsius.network
- claimsportal.celsius.network
- stretto.com
- cases.stretto.com
- celsiusnetwork.medium.com
- cases.stretto.com/Celsius

Note the specific punctuations, and don't be tricked by similar but differently worded or punctuated URLs using dashes instead of periods. Remember some URL and website addresses may seem similar to the above, but you must ensure they are any of the ones shown above. ***Sometimes the difference between a legitimate email or domain and a phishing attempt can be a single letter.***

Check the sender's email address and where the email links will take you. Examine the sender's email address carefully. Phishers often use similar-looking addresses to mimic legitimate

ones. Look for misspellings, extra characters, or unusual domain names. Verify email content and formatting.

Be skeptical of emails with poor grammar, spelling errors, or unusual formatting. Legitimate organizations usually maintain a professional standard in their communication.

Hover over links. If on your computer, hover your mouse over any links in the email to preview the destination URL. Ensure it matches the expected website and is not a disguised link pointing to a phishing site.

Check for generic greetings. Phishing emails often use generic greetings like "Dear Customer" instead of addressing you by name. Legitimate organizations typically use your name in their communications.

Beware of urgent or threatening language. Phishing emails often create a sense of urgency or use threatening language to manipulate recipients into taking immediate action. Be cautious if an email demands urgent attention.

Verify unexpected attachments. Avoid opening unexpected attachments, especially if they come from unknown or unexpected sources. Malicious attachments may contain malware or phishing links.

Do not open these links for the first time on a mobile phone, as a mobile phone does not allow you to hover over links and ensure the stated link and the hyperlink match.

Examine the email signature. Legitimate emails from companies usually include a consistent and professional email signature. Lack of contact information or inconsistencies can be red flags.

Enable two-factor authentication (2FA) everywhere possible. Implementing 2FA adds an extra layer of security, making it more challenging for attackers to gain unauthorized access even if they obtain your credentials through phishing.

Use email security features. Many email providers offer built-in security features. Enable features like spam filters and phishing detection to enhance your email security.

Educate yourself and stay informed. Stay informed about the latest phishing techniques and trends. Regularly update yourself on common phishing tactics to recognize new and sophisticated attempts. Review the Celsius Knowledge Base site, as well as the official docket on Stretto to keep yourself up to date.

https://celsiusdistribution.stretto.com/support/solutions
https://cases.stretto.com/Celsius
https://twitter.com/celsiusnetwork
https://x.com/celsiusnetwork

Verify unexpected requests. If an email requests sensitive information or actions that seem unusual, independently verify the request by contacting the organization through official channels before providing any personal information.

Check for HTTPS. Verify that the website you are directed to uses HTTPS. While this alone does not guarantee legitimacy, it adds an additional layer of security. When in doubt, verify the SSL certificate used.

Stay cautious with pop-ups and forms. Be cautious if an email or website opens unexpected pop-ups or prompts you to enter sensitive information in forms. Legitimate organizations typically handle such interactions securely, not over a single-click email.

Never connect your Crypto Wallet anywhere, even if it looks like a Celsius or Stretto Website. If you follow the above tips, proceed with caution, and stay up to date with official site updates, you will be more secure in these trying times.