

**WHITE & CASE LLP**

David M. Turetsky  
Keith H. Wofford  
Samuel P. Hershey  
1221 Avenue of the Americas  
New York, New York 10020  
Telephone: (212) 819-8200  
Facsimile: (212) 354-8113  
Email: david.turetsky@whitecase.com  
kwofford@whitecase.com  
sam.hershey@whitecase.com

**WHITE & CASE LLP**

Aaron E. Colodny (admitted *pro hac vice*)  
555 South Flower Street, Suite 2700  
Los Angeles, California 90071  
Telephone: (213) 620-7700  
Facsimile: (213) 452-2329  
Email: aaron.colodny@whitecase.com

– and –

**WHITE & CASE LLP**

Michael C. Andolina (admitted *pro hac vice*)  
Gregory F. Pesce (admitted *pro hac vice*)  
111 South Wacker Drive, Suite 5100  
Chicago, Illinois 60606  
Telephone: (312) 881-5400  
Facsimile: (312) 881-5450  
Email: mandolina@whitecase.com  
gregory.pesce@whitecase.com

*Proposed Counsel to the Official Committee of Unsecured Creditors*

**UNITED STATES BANKRUPTCY COURT  
SOUTHERN DISTRICT OF NEW YORK**

In re:	)	Chapter 11
CELSIUS NETWORK LLC, <i>et al.</i> , <sup>1</sup>	)	Case No. 22-10964 (MG)
Debtors.	)	(Jointly Administered)
	)	<b>Related Docket Nos.: 344, 399, 607, 633, 638, 639, and 642</b>

**THE OFFICIAL COMMITTEE OF UNSECURED  
CREDITORS' (I) SUPPLEMENTAL JOINDER TO THE DEBTORS'  
MOTION TO REDACT PERSONALLY IDENTIFIABLE INFORMATION AND (II)  
JOINDER TO THE DEBTORS' MOTION TO REDACT NAMES IN CONNECTION  
WITH FINANCIAL INFORMATION IN PUBLICLY FILED PLEADINGS**

<sup>1</sup> The Debtors in these chapter 11 cases and the last four digits of their federal tax identification number are as follows: 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); and Celsius US Holding LLC (7956). The location of Debtor Celsius Network LLC's principal place of business and the Debtors' service address in these chapter 11 cases is 121 River Street, PH05, Hoboken, New Jersey 07030.

The Official Committee of Unsecured Creditors (the “**Committee**”) of the above-captioned debtors and debtors in possession (collectively the “**Debtors**”) files this (a) joinder to the *Debtors’ Motion Pursuant to Section 107 of the Bankruptcy Code Seeking Entry of an Order (I) Authorizing the Debtors to (A) Redact Individual Names, and (B) Implement an Anonymized Identification Process, and (II) Granting Related Relief* [Docket No. 639] (the “**Motion to Redact Names**”) and (b) supplemental joinder to the *Debtors’ Ex Parte Motion Pursuant to Section 107 of the Bankruptcy Code Seeking Entry of an Order (I) Authorizing the Debtors to Redact Certain Personally Identifiable Information From the Creditor Matrix, Schedules and Statements, and Related Documents and (II) Granting Related Relief* [Docket No. 344] (the “**Motion to Redact PII**”). In connection with the Motion to Redact PII, the Committee previously filed a joinder [Docket No. 399] (the “**Original PII Joinder**”). In support of this Joinder and the Original PII Joinder (collectively referred herein as the “**Joinders**”), the Committee also submits the *Declaration of Maxwell Galka In Support of the Official Committee of Unsecured Creditors’ (I) Supplemental Joinder to the Debtors’ Motion to Redact Personally Identifiable Information and (II) Joinder to the Debtors’ Motion to Redact Names In Connection With Financial Information In Publicly Filed Pleadings*, attached hereto as **Exhibit A**, (the “**Galka Declaration**”) and states as follows in support of hereof:

### **Joinder**

**I. Both Motions Should be Granted Pursuant to Section 107(c) of the Bankruptcy Code to Protect Against Unlawful Injury to the Account Holders.**

1. Section 107(c) of the Bankruptcy Code permits this Court to redact personally identifiable information “for cause” to “protect an individual, with respect to” information related to any “means of identification”, if this Court “finds that disclosure of such information would create undue risk of identity theft or other *unlawful injury* to the individual or the individual’s

property.” 11 U.S.C. § 107(c) (emphasis added).<sup>2</sup> The Committee joins in the Debtors’ Motion to Redact Names and the Motion to Redact PII, because such redactions will serve to protect individual account holders from unlawful injury. There will be undue risk of unlawful injury if account holder names are unredacted in Court filings, because such filings pair names with amounts of cryptocurrency associated with such holders.

2. As the Court is aware, the Schedules and Statements<sup>3</sup> are the subject of the relief requested in both the Motion to Redact Names and the Motion to Redact PII. The Schedules will detail (on an account holder by account holder basis) the names, addresses, and amounts owed by the Debtors on (a) Schedule D: Creditors Who Have Claims Secured By Property, (b) Schedule E/F: Creditors Who Have Unsecured Claims, and (c) Schedule G: Executory Contracts and Unexpired Leases. The Statements will show payments or transfers to creditors within 90 days before the filing of these cases. The Statements will show, for each payment or transfer, each holder’s name and address, the type of coin, the amount of each coin transferred, and the date of such transfer.

3. The Creditor Matrix<sup>4</sup> will list the names, address, city, state, zip code, and country of account holders. The Motion to Redact PII applies to the Creditor Matrix, but the Motion to Redact Names does not. *See* Motion to Redact Names, Ex. A ¶ 2. Because only the Motion to

---

<sup>2</sup> “Means of identification” is defined as “any name or number that may be used, along or in conjunction with any other information, to identify a specific individual[.]” 18 U.S.C. § 1028(d)(7).

<sup>3</sup> “**Schedules and Statements**” has the meaning ascribed to it in the *Order (I) Extending Time to File Schedules of Assets and Liabilities, Schedules of Current Income and Expenditures, Schedules of Executory Contracts and Unexpired Leases, Statements of Financial Affairs, (II) Extending Time to File Rule 2015.3 Financial Reports, and (III) Granting Related Relief* [Docket No. 57].

<sup>4</sup> “**Creditor Matrix**” has the meaning assigned to it in the *Order (I) Authorizing the Debtors to Prepare a Consolidated List of Creditors in Lieu of Submitting a Separate Mailing Matrix for Each Debtor, (II) Authorizing the Debtors to File a Consolidated List of the Debtors’ Fifty Largest Unsecured Creditors, (III) Authorizing the Debtors to Redact Certain Personally Identifiable Information, (IV) Approving the Form and Manner of Notifying Creditors of Commencement of these Chapter 11 Cases, and (V) Granting Related Relief* [Docket No. 55].

Redact PII applies to the Creditor Matrix, this means that the names of U.S. citizens residing in the U.S. are not included in the request to redact the Creditor Matrix.

4. There are more than 1.7 million account holders who have cryptocurrency in wallets on the Debtors' platform. *See Declaration of Alex Mashinsky, Chief Executive Officer of Celsius Network LLC, In Support of Chapter 11 Petitions and First Day Motions* ¶ 9 [Docket No. 23]. The Debtors publicly disclosed that they have about \$3.8 billion in coin assets valued as of July 29, 2022, which included \$713 million in Ethereum and \$348 million in Bitcoin.<sup>5</sup> *See Notice of Filing of Budget and Coin Report*, at 6 [Docket No. 447]. If this Court denies the Motion to Redact Names, resulting in the names being unredacted on the Schedules and Statements, the individual account holder entitlements to \$3.8 billion in crypto will be public. Such disclosure of the cryptocurrency amounts that each particular individual holds, or may be entitled to, is of great concern for the Committee and its constituents. People with a relatively larger share of cryptocurrency are even more likely to be targeted. *See Galka Decl.* ¶ 7.

5. Cryptocurrency is an anomaly — it is a bearer instrument that is intangible and can be stolen within minutes. *Galka Decl.* ¶ 14. Cyber malefactors target cryptocurrency and its holders precisely because it is easy to liquidate and transactions (although traceable with difficulty) are anonymous. Globally, scammers stole “\$14 billion in cryptocurrency in 2021,” and “cryptocurrency theft increased 516%” compared to 2020.<sup>6</sup> Once someone steals cryptocurrency, it is nearly impossible to recover those assets or find the perpetrator. *See Galka Decl.* ¶ 15. As discussed further in the Galka Declaration, malefactors can execute several schemes using

---

<sup>5</sup> Bitcoin and Ethereum are the world's first and second largest cryptocurrency, respectively, by market capitalization.

<sup>6</sup> MacKenzie Sigalos, *Crypto scammers took a record \$14 billion in 2021*, CNBC (Jan. 6, 2022 at 4:00 a.m. EST) (last updated Jan. 7, 2022 at 4:31 a.m. EST), <https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html>.

personally identifiable information (“PII”) to steal cryptocurrency or private keys (*i.e.*, a secret number that is used to sign transactions and prove ownership of a blockchain address). Galka Decl. ¶¶ 7-12. These schemes include (a) phishing attacks, (b) account spoofing, (c) SIM-swapping and (d) real-life threats. *Id.*

6. The public record is replete with incidences of cryptocurrency theft from unsuspecting users. Recently, Etherscan, CoinGecko, and other crypto data websites publicly reported a phishing attack that prompted users to connect their wallets as a way for malefactors to drain assets stored in these wallets.<sup>7</sup> Curve Finance, an exchange liquidity pool of cryptocurrency, was also exploited recently through a spoofing attack, resulting in \$573,000 gone from the platform.<sup>8</sup> Further, the number of SIM-swapping incidents have exploded since 2020. The Federal Bureau of Investigation received more than 1,600 SIM-swap complaints in 2021 that have alleged losses up to \$68 million.<sup>9</sup> Finally, the threat of unlawful injury to an individual cannot be overlooked. A man in New York, New York, was robbed of \$1.8 million of Ethereum at gunpoint.<sup>10</sup> Early this year, a Miami businessman had his cryptocurrency wallet (estimated at \$1 million) stolen at gunpoint after the thief had waited for him at the victim’s home.<sup>11</sup>

7. Further, a potential malefactor may use information provided by these Debtors to

---

<sup>7</sup> Tracy Wang, *Popular Crypto Data Sites Targeted with Phishing Attack*, COINDESK (May 13, 2022 7:42 a.m. CDT), <https://www.coindesk.com/tech/2022/05/13/popular-crypto-data-sites-targeted-with-phishing-attack>.

<sup>8</sup> Jeffrey Albus, *Curve Finance Resolves Site Exploit, Directs Users to Revoke Any Recent Contracts*, COINTELEGRAPH (Aug. 9, 2022), <https://cointelegraph.com/news/breaking-curve-finance-team-warns-users-to-avoid-using-site-until-further-notice>.

<sup>9</sup> Ginger Adams Otis, *SIM-Swapping Attacks, Many Aimed at Crypto Accounts, are on the Rise*, WALL STREET JOURNAL (Feb. 18, 2022 6:36 p.m. EST), <https://www.wsj.com/articles/sim-swapping-attacks-many-aimed-at-crypto-accounts-are-on-the-rise-11645227375>.

<sup>10</sup> Jeff Francis, *Man Robbed of \$1.8 Million in Ether at Gunpoint*, BITCOINIST, <https://bitcoinist.com/man-robbed-1-8-million-ether-gunpoint/>.

<sup>11</sup> Connor Sephton, *Armed Robbery Steals Watch and Crypto Wallet Worth \$1M*, COINMARKETCAP, <https://coinmarketcap.com/alexandria/article/armed-robber-steals-watch-and-crypto-wallet-worth-1m>.

try to gain access to cryptocurrency wallets outside of the Debtors' platform. An account holder in these cases may store cryptocurrency in more than one wallet or use multiple online platforms (e.g., Coinbase, FTX, Gemini, etc.). *See* Galka Decl. ¶ 14. If a malefactor has access to an account holder's PII, it is reasonable to expect that the malefactor is capable of using that information to steal that holder's cryptocurrency in non-Celsius wallets and from other platforms as well.

8. Protective measures should be taken to safeguard names (and other PII) in the first instance, rather than seek to remedy the effect that a theft or other unlawful injury can have on a victim. Otherwise, those people who have not had access to their crypto to meet their financial needs since June 12, 2022, when the Debtors paused withdrawals, may be victims with respect to their non-Celsius assets.

9. Merely redacting addresses does not go far enough on these publicly filed documents, as there is a repository of data containing account holder information from other platforms on the dark web. *See* Galka Decl. ¶¶ 13-15. That data can be reconciled with the names disclosed in these cases. *See id.*

## **II. This Court Should Follow the Section 107(c) Rationale to its Conclusion and Consider Broadening the Relief Granted in the Motion to Redact PII to Include All Names.**

10. In fact, if the rationale of section 107(c) protection is accepted, the Committee respectfully submits that the Motion to Redact PII does not go far enough. The Debtors are seeking to redact only the home addresses and email addresses of U.S. citizens located in the U.S. in their Motion to Redact PII, leaving their names subject to public disclosure. *See* Docket No. 344, ¶ 3. The Committee disagrees with this approach and prefers not to leave any account holders' or unsecured creditors' name unredacted. For the reasons stated above and Galka Declaration, all individual names and other PII should be redacted from publicly filed documents.

**III. Impoundment Under Bankruptcy Rule 1007 Could Provide Some Protection, But It Is Likely Inferior to the Relief Requested by the Motions.**

11. The Committee joins in the arguments of the Debtors with respect to impoundment set forth in its supplemental reply. *See* Docket No. 782, ¶¶ 21-23. While impoundment would grant some welcomed protections when compared to full disclosure, there are two concerns. First, the Court would have to formulate the methods to administer the impoundment and who would be permitted to access the data notwithstanding the impoundment. Second, depending on how impoundment is implemented by the Court, the public would potentially have less information with respect to the Schedules and Statements in an impoundment than it would if the names were replaced with code numbers. For example, with respect to 90-day transfers in the Statements, the Motion to Redact PII and Motion to Redact Names will result in parties in interest seeing the dates and magnitude of transfers on the public record (although without names). In an impoundment, only parties given access by the Court will see such information.

**Conclusion**

12. Therefore, the Committee respectfully submits that there is ample cause to justify granting the Motion to Redact PII and the Motion to Redact Names. The U.S. Trustee has objected to such relief based upon section 107(b). But neither the U.S. Trustee nor any other party has set forth grounds to deny granting such relief under section 107(c) of the Bankruptcy Code, and the grounds under section 107(c) are compelling.<sup>12</sup>

**Reservation of Rights**

13. The Committee reserves all of its rights to supplement or amend this joinder and present evidence at the hearing.

---

<sup>12</sup> The U.S. Trustee filed the sole objection to the Debtors' Motion to Redact PII [Docket No. 607], which argues that the Debtors did not meet their burden under section 107(b) of the Bankruptcy Code. UST Obj. ¶¶ 8-22.

Dated: September 12, 2022  
New York, New York

Respectfully submitted,

*/s/ Keith Wofford*

---

**WHITE & CASE LLP**

David M. Turetsky  
Keith H. Wofford  
Samuel P. Hershey  
1221 Avenue of the Americas  
New York, New York 10020  
Telephone: (212) 819-8200  
Facsimile: (212) 354-8113  
Email: david.turetsky@whitecase.com  
kwofford@whitecase.com  
sam.hershey@whitecase.com

– and –

**WHITE & CASE LLP**

Michael C. Andolina (admitted *pro hac vice*)  
Gregory F. Pesce (admitted *pro hac vice*)  
111 South Wacker Drive, Suite 5100  
Chicago, Illinois 60606  
Telephone: (312) 881-5400  
Facsimile: (312) 881-5450  
Email: mandolina@whitecase.com  
gregory.pesce@whitecase.com

– and –

**WHITE & CASE LLP**

Aaron E. Colodny (admitted *pro hac vice*)  
555 South Flower Street, Suite 2700  
Los Angeles, California 90071  
Telephone: (213) 620-7700  
Facsimile: (213) 452-2329  
Email: aaron.colodny@whitecase.com

*Proposed Counsel to the Official Committee of  
Unsecured Creditors*

**EXHIBIT A**

**Declaration of Maxwell Galka**

**WHITE & CASE LLP**

David M. Turetsky  
Keith H. Wofford  
Samuel P. Hershey  
1221 Avenue of the Americas  
New York, New York 10020  
Telephone: (212) 819-8200  
Facsimile: (212) 354-8113  
Email: david.turetsky@whitecase.com  
kwofford@whitecase.com  
sam.hershey@whitecase.com

**WHITE & CASE LLP**

Aaron E. Colodny (admitted *pro hac vice*)  
555 South Flower Street, Suite 2700  
Los Angeles, California 90071  
Telephone: (213) 620-7700  
Facsimile: (213) 452-2329  
Email: aaron.colodny@whitecase.com

– and –

**WHITE & CASE LLP**

Michael C. Andolina (admitted *pro hac vice*)  
Gregory F. Pesce (admitted *pro hac vice*)  
111 South Wacker Drive, Suite 5100  
Chicago, Illinois 60606  
Telephone: (312) 881-5400  
Facsimile: (312) 881-5450  
Email: mandolina@whitecase.com  
gregory.pesce@whitecase.com

*Proposed Counsel to the Official Committee of Unsecured Creditors*

**UNITED STATES BANKRUPTCY COURT  
SOUTHERN DISTRICT OF NEW YORK**

In re:	)	Chapter 11
CELSIUS NETWORK LLC, <i>et al.</i> , <sup>1</sup>	)	Case No. 22-10964 (MG)
Debtors.	)	(Jointly Administered)

**DECLARATION OF MAXWELL GALKA IN  
SUPPORT OF THE OFFICIAL COMMITTEE OF UNSECURED  
CREDITORS’ (I) SUPPLEMENTAL JOINDER TO THE DEBTORS’ MOTION  
TO REDACT PERSONALLY IDENTIFIABLE INFORMATION AND (II)  
JOINDER TO THE DEBTORS’ MOTION TO REDACT NAMES IN CONNECTION  
WITH FINANCIAL INFORMATION IN PUBLICLY FILED PLEADINGS**

<sup>1</sup> The Debtors in these chapter 11 cases and the last four digits of their federal tax identification number are as follows: 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); and Celsius US Holding LLC (7956). The location of Debtor Celsius Network LLC’s principal place of business and the Debtors’ service address in these chapter 11 cases is 121 River Street, PH05, Hoboken, New Jersey 07030.

I, MAXWELL GALKA, hereby declare under penalty of perjury, as follows:

1. I am the founder and chief executive officer of Elementus, Inc., a blockchain intelligence and forensics company based in New York, New York, and a forensics advisor to the Official Committee of Unsecured Creditors (the “**Committee**”) of the above-captioned Debtors and Debtors in Possession.

2. I submit this declaration (the “**Declaration**”) in support of (a) *The Official Committee of Unsecured Creditors’ (I) Supplemental Joinder to the Debtors’ Motion to Redact Personally Identifiable Information and (II) Joinder to the Debtors’ Motion to Redact Names in Connection with Financial Information in Publicly Filed Pleadings*, (b) *the Official Committee of Unsecured Creditors’ Joinder to Debtors’ Ex Parte Motion Pursuant to Section 107 of the Bankruptcy Code Seeking Entry of an Order (I) Authorizing the Debtors to Redact Certain Personally Identifiable Information from the Creditor Matrix, Schedules and Statements, and Related Documents and (II) Granting Related Relief* [Docket No. 399] (the “**Joinder**”), (c) *the Debtors’ Ex Parte Motion Pursuant to Section 107 of the Bankruptcy Code Seeking Entry of an Order (I) Authorizing the Debtors to Redact Certain Personally Identifiable Information From the Creditor Matrix, Schedules and Statements, and Related Documents and (II) Granting Related Relief* [Docket No. 344] (the “**Motion to Redact PII**”), and (d) *the Debtors’ Motion Pursuant to Section 107 of the Bankruptcy Code Seeking Entry of an Order (I) Authorizing the Debtors to (A) Redact Individual Names, and (B) Implement an Anonymized Identification Process, and (II) Granting Related Relief* [Docket No. 639] (the “**Motion to Redact Names**”).<sup>2</sup> I am over 18 years old and authorized to submit this Declaration on behalf of the Committee.

3. I hold degrees in finance and computer science engineering from the University of

---

<sup>2</sup> Capitalized terms used but not defined herein have the meanings ascribed to them in the Joinder.

Pennsylvania. I have also served as an adjunct lecturer in data science at the University of Pennsylvania. I have over 15 years of data science, finance, and quantitative analysis experience, including experience trading complex derivatives at global investment banks.

4. I specialize in blockchain intelligence and forensics analysis, including investigating complex transactions and flow of funds activities that occur on blockchains. I also specialize in analyses that monitor and trace illicit activity and ransomware attacks that are often designed to be hidden on blockchains. My analyses are often performed to help protect individuals and businesses from risks associated with blockchains and cryptocurrencies.

5. In particular, I have substantial experience assisting federal law enforcement in investigating thefts of cryptocurrency and other crimes in which cryptocurrency was used to facilitate unlawful activities. A core part of my business as chief executive officer of Elementus is to find addresses onchain that belong to malefactors. I also advise cryptocurrency service providers on ways to avoid contact with suspected malefactors who might be engaged in money laundering or other unlawful activities. Based upon this work, I have become familiar with the methods and tactics malefactors commonly use to target businesses and individuals.

6. The statements in this Declaration are, except where noted specifically, based on my personal knowledge or on information that I have received from either the Committee or employees of Elementus working directly with me or under my supervision, direction, or control. Neither Elementus nor I am being compensated specifically for this testimony other than compensation to Elementus as a professional services firm employed by the Committee. If I were called upon to testify, I could and would competently testify to the facts set forth herein on that basis.

**A. Public Disclosure of Personally Identifiable Information Creates a Risk of Unlawful Injury to Account Holders and Their Cryptocurrency.**

7. In my experience, malefactors target known cryptocurrency holders. A malefactor will know that a person holds cryptocurrency if his or her personally identifiable information is disclosed in these cases. It becomes substantially easier for malefactors to target cryptocurrency holders if the malefactors possess those holders' personally identifiable information. I understand that the Debtors' statements of financial affairs and schedules of assets and liabilities, the creditor matrix, and other documents to be filed in these chapter 11 cases will contain personally identifiable information, including (a) names, (b) physical addresses, (c) mailing addresses, or (d) email addresses (collectively, "**PII**"), if the Motion to Redact PII and Motion to Redact Names are not granted. The schedules of assets and liabilities is of particular concern because it lists individual account holders and their respective cryptocurrency holdings, thus identifying account holders who hold relatively larger amounts of cryptocurrency for malefactors. However, any release of account holder PII poses significant risks. Every commonly used scheme to steal cryptocurrency (whether in hot wallets or hardware wallets) will be easier to perform if malefactors know the PII of people who hold cryptocurrency. Some of the main risks to account holders are described below.

8. **Phishing Attacks.** There are multiple types of phishing attacks. One type occurs when an account holder receives a message (either via email, instant message, or text message) from an attacker masquerading as a trusted entity. An unsuspecting account holder may willingly provide sensitive information directly to the malefactor if he or she believes that a fraudulent email is from a trusted source. Alternatively, an account holder may indirectly provide such information and access by clicking on a link in an email, instant message, or text message received from a malefactor that causes a computer program (a "**Trojan**") to infect that holder's target device. The

Trojan can then send sensitive information from the targeted account holders' infected device to the malefactor. Additionally, an attack that is becoming increasingly common involves a malefactor pretending to be someone with whom the account holder has a relationship and using that appearance of a relationship to exploit the holder into providing sensitive information. From my experience, I know that these different phishing attacks have been used to obtain private keys and account credentials to steal cryptocurrency.

9. What all of these “phishing” attacks have in common is that, in order to succeed, they must appear authentic. A fraudulent source can appear legitimate with the inclusion of the trusted source's logo/trademark, color scheme, or typography. However, one of the most reliable means of feigning legitimacy is to include the particular account holder's PII in the message, which adds a veil of authenticity and credibility to the fraudulent communication. This makes the release of account holders' PII (which most account holders will not even be aware has occurred) particularly dangerous.

10. **Account Spoofing.** Spoofing is when a malefactor disguises an email address, display name, phone number, text message, or website URL to convince an account holder that he or she is interacting with a trusted source. As an example, a malefactor might write an account holder in these cases from an email address that appears to be from a trusted source but is actually from a fake domain name with a subtle aberration like “@celsuis.com” (in which the “i” and “u” have been switched) or “@celsius.net” (rather than “.com”). An account holder is less likely to be suspicious of these emails—and thus less likely to notice the minor errors in domain names that might alert them to the fraud—if the emails contain the account holder's PII, which the account holder perceives as indicia of authenticity. I know from experience that a malefactor will more easily be able to steal private keys or cryptocurrency from wallets once he or she has obtained the

necessary information from the account holder.

11. **SIM Swapping.** Another risk to account holders if PII is disclosed is “SIM swapping,” which is when a malefactor gains access to an account holder’s account vis-à-vis the holder’s cellphone through an accomplice at a wireless provider. That provider will issue a new SIM card for the account holder’s phone to the malefactor so the malefactor can take over the holder’s number on a new device with the new SIM. Most providers of online wallets rely on text messaging for resetting passwords or perform two-step multifactor authentication to gain access to the wallets or private keys. A malefactor who has obtained a SIM swapped device can effortlessly authenticate and obtain access to the contents of the phone belonging to the targeted account holder, including private keys and other sensitive information.

12. **Real Life Threats.** In addition to these virtual threats, if account holders’ PII is disclosed, they may be vulnerable to real-life threats, including robberies and other threats of violence. I am aware of various incidents in which holders of cryptocurrency have been robbed at gun point, being forced to surrender private keys, passwords, and other access credentials to online wallets.

**B. There is Still a Risk of Harm to Account Holders if Only Their Names are Made Public.**

13. The types of attacks described above can occur even if only names are disclosed. I know from my experience that merely the name of an individual who holds cryptocurrency is enough for a malefactor to obtain additional information about that individual from data that has been aggregated from hacks of other cryptocurrency companies, such as Coinbase and Kraken. This account holder data is available on the so-called “dark web.” The dark web is a part of the internet that contains encrypted content that is accessible with only a special software or browser. Those with access to the dark web can remain anonymous and untraceable, allowing malefactors

to engage in illegal activities with impunity. I also know from experience that a malefactor could run an account holder name through a “people search” on the internet to obtain more information in an effort to steal the account holder’s cryptocurrency holdings. A people search is a query function on a website that is not on the dark web and is accessible upon paying a small fee. I have personal knowledge of account holders who have been victims of cryptocurrency theft or other cryptocurrency crimes after their information was obtained on the dark web or via people searches.

14. In addition, cryptocurrency is an intangible bearer instrument and must be stored by the owner in a wallet or on a platform. I know that cryptocurrency holders typically store their cryptocurrency in more than one wallet or use multiple online platforms. This is the case because, among other things, (a) certain wallets are only capable of storing certain types of cryptocurrency and cryptocurrency holders typically have more than one type of currency, (b) cryptocurrency companies vary as to what types of cryptocurrency transactions can be performed on their platforms, and (c) cryptocurrency companies differ in the services they offer account holders. A malefactor who knows the names of people in these cases can reasonably expect that they have other wallets or use other platforms that are unaffiliated with the Debtors (*e.g.*, Coinbase, FTX, Gemini, etc.). Thus, the public disclosure of names makes cryptocurrency stored elsewhere a target.

15. I know from experience that having the name of a person who holds cryptocurrency is enough to subject him or her to phishing, account spoofing, physical attacks, and other unlawful injury. This risk of unlawful injury is also material if either addresses or email addresses are disclosed. Cryptocurrency is an attractive target for malefactors because it is easy to liquidate and transactions are anonymous. Once someone’s cryptocurrency is stolen, it is near impossible to recover those assets or find the perpetrator. I, therefore, believe this it is prudent to safeguard

account holders' names and other PII in the first instance rather than seek to remedy the deleterious effects of a crime should one occur as a result of PII being publicly disclosed—a disclosure to which the Debtors' account holders have not consented and are likely not aware.

Dated: September 12, 2022  
New York, New York

Respectfully submitted,

*/s/ Maxwell Galka*

Name: Maxwell Galka  
Title: Founder and Chief Executive Officer  
Elementus, Inc.