

**IN THE UNITED STATES BANKRUPTCY COURT
DISTRICT OF DELAWARE**

In re:)	
)	Chapter 11
FTX TRADING LTD., <i>et al.</i> , ¹)	Case No. 22-11068 (JTD)
)	
Debtors.)	(Jointly Administered)
)	
)	

**DECLARATION OF JEREMY A. SHERIDAN IN
SUPPORT OF THE JOINT MOTION OF THE DEBTORS AND THE OFFICIAL
COMMITTEE OF UNSECURED CREDITORS FOR AN ORDER
AUTHORIZING MOVANTS TO REDACT OR WITHHOLD CERTAIN
CONFIDENTIAL INFORMATION OF CUSTOMERS
AND PERSONAL INFORMATION OF INDIVIDUALS**

I, Jeremy A. Sheridan, declare pursuant to 28 U.S.C. § 1746 as follows:

1. I am a Managing Director in the Blockchain and Digital Assets practice for FTI Consulting, Inc. (“FTI Consulting”). FTI Consulting is the financial advisor for the Official Committee of Unsecured Creditors (the “Committee”) appointed in the above-captioned bankruptcy cases (the “Chapter 11 Cases”) of the debtors (collectively, the “Debtors”).

2. I submit this declaration (the “Declaration”) in support of the *Joint Motion Of The Debtors And The Official Committee Of Unsecured Creditors For An Order Authorizing Movants To Redact Or Withhold Certain Confidential Information Of Customers And Personal Information Of Individuals*, filed contemporaneously herewith (the “Motion”), which seeks this Court’s authority to redact and seal the names, addresses and email addresses of the Debtors’

¹ The last four digits of FTX Trading Ltd.’s tax identification number are 3288. Due to the large number of debtor entities in these Chapter 11 Cases, a complete list of the Debtors and the last four digits of their federal tax identification numbers is not provided herein. A complete list of such information may be obtained on the website of the Debtors’ claims and noticing agent at <https://cases.ra.kroll.com/FTX>.

customers who are natural persons (the “Confidential Customer Information”), from disclosure in the Chapter 11 Cases, subject to certain exceptions as set forth in the Motion.²

3. The statements in this Declaration are true to the best of my knowledge, information and belief after a reasonable inquiry under the circumstances, and except where noted specifically, are based on my personal knowledge or on information that I have received from either the Committee and its professionals or other employees of FTI Consulting working directly with me or under my supervision, direction or control. Neither FTI Consulting nor I am being compensated specifically for this testimony beyond the compensation being provided to FTI Consulting as a Court-approved professional services firm employed by the Committee. If I were called upon to testify, I could and would competently testify to the facts and opinions set forth herein. I am authorized to submit this Declaration on behalf of the Committee.

4. I have a Master’s Degree in Public Administration, Criminal Justice from the University of Arizona. I have blockchain, cryptocurrency, and cybersecurity certifications from the Blockchain Council, Columbia University, Carnegie Mellon University, Information Systems Audit and Control Association (ISACA), and the Global Information Assurance Certificate (GIAC). I possess a Top Secret / Sensitive Compartmented Information security clearance. My resume is attached to this Declaration as Exhibit A.

5. I specialize in investigations of financial crime involving complex, cyber-enabled fraud and have substantial experience investigating and analyzing illicit cryptocurrency transactions. These investigations require blockchain analytics and digital asset tracing to investigate transaction flows and assign attribution to individuals transacting on blockchains. I

² I understand that there is no objection to the sealing of the physical addresses and email addresses of customers who are natural persons. Accordingly, the issue on the Motion is whether the names of such customers (the “Individual Customer Names”), should be redacted and sealed. Nevertheless and for the avoidance of doubt, it

also specialize in network intrusion, ransomware and cyber incident response operations. My investigative and regulatory expertise has been applied to protect the financial infrastructure of the United States, strengthen the safety and soundness of the digital asset ecosystem, protect the American public from cyber incidents and bring consequence to illicit actors operating in cyberspace. I am also skilled at regulatory, government and public affairs related to blockchain, cryptocurrency, digital asset strategy, policy, legislation, enforcement and regulation.

6. For 24 years, from September 1997 to April 2022, I worked for the Office of Investigations for the United States Secret Service (the “Secret Service”), where I was promoted to Assistant Director on October 11, 2020. The Secret Service Office of Investigations is comprised of 162 offices and more than 3,000 personnel. As the Assistant Director, I led the global investigative mission of the Secret Service, which included safeguarding the financial systems of the United States from financial and cyber-based crimes, and served as an expert witness in congressional hearings related to cryptocurrency before both the United States Senate and United States House of Representatives. During my time with the Secret Service, I headed and worked on multiple investigations involving crimes that contained a blockchain and/or cryptocurrency component. A selection of my work is below:

- (a) I have been the primary (arresting) case agent for 60 state and federal financial crime investigations, resulting in 37 arrests with a 100% conviction rate;
- (b) I pioneered cyber investigative advancements and modernization for the Secret Service, including the implementation of an Integrated Investigations Operations Platform (“IIO”) to enhance data aggregation, migration and evaluation. These augmentations improved the agency’s investigative capabilities through data processing efficiencies;

is my opinion that all of the potential harm that may befall a customer to the extent its name is disclosed would be magnified tenfold to the extent its physical addresses and email addresses is disclosed as well.

- (c) I established the Secret Service's first dedicated illicit finance and digital asset tracing team to conduct investigations into illicit financial activity involving cryptocurrency and other forms of digital payments;
- (d) I directed the analysis of approximately 1381.25 terabytes of data, 145,971 digital forensic exams, and 696 network intrusion investigations related to financial fraud;
- (e) I had oversight of the National Computer Forensics Institute, the only United States government federal facility which trains and equips the nation's state, local, territorial and tribal law enforcement officers in cyber forensic investigations;
- (f) I led the agency's investigative teams to prevent approximately \$5.825 billion in cyber and financial crime loss, executed 1,590 arrests for financial crimes and investigated 13,171 criminal and protective intelligence cases; and
- (g) I directed the return of approximately \$3.28 billion of seized funds to financial institutions and private citizens who were victims of financial crimes.

7. After my retirement from the Secret Service, and just prior to joining FTI, I was the Vice President of Regulatory Affairs for Prime Trust, LLC ("Prime Trust"). Prime Trust is a software-as-a-service financial infrastructure company, which provides application programming interface ("API") services for business-to-business digital asset transactions, such as qualified custody, payment rails, indemnity, liquidity and settlement services. Prime Trust is a licensed custodian for more than 200 individual digital tokens, processing up to 300 million API calls per month, and settling up to \$3.5 billion in transactions per month. At Prime Trust, I partnered with legislators, enforcement agencies and regulators for legislative action and government engagement in the digital asset industry. I also led Prime Trust's Legal and Compliance departments in regulatory affairs.³

³ FTX was a customer of Prime Trust. During my short tenure at Prime Trust, my only involvement with FTX was to assist with response to media inquiries related to our processing of FTX customer funds.

8. In my experience, malefactors often use cryptocurrency to facilitate financial fraud. I have substantial experience investigating and analyzing such illicit cryptocurrency transactions. Similarly, I have become familiar with the methods and tactics malefactors commonly use to target businesses and individuals for illicit activity. Based on my experience, as well as my understanding of the Debtors' prepetition activities and the high profile nature of these proceedings, I believe that revealing the Individual Customer Names imposes a severe and unusual risk of identity theft, asset theft, personal attack, and further online victimization. These risks are heightened with respect to the Debtors' customers because malefactors typically target (x) consumers they believe to be holders of cryptocurrency and (y) consumers who are in a vulnerable state, including because they have sums of money tied up in bankruptcy proceedings.

9. Identity and asset theft schemes are often extremely successful using blind or blanket attack methods, where the malefactor has no background information on their victims. These crimes become significantly more effective when malefactors employ targeted approaches equipped with some measure of background or personal information about the victim. In that regard, even if only Individual Customer Names are disclosed, through combining a customer name with other publicly available sources—*i.e.*, a malefactor can correlate additional information from public databases, including telephone numbers, home addresses, email addresses, places of employment, social media presence, associates, etc.—a malefactor will be able to harvest a full target biography of a customer, *i.e.*, a customer dossier. This dossier vastly increases the malefactor's probability of success in committing a crime against these targets based on the ability to implement bespoke attack vectors and techniques. Although customers with extremely common names may be afforded slightly more protection against a malefactor who tries to locate the customer's online presence, simply being able to tie a name to a certain

trait—such as an individual who holds and invests in cryptocurrency—can significantly increase the likelihood that a malefactor may locate an individual’s online presence and information, and thus provide the malefactor the opportunity to create a customer dossier.

10. Odds of success for identify and asset theft crimes are increased even further if they are committed against vulnerable persons, such as the Debtors’ customers in these Chapter 11 Cases, whose circumstances provide greater opportunity to, or reduced defense against, the malefactor. Some of the Debtors’ individual customers may be vulnerable due to the monetary losses they have experienced resulting from the misconduct and alleged fraud by the Debtors’ former management.⁴

A. Disclosure of Individual Customer Names, Creates an Undue Risk of Identify Theft or Unlawful Injury.

11. In my experience, cryptocurrency offers several opportunities to malefactors seeking to commit illicit activities. It serves as a distributed, instantaneous transfer of value that does not provide the immediate identity of its user and can serve as both the method and the means to conduct illicit activity. As such, malefactors target known cryptocurrency holders for scams. If Individual Customer Names are made public in these Chapter 11 Cases, such information will provide potential malefactors an itemized list of vulnerable targets.⁵ In particular, it will provide malefactors with a menu of potential targets via disclosure of the Debtors’ schedules of assets and liabilities list (if the Individual Customer Names are not redacted), and each of the Debtors’ customers’ respective cryptocurrency holdings. By making

⁴ See **Exhibit B**, Erika Harrell, *Victims of Identity Theft, 2018*, BUREAU OF JUSTICE STATISTICS (Apr., 2021), at 11, <https://bjs.ojp.gov/library/publications/victims-identity-theft-2018> (discussing percentages of victims who reported emotion distress after experiencing identity theft).

the names of the Debtors' customers public, these schedules would serve to identify individual customers of the Debtors who hold relatively larger amounts of cryptocurrency, thereby placing a target on their back and facilitating fraudulent schemes by malefactors.

12. Moreover, as mentioned above, the likelihood of successfully executing a cybercrime is vastly increased if the malefactor has knowledge of their target. This is evidenced in the most prevalent types of online financial fraud scams.

13. Business Email Compromise ("BEC"). BECs exploit knowledge of the target's personal and professional online business activity. In these schemes, the malefactor will send the target an email message that appears to be a legitimate request for some business function, such a payment of an invoice or wiring of funds to complete a transaction. Knowledge of the target's personal details is integral to the execution of this scheme, such that the Federal Bureau of Investigation's first recommended safeguard against them is to "[b]e careful with what information you share online"⁶

14. Romance Scams. Romance scams are those in which the malefactor pretends to build a romantic relationship with the victim in order to convince them or guilt them in to sending them money. The backbone of these scams is establishing an online connection and rapport with the target. Malefactors are successful at these scams when they are conducted with random targets with no intelligence related to their identity. A directed romance scam based on knowledge of the target's identity exponentially increases the likelihood of these attacks being

⁵ See Exhibit C. Zhiyuan Sun, *Crypto Users Claim Gemini Email Leak Occurred Much Earlier Than First Reported*, COINTELEGRAPH, (Dec. 14. 2022), <https://cointelegraph.com/news/crypto-users-claim-gemini-email-leak-occurred-much-earlier-than-first-reported> (reporting that multiple customers of the cryptocurrency exchange Gemini received phishing emails after Gemini experienced a leak of customer emails and partial phone numbers).

⁶ See Exhibit D. *Business Email Compromise*, FBI, <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise> (last visited Apr. 10, 2023).

successful. The malefactors who are able to perform reconnaissance to see which victims have the most investment potential are those most likely to execute the fraud.⁷

15. Pig Butchering. The practice of increasing a victim's cryptocurrency account, known as "fattening" before draining of all funds, is called "Pig Butchering". This scam has grown rapidly in the past year and cost U.S. victims "more than \$429 million in losses" in 2022.⁸ These scams are perpetrated by malefactors who form online relationships with their targets, convince them to invest in cryptocurrency accounts, and then steal the invested funds. In most of these schemes, the malefactor doesn't know their target prior to executing the fraud and has to persuade them to set up a cryptocurrency wallet. Both of these requirements will be eliminated with the release of Individual Customer Names, as the malefactor will be able to specifically identify their target as someone who is already versed in cryptocurrency and who already has a cryptocurrency wallet established.

16. Phishing Attacks. There are multiple types of phishing attacks, including cryptocurrency credential harvesting, cryptocurrency transfer solicitation and commodity stealers that target cryptocurrency values. Phishing involves the malefactor posing as a known or trusted entity through an email, text message or instant message. A malefactor can easily pose as a known entity to increase the appearance of legitimacy by including that entity's logo, color scheme or other identifying attributes. Even more effective is to purport legitimacy by including personal information about the target in the phishing message from which, based on the malefactor's misrepresentation, the target provides sensitive personal, business or financial

⁷ See Exhibit E. The 2023 Crypto Crime Report, CHAINALYSIS, (Feb. 2023), at 87 and 100, <https://go.chainalysis.com/2023-crypto-crime-report> (explaining that scammers often perform reconnaissance on potential victims).

⁸ See Exhibit F. Robert McMillan, *A Text Scam Called 'Pig Butchering' Cost Her More Than \$1.6 Million*, WALL ST. J. (Oct. 20, 2022), <https://www.wsj.com/articles/a-text-scam-called-pig-butchering-cost-her-more-than-1-6-million-11666258201>.

information. This information can be provided by the target directly in a response to the imposter or indirectly by clicking on a link that allows the malefactor unauthorized access to the target's device (a "Trojan") or injects some other form of malware or virus to infect the target's device. With access to the target's network, the malefactor can then obtain account information, change permissions and authorizations for further illicit activity, transfer funds into their possession, and send sensitive information from the targeted account holders' infected device to the malefactor. I have seen phishing attacks in my professional experience used, and succeed, in obtaining both victims' account credentials and their private keys to online wallets containing cryptocurrency. These attacks do not require a high degree of sophistication and are facilitated by phish kits that can be used to create fraudulent landing pages⁹ with pre-packaged sets of code, graphics and configuration files. The only missing element to these kits is the target of the attack, which will be available if the Individual Customer Names are disclosed in these Chapter 11 Cases.

17. Account Spoofing. Spoofing entails a malefactor disguising an email address, display name, phone number, text message, or website URL to convince a target that the source of the message is a legitimate entity. A malefactor could target one of the Debtors' customers, locate their email address from other public sources and contact them from a spoofed email address that appears to relate to the proceedings in these Chapter 11 Cases. A customer of the Debtors is less likely to be suspicious of emails that appear to be related to these Chapter 11 Cases—and thus unlikely to notice the minor errors in domain names that might alert them to the fraud—if the emails target the account holder based on the malefactor's knowledge of their cryptocurrency holdings and the circumstances of this case.

⁹ See Exhibit G. Jared Peck, *Have Money for a Latte? Then You Too Can Buy a Phish Kit*, PROOFPOINT, (Dec. 16, 2021), at 5, <https://www.proofpoint.com/us/blog/threat-insight/have-money-latte-then-you-too-can-buy->

18. Again, the success of this scheme will be significantly enhanced if the spoofed message contains the target's personally identifiable information, such as Individual Customer Names, which the target perceives as indicia of authenticity. This increased risk is not merely speculative or conjecture. In the currently ongoing cryptocurrency bankruptcy case of *In re Celsius Network LLC* ("Celsius"), the names of Celsius' customers were made public. Subsequently, many Celsius customers became the target of phishing attacks by scammers posing as bankruptcy lawyers using emails and phone calls.¹⁰ These examples of phishing attacks targeting the Celsius customers ranged from simple attempts to connect over messaging applications, to sophisticated emails using Celsius logos and impersonating legal counsel, and in one instance resulted in the bankruptcy court involving the U.S. Marshal.¹¹ Even though Celsius customer email addresses and phone numbers were redacted, malefactors were still able to reach customers based solely upon the disclosed names. An even greater risk of attacks exists in the Chapter 11 Cases if Individual Customer Names are disclosed because there are approximately 9 million customer accounts on the Debtors' exchanges as compared to the approximately 1.7 million registered users in Celsius, of which only approximately 300,000 are active users that

phish-kit.

¹⁰ See Exhibits H. James Nani, *Scammers, Posing as Kirkland Lawyers, Phishing Celsius Customers*, BLOOMBERG LAW (Dec. 1, 2022), <https://news.bloomberglaw.com/bankruptcy-law/scammers-posing-as-kirkland-lawyers-phishing-celsius-customers> (reporting on phishing attempts that occurred after the unsealing of customer names in the Celsius bankruptcy proceeding); see also Exhibit I, *Notices of Phishing Attempts, In re Celsius Network LLC*, Case No. 22-10964 (MG) (Bankr. S.D.N.Y.) [Docket Nos. 1527, 1681, 1904, 1992 and 2082].

¹¹ The attack in question involved a phishing attempt in which malefactors sent emails to Celsius customers, purportedly from the claims agent in that case, requesting additional personally indefinable information from customers and requiring a filing fee and tax fee to be paid. The email address used by the scammers to send the phishing attempt came from "celsius@cases.stretto.restructuring.ltd", which is similar to the domain name of the official claims agent in the Celsius cases. As part of the scam, an order from the Celsius bankruptcy court was attached, which had been modified to include false information, thereby making it appear that that the request for personal information and fees was legitimate. *Supra* Exhibit I, *Second Supplemental Notice of Additional Phishing Attempts, In re Celsius Network LLC*, Case No. 22-10964 (MG) (Bankr. S.D.N.Y. Jan. 12, 2023) [Docket No. 1904]; see also Exhibit J. Hr'g Tr. (Feb. 6, 2023) at 17:9-16, *In re Celsius Network LLC*, Case No. 22-10964 (MG) (Bankr. S.D.N.Y. Feb. 6, 2023) [Docket No. 2016].

hold an account balance of more than \$100.¹² Moreover, I know from experience that a malefactor will more easily be able to steal private keys or cryptocurrency from wallets by obtaining the necessary information from the target via account spoofing.

19. Each of the aforementioned financial fraud scams, BEC, Romance Scams, Pig Butchering, Phishing attacks, and Spoofing relies on the malefactor impersonating a trusted entity. Historically, these efforts have been hampered by linguistic, grammatical, or content errors committed by the malefactor, especially those in foreign locations. Simply put, the malefactor makes errors in the impersonation message that raise suspicion in their target and prevent the scheme from being successful. However, the arrival and refinement of artificial intelligence programs, such as ChatGPT, a language model that can generate, proofread and enhance technical writings (including emails), has further propelled the success of these impersonation attacks by essentially eliminating previous telltale signs of poor grammar, typos, and recycled material/narratives.¹³ This further increases both the likelihood of phishing emails bypassing spam filters and the success of the attack itself against individuals. Furthermore, the Debtors' customer base contains a large number of foreign individuals, who may not be familiar with the U.S. bankruptcy process. This lack of familiarity increases the risk and likelihood of a customer falling victim to one of the above scams or attacks because a customer may not realize that the Debtors would never request certain information from their customer base, such as their account password or private keys.

¹² See Declaration of Alex Mashinsky, Chief Executive Officer of Celsius Network LLC, in Support of Chapter 11 Petitions and First Day Motions, ¶ 9, *In re Celsius Network LLC, et al.*, Case No. 22-10964 (MG) (Bankr. S.D.N.Y. July 14, 2022) [Docket No. 23].

¹³ See **Exhibit K**. Mark Sweney, *Darktrace Warns of Rise in AI-Enhanced Scams since ChatGPT Release*, THE GUARDIAN, (Mar. 8, 2023), <https://www.theguardian.com/technology/2023/mar/08/darktrace-warns-of-rise-in-ai-enhanced-scams-since-chatgpt-release> (reporting on the warning of cybersecurity firm Darktrace concerning an increase in criminals using artificial intelligence to create sophisticated and convincing scams since the launch of ChatGPT in November, 2022).

20. SIM Swapping. SIM swapping is when a malefactor gains access to a target's cellphone, which allows the malefactor to receive communications associated with the target's phone number, including those that involve multi-factor authentication ("MFA"). MFA is predominantly used to access financial accounts. To accomplish SIM swapping, a malefactor transfers the target's cell phone number to another device without authorization through the target's wireless provider, and the wireless provider is tricked into conducting this transfer based on the malefactor's impersonation of the target. This impersonation is carried out through various forms of social engineering conducted by the malefactor, wherein they convincingly act as the true owner of a cellphone account with the wireless provider. In this scenario, the malefactor's odds at claiming to be the authorized account holder are vastly increased if they are able to provide accurate personal information about the authorized account holder. Malefactors are able to complete this illicit activity even if armed solely with an account holder's name, as there are numerous online avenues to search for cellphone numbers by name only and U.S. carriers have a poor track record of preventing these attacks. Additionally, most providers of online cryptocurrency wallets rely on MFA via text messaging for a number of account functions, including resetting passwords, conducting transactions and gaining 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 to wallets containing cryptocurrency.¹⁴ In my experience, SIM swapping is a particularly effective fraud scheme as it circumvents and leverages the perceived austere security mechanism of MFA.

¹⁴ See Exhibit R, *Lorenzo Franceschi-Bicchierai Cops Arrest Infamous SIM Swapper Who Allegedly Stole \$14 Million in Cryptocurrency* (Oct. 11, 2018), <https://www.vice.com/en/article/7x3may/cops-arrest-sim-swapper-14-million-cryptocurrency> (reporting on a sim swapping scheme where \$14 million in cryptocurrency was stolen).

21. Physical Threats. Finally, in addition to online financial fraud scams, customers of the Debtors whose Individual Customer Names are disclosed may face physical threats, such as robberies, stalking, vandalism, cyber-bullying, and other threats of violence.¹⁵ There have been notable recent reports of kidnappings in which victims are targeted because they are known to hold a large amount of cryptocurrency. In my experience and in investigations I have conducted involving targeted violence, these cases often involve subjects suffering from mental disorders preying on targets who often are identified through online information connected to high profile events. Disclosing Individual Customer Names would expose some customers to this type of aggression.¹⁶

22. Beyond the potential for physical harm, emotional distress, cyber threats, kidnapping, stalking, and bullying that could occur, malefactors could likely determine the physical addresses of the Debtors' customers as a result of disclosure of Individual Customer Names. In my opinion and experience, known holders of cryptocurrency are frequently targeted because malefactors are cognizant that cryptocurrency assets are easy to liquidate and very difficult to trace.¹⁷

¹⁵ See Exhibit L. Francisco Memoria, *Victim of Brazil Bitcoin Ransom Kidnapping Plot Rescued*, CCN, (last modified on Mar. 4, 2021), <https://www.ccn.com/victim-of-brazilian-bitcoin-ransom-kidnapping-rescued> (reporting that a woman married to a cryptocurrency businessman in São Paulo, Brazil was kidnapped and ransomed for Bitcoin and another cryptocurrency, with police believing the victim was targeted specifically due to her ties with cryptocurrency); see also Exhibit M. Jamie Redman, *London Student Robbed at Knifepoint by 8 Thugs for \$93k in Bitcoin*, BITCOIN.COM, (Sept. 25, 2021), <https://news.bitcoin.com/london-college-student-robbed-at-knifepoint-by-8-thugs-for-93k-in-bitcoin> (reporting that a student was robbed immediately after disclosing to a friend his ownership of Bitcoin).

¹⁶ See Exhibit N. Chris Morris, *Some Teenagers Are Making a Fortune Trading Bitcoin—One Even Got Kidnapped Because of His Success*, FORTUNE, (Oct. 21, 2021), <https://fortune.com/2021/10/21/trading-bitcoin-teenagers-kidnapped> (reporting that a 14-year-old was kidnapped and beaten after publicly announcing his success in Bitcoin trading).

¹⁷ See Exhibit O. Rob Davies, *'Crypto Muggings': Thieves in London Target Digital Investors by Taking Phones*, THE GUARDIAN, (May 8, 2022), <https://www.theguardian.com/technology/2022/may/08/crypto-muggings-thieves-in-london-target-digital-investors-by-taking-phones> (reporting that there have been multiple incidents of violent crimes, with thieves targeting cryptocurrency investors due to the irreversible nature of transfer of cryptocurrency).

B. *Malefactors Only Need Access to the Individual Customer Names in Order to Steal Customers' Identity or Produce Unlawful Injury.*

23. If Individual Customer Names are disclosed (even if no other Confidential Customer Information is made available), malefactors can much more easily target the Debtors' customers. Cryptocurrency fraud is easier to enact if malefactors have access to a target's name, because malefactors can then assemble and correlate other identifying information about an individual using various means, including social media, public and private databases, and other data sourced from past hacks. For example, data breaches over the past decade involving, for example, Yahoo, LinkedIn, Facebook and Marriott have flooded illicit marketplaces with a treasure trove of personally identifiable information.¹⁸ Hackers have sold this information through encrypted chat groups or the dark web for pennies per record. Additionally, the plethora of hacks occurring at other cryptocurrency companies, such as BaderDAO, BitMart, Binance, Bitfinex and KuCoin, adds to the volume of personally identifiable information and cryptocurrency-specific personally identifiable information available in illicit marketplaces.¹⁹ It is not difficult for malefactors to correlate all of this publicly available information, especially information that originates from cryptocurrency hacks, with disclosed Individual Customer Names.

24. Furthermore, it is common for cryptocurrency holders to use multiple wallets or online platforms to store their cryptocurrency assets, as some wallets only support certain types of cryptocurrency and some online platforms only support limited types of transactions or services. It is my understanding that a vast number of the Debtors' customers use other online

¹⁸ See generally **Exhibit P**. Michael Hill, Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO, (Nov. 8, 2022), <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century>.

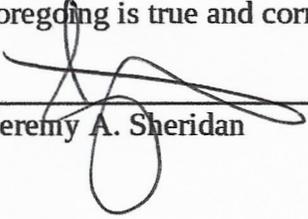
¹⁹ See generally **Exhibit Q**. *17 Biggest Crypto Heists of All Time*, COINTELEGRAPH, (Mar. 10, 2023), <https://cointelegraph.com/explained/the-biggest-crypto-heists-of-all-time>.

platforms or exchanges to hold digital assets (*e.g.*, Coinbase, Metamask, etc.). Therefore, disclosing Individual Customer Names will put at risk of attacks and schemes the cryptocurrency held by those individuals stored on non-Debtor exchanges.

25. I know from experience that a malefactor who possesses the name of a person who holds cryptocurrency is enough to subject that person to BECs, romance scams, pig butchering, phishing, account spoofing, SIM swaps, physical attacks and other unlawful injury. These risks are material and exacerbated if other identifying information is obtained, such as physical address or email address. Although online attacks and cyber threats, stalking, and bullying are endemic in today's virtual world, the release of Individual Customer Names would greatly exacerbate such risks for the Debtors' customers. Perpetrators of frauds and online attacks are emboldened by, motivated from and attracted to high profile cases like the Chapter 11 Cases. Adding to this environment is the fact that cryptocurrency is already an attractive target for malefactors because it is easy to liquidate, instantaneous, global and pseudo anonymous. In that regard, disclosing the names of customers of a cryptocurrency exchange, is different, than, for instance, disclosing the names of creditors of a non-cryptocurrency related debtor. And while I understand that there is normally a presumption of transparency and disclosure in bankruptcy cases, the dangers I have described from disclosing Individual Customer Names serve to highlight the uniqueness of these cases. Therefore, I believe it is prudent to protect the Debtors' customers' identities by ensuring that those names are sealed, rather than accepting the significant risks that the Debtors' customers will be subject to criminal activity as a result of the disclosure of the Individual Customer Names.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: April 19, 2023
Fairfax, Virginia



Jeremy A. Sheridan