

CORNELIUS P. MCCARTHY (CM-3544)  
CHEHEBAR DEVENEY & PHILLIPS  
485 Madison Avenue Suite 1301  
New York, New York 10022  
Tel.: 212-532-8204  
Cell: 914-629-0687  
Fax: 212-753-8101  
E-mail: cmccarthy@cdlawllp.com

PIERCE O'DONNELL (PO-5724)  
GREENBERG GLUSKER FIELDS CLAMAN  
& MACHTINGER  
2049 Century Park East, 26<sup>th</sup> Floor  
Los Angeles, California 90067  
Tel.: 310-201-7558  
Cell: 310-480-3366  
Fax: 310-201-1792  
E-mail: podonnell@greenbergglusker.com

Attorneys for Plaintiff  
MICHAEL TERPIN

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

<p>MICHAEL TERPIN,</p> <p>Plaintiff,</p> <p>-against-</p> <p>ELLIS PINSKY, as an individual; and DOES 1-20, Inclusive,</p> <p>Defendants.</p>	<p>Civil Action No. _____</p> <p><b>COMPLAINT FOR: (1) VIOLATIONS OF THE RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS ACT( (RICO) (18 U.S.C. § 1962(C)); (2) CONVERSION; (3) MONEY HAD AND RECEIVED; (4) REPLEVIN; (5) VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (18 U.S.C. § 1930(A)(4)); AND (6) PRELIMINARY AND PERMANENT INJUNCTION</b></p> <p><b>DEMAND FOR JURY TRIAL</b></p>
---	---

Plaintiff MICHAEL TERPIN, (“Plaintiff”), for his claims for relief against defendants ELLIS PINSKY (“Pinsky”) and DOES 1 through 20, inclusive (“Doe Defendants”) (collectively, “Defendants”), based on personal knowledge as to his own acts and information and belief as to the acts of all others, alleges as follows:

## **INTRODUCTION**

1. This case involves a sophisticated cybercrime spree masterminded by a then 15-year-old high school student in coordination with and with the active participation of other individuals, including several other minors. In this case, the cybercrime enterprise hacked accounts and then stole and laundered tens of millions of Plaintiff’s cryptocurrency. Working with confederates on multiple continents, the ringleader of this scheme, Defendant Ellis Pinsky (“Pinsky”) has stolen over \$100 million in cryptocurrency. One prominent victim is Plaintiff Michael Terpin, a high-profile cryptocurrency pioneer, who lost nearly \$24 million worth of cryptocurrency as a result of a hack perpetrated by Pinsky and his gang of digital bandits.

2. Pinsky, who recently turned 18, attends and is apparently now set to graduate from a suburban New York high school. In his early teens, he began hacking computers with the mission of accessing his victims’ private accounts where they store their cryptocurrency holdings or private information. Once his cohorts or he breach the security wall with a stolen mobile phone SIM card belonging to his “mark,” they use that victim’s telephone or computer to locate information to take charge of the victim’s cryptocurrency accounts and to transfer the proceeds of those accounts to their control.

3. One of Pinsky’s partners was Nicholas “Nick” Truglia, a then 20-year-old New York hustler who, until recently, was imprisoned in Santa Clara County, California, on grand larceny charges for a separate cryptocurrency theft, is currently on bail awaiting criminal trials in

the state court in California and in the federal court in New York. His federal trial is based on his indictment for stealing Plaintiff's cryptocurrency. Truglia's assignments included identifying victims, obtaining their cell phone and passcode numbers, conning the mobile phone carrier into giving him or another imposter a new SIM card, and then handing off the scam to Pinsky to execute the hack. Truglia is part of the conspiracy but not a Defendant in this action – Plaintiff has already sued Truglia in a separate action and obtained a judgment against him from the Los Angeles County Superior Court in the State of California.

4. It is believed that Pinsky met other accomplices in a chat room called the "Original Gangsters" or "OGUsers Forum."

5. Pinsky, Truglia, and others in the criminal conspiracy, who are sued herein as Doe Defendants, operated the enterprise by locating potential targets (preferably those with large cryptocurrency holdings), obtaining information about their victims, such as telephone numbers and carriers, either impersonating the victims or coopting or bribing employees of the carriers to cooperate with the theft, forging identity papers for the victims, and then taking over the victim's mobile telephone. Once in control of the telephone, Pinsky, Truglia, and/or their co-conspirators would then roam openly through files of the victim that they were able to access and intercept two factor authentication messages until they located information about cryptocurrency holdings that would allow them to exfiltrate such holdings from their mark's accounts. The nucleus of Pinsky's global criminal organization is more than a dozen members of the OGUsers' forum frequented by hackers committing SIM swapping attacks.

6. Truglia has identified Pinsky and others as his confederates in cryptocurrency thefts. In several recorded conversations after the 2018 theft, Truglia admitted how Plaintiff's cryptocurrency was purloined, described Pinsky's integral role in the theft, named other

participants in the theft, and described how the proceeds of the theft were divided among the gang. Along with other highly incriminating evidence, Truglia's detailed account of Pinsky's penetration of Plaintiff's accounts and how he unlocked the unique secret to the passcodes for his crypto-wallets conclusively demonstrates that Pinsky was one of the hackers.

7. The financial crimes of Pinsky, Truglia, and their confederates in hacking others are no less insidious than bank robberies, credit card and bank fraud, and money laundering by drug traffickers and terrorists. They are all egregious crimes against society that evince an utter callous disregard for the property and feelings of others. And they are deserving of the same severe punishment and public opprobrium.

8. On the surface, Pinsky is an "All American Boy." The son of privilege, he is active in extracurricular activities and lives a suburban life with a doting mother who is a prominent doctor.

9. Despite their wholesome appearances, Pinsky and his other cohorts are in fact evil computer geniuses with sociopathic traits who heartlessly ruin their innocent victims' lives and gleefully boast of their multi-million-dollar heists. As one of many examples, one victim of Truglia lost all the money set aside for his children's college education. The apparent ringleader of the group, Pinsky is constantly reaching out for the support of equally callous offenders who think nothing of stealing millions from their victims to live a life of conspicuous consumption. For example, Pinsky is reputed to have used his ill-gotten gains to purchase multi-million-dollar watches and is known to go on nightclub sprees at high end clubs in New York City, and Truglia rented private jets and played the part of a dashing playboy with young women pampering him.

10. Pinsky also has continually boasted to friends that he is invincible and would never get caught. In early 2019, Pinsky texted:

“You think I’m fucking dumb. . . . I’m not fucking stupid. . . . I threw out all my shit [computers]. . . . Fuck that attorney [Terpin’s lawyer]. They don’t have shit on me. . . . You think I’m dumb enough to keep all my money in America. . . . [Truglia] is a dumb ass . . . and got caught.”

11. Since the theft, Plaintiff has mounted an all-out, global effort to track down Pinsky, Truglia, and others to find evidence about their involvement in the theft of his cryptocurrency and to recover his assets. In a California lawsuit, Mr. Terpin obtained a writ of attachment for Truglia’s assets, and later obtained a judgment against Truglia for almost \$75.8 million. As Plaintiff increased the pressure, Pinsky began to panic. Following Terpin’s lawyer calling his mother and contacting her lawyer, Pinsky made a series of devastating admissions in texts with an acquaintance who is an African-American. Among other things, he acknowledged that: “I’m well off I’m good I don’t need extra money I’m set for life . . . You’re a dumb nigger I could buy you and all your family . . . **I have 100 million dollars**”

12. Since that date, Pinsky admitted his participation in the theft by making a payment to Plaintiff of cryptocurrency, cash, and a watch. On the one hand, the value of slightly over \$2 million at the time of return represents a fraction of the amount for which Pinsky is responsible, yet on the other hand it confirms Pinsky’s involvement since there is obviously no other explanation for his possession of such funds or his delivery to Plaintiff of any amount.

13. Pinsky has redefined the conventional meaning of “spoiled brat.” Overindulged by his parents, Pinsky is arrogant, remorseless, and accustomed to getting what he wants—private jet flights, luxury cars, and expensive accessories. Whether this evil mastermind’s parents were recklessly negligent or worse in failing to monitor and control their wayward son remains to be seen.

14. The tables are now turned on Pinsky, Truglia, and their confederates. Plaintiff will expose this secret dark side of their teenage counterculture of SIM swaps and cryptocurrency thefts that operate – with fellow hackers in the OGUUsers’ forum – beneath a seemingly wholesome facade. In view of Pinsky’s boast that he has salted away \$100 million in ill-gotten gains, nothing less than full restitution of Plaintiff’s losses, plus interest, attorneys’ fees, costs, and expenses will satisfy Plaintiff that Defendants have adequately compensated him for his loss. And, an award of treble damages or punitive damages will send the appropriate message to Defendants and others that the epidemic of these types of SIM card attacks have real consequences and must immediately cease.

#### **NATURE OF ACTION**

15. This is an action for violation of the Racketeering Influenced and Corrupt Organizations Act (“RICO”), 18 U.S.C. §§ 1961-1968); conversion and conspiracy to commit conversion; money had and received; replevin; aiding and abetting unlawful conduct; violation of the Computer Fraud and Abuse Act. 18 U.S.C. § 1030(a)(4); and a preliminary and permanent injunction.

#### **JURISDICTION AND VENUE**

16. This Court has subject matter jurisdiction of this civil action pursuant to 28 U.S.C. §§1332 (a), and 1367(a) and the doctrine of pendent jurisdiction. This Court also has subject matter jurisdiction of this civil action pursuant to 28 U.S.C. Section 1332(a)(1) because this dispute involves citizens of different states and the amount in controversy exceeds \$75,000, exclusive of interest and costs.

17. This Court also has personal jurisdiction over Defendant Pinsky. As alleged more fully below, each of the Defendants, acting in person or through their respective

employees, agents and/or alter egos, has engaged in substantial, continuous, and systematic activities within the State of New York. Pinsky resides within the State of New York and this Judicial District. The claims sued upon arise out of Defendants' forum-related, unlawful activities directed towards Plaintiff.

18. Venue is proper in this Court under 28 U.S.C. §§1391(a)(2), (b)(2) and (c), because a substantial part of the events or omissions giving rise to Plaintiff's claims against Defendants occurred in this Judicial District and a substantial part of the property that is the subject of the action is situated within this Judicial District.

### **PARTIES**

19. Plaintiff Michael Terpin is a citizen of the United States who has a residence in Los Angeles County, California. Mr. Terpin obtained wireless services from AT&T Mobility, Inc. ("AT&T") in Los Angeles County in the mid-1990s. Mr. Terpin continued at all times relevant to the allegations herein to receive wireless services from AT&T for a telephone number with a Southern California area code.

20. Mr. Terpin is well known for his involvement with cryptocurrency. Cryptocurrency is digital or virtual currency designed as a medium of exchange in which encryption techniques generate units of currency that verify the transfer of funds through an encrypted and decentralized ledger called "blockchain." The blockchain records transactions and manages the issuance of new units of currency. Cryptocurrency is decentralized, operates independently of a central bank or other regulatory authority, and is often traded by parties through "exchanges." Once a transfer of cryptocurrency has occurred, it is impossible to trace or reverse the transaction without possession of certain private and complex key numbers held only by the transferor.

21. Ellis Pinsky is an 18-year-old citizen of the United States residing with his mother in Westchester County in the city of Irvington, New York. At the time in 2018 that he stole nearly \$24 million of cryptocurrency holdings from Plaintiff, he was 15 years old. Pinsky is highly adept in matters regarding computers, the digital world, cryptocurrency holdings, the blockchain, and laundering cryptocurrency holdings and money.

22. Non-party Nicholas Truglia is a former resident of New York, New York, who until recently was incarcerated in the Santa Clara County jail in California on charges of grand theft, identity theft, unauthorized computer access, and other felony charges. Truglia is currently out on bail for charges in the California state court system and a federal indictment in the Southern District of New York involving the theft of Plaintiff's \$24 million cryptocurrency.

23. Plaintiff is ignorant of the true names and capacities of defendants sued herein as DOES 1-20, inclusive, and therefore sues these defendants by such fictitious names. Plaintiff will amend this Complaint to allege their true names and capacities when ascertained.

24. Plaintiff is informed and believes and, on that basis, alleges that Defendants, and each of them, were and are the agents, employees, representatives, principals, partners, co-conspirators, joint venturers and/or alter egos of each of the other Defendants, and/or otherwise were acting in concert with each of the other Defendants, and in such capacity or capacities participated in the acts or conduct alleged herein. They were also acting within the scope of such relationship, such that each should be held liable for the acts of the other. In addition, they are each in some manner responsible for the damages suffered by Plaintiff and the relief sought here as alleged below.

### **COMMON ALLEGATIONS**

25. This lawsuit is about the unauthorized and wrongful taking from Plaintiff of



nearly \$24 million in cryptocurrency. Pinsky and his co-conspirators, including Truglia and the Doe Defendants, were at the center of the conspiracy to gain unlawful access to Plaintiff's accounts and information via bribery and/or impersonation, and to steal and to launder his cryptocurrency.

### **SIM SWAPS AKA SIM-JACKING**

26. The theft here was made possible by the increasingly prevalent practice of unauthorized SIM swaps. This is an illegal maneuver by which a hacker takes over a victim's cellular phone account to intercept messages to facilitate the theft of funds (often cryptocurrency) and transfer such funds to the hacker or the hacker's accomplices or to cryptocurrency accounts under the hackers' control. Increasingly publicized, SIM swaps have become a focus of federal and state law enforcement authorities.

27. A "SIM" or "Subscriber Identity Module" (also known as a "SIM card") is a small card inserted into a mobile device enabling the device to communicate with the service provider. A SIM contains data necessary to make a successful connection between the mobile phone and the telecommunication provider. SIM cards store files that are used to uniquely identify them.

28. A "SIM swap" is a practice whereby a hacker gains access to a victim's telephone account or number in order to intercept communications, including text messages, to the mobile telephone. The process is also referred to as "SIM-jacking." A perpetrator of a SIM-jack typically arranges through bribery of someone (often a carrier employee) with access to customer information at the carrier to change the SIM card assigned to a user to a telephone under the control of the hacker or the hacker's accomplices. Once the SIM transfer has occurred, the hacker uses the hacker's phone to impersonate the victim with service providers, such as e-mail

providers, and uses the victim's phone number to request changes to account settings and to reset passwords to take control of the victim's accounts.

29. Perpetrators of SIM swap fraud, such as Pinsky, Truglia, and the Doe Defendants (the "Pinsky Gang"), frequently intercept "2-Factor Authentication" (or "2FA") messages sent to the victim's telephone. 2FA is frequently used as a security mechanism for authentication purposes. Perpetrators of SIM swaps, including Pinsky, Truglia, and the Doe Defendants, intercept the messages to gain access to the accounts owned by the victim, including cryptocurrency accounts or other accounts providing access to such accounts. Once the perpetrator gains access to the account, the perpetrator transfers the funds in such accounts to an account controlled by the perpetrator or confederates.

30. The perpetrators of SIM swap fraud – SIM-jackers – specifically target victims owning cryptocurrency because of the nature of cryptocurrency transactions. The digital assets embodied by cryptocurrency (such as Bitcoin or Ethereum) are a medium of exchange using cryptography to secure the transaction. Typically, the holder of cryptocurrency has both a "public" and a "private" key or address that the holder uses to receive, transfer, or use cryptocurrency. The private key, which is individual to the owner of the cryptocurrency, is used to write in the public ledger to transfer cryptocurrency. Because the key can be used to "spend" cryptocurrency, owners typically keep such keys secure. Such keys are complex. For example, in the case of Bitcoin, a 256-bit private key may contain 64 characters consisting of numbers and capitalized and uncapitalized letters.

31. Once a transfer of cryptocurrency has occurred, it cannot be reversed. Although the transaction is displayed in a public ledger, it is not readily possible to identify the transferor or transferee without knowing the parties' private keys. Cryptocurrency thus makes an attractive

target for perpetrators of SIM swap fraud, such as the Pinsky Gang, because the perpetrators can transfer stolen digital assets to accounts that are not readily traced or reversed and can be accessed anywhere in the world free from government regulation or inspection.

### **THE JANUARY 7, 2018 SIM-JACK**

32. Pinsky and Truglia, with the active assistance of the Doe Defendants, orchestrated the SIM swap of Plaintiff's cell phone and the hack, theft, and laundering of Plaintiff's cryptocurrency. Some time ago, a group of young video game players—with participants in the United States and Great Britain—formed a user group called “Original Gangsters” or “OGUsers.” In time, this moniker proved apt as they morphed into the nucleus of a sophisticated criminal enterprise operating in North America, Europe, and Asia. Their racket was theft of cryptocurrency by means of SIM swaps. Each of the dozen or more gangsters in the Pinsky Gang had assigned roles, including identifying the victims, obtaining their cell phone and passcode numbers, forging identity cards, conning or bribing the mobile phone carrier employee into giving the imposter a new SIM card, handing off the personal identity information to Pinsky who with the assistance of his cohorts executed the hack and laundered the cryptocurrency holdings into Bitcoins or fiat money.

33. On January 7, 2018, the Pinsky Gang struck hard and quickly at the cryptocurrency owned by Plaintiff. With uncanny efficiency, they obtained Plaintiff's SIM card and took over Plaintiff's cell phone with his AT&T wireless number. Plaintiff's phone went dead. The SIM-jackers for all intents and purposes had hijacked Plaintiff's digital identity. They then intercepted 2FA messages, gained control over Plaintiff's accounts, and stole nearly \$24 million worth of cryptocurrency in the form of Triggers, Skycoin, and Steem from him on January 7 and 8, 2018.

34. In November 2018, Truglia was arrested for the theft of \$1 million of cryptocurrency holdings owned by someone other than Plaintiff. On December 18, 2018, the Santa Clara County Superior Court held a bail hearing for Truglia. In this hearing, the Court cited evidence that on January 7, 2018, which the Court states was the same date that Terpin lost more than \$20,000,000 through a SIM swap, Truglia told someone named Ryan O’Keefe that he had stolen a cryptocurrency wallet with 20 million in it. On the same date, Truglia texted a friend: “I’m a millionaire. I’m not kidding. I have 100 Bitcoin.”

35. On January 7, 2018, the average price of one Bitcoin varied between \$16,033 and \$17,244. *See <https://www.livebitcoinnews.com/bitcoin-price-analysis-january-7-2018-bears-control/>*. On the date of the Terpin SIM swap, Truglia boasted that “today my life changed forever,” and he offered to hire “porn star escorts” and take his friends to the Super Bowl.

#### **LAUNDERING PLAINTIFF’S STOLEN COINS**

36. Like drug cartel money, stolen cryptocurrency holdings are dirty, give rise to suspicion, and may be very difficult to spend if they are not either washed or converted to other forms of readily-spendable currency. The Pinsky Gang attempted to launder their victims’ cryptocurrency holdings in several steps. First, they moved the various coins out of the rightful owner’s account to new addresses/accounts that they controlled. Often, these stolen coins are stored on one of the crypto-exchanges like Binance, Gemini, or C2CX. Next, the gang converted a less common type of stolen coin into a more recognized, easily-tradeable crypto like Bitcoin. Then, the gang withdrew the coins. Due to daily withdrawal limits and “Know Your Customer” (KYC) requirements, however, each individual must present a passport to prove that he is the account owner, so they often used stolen or forged passports.

37. The Pinsky Gang stole three types of coins from Plaintiff’s wallet: 3,000,000

Triggers; 12,500 Steem, and 20,000 Skycoin, all of which he and his cohorts moved in different ways.

38. Pinsky and his co-conspirators moved the Triggers to at least five accounts that they controlled at Binance, and they then converted the cryptocurrency in those accounts to Bitcoin before transferring the proceeds off the exchange to privately held wallets.

39. On information and belief, Defendants attempted to launder, and in fact laundered, the Steem coins as well.

40. Laundering the Skycoin proved more difficult. At the C2CX exchange, Defendants opened an account in the name of a Florida State student, which was apparently a stolen identity. Defendants proceeded to convert the Skycoin into Bitcoin at a substantially below market valuation, but were ultimately unable to move the proceeds off the exchange.

#### **PINSKY AND TRUGLIA ADMIT THEIR CRIMES**

41. The evidence of Pinsky's and Truglia's culpability for organizing and directing scores of SIM swaps and thefts, collectively totaling well over \$100 million of cryptocurrency holdings, including Plaintiff's nearly \$24 million, is overwhelming and irrefutable.

42. Truglia has been identified in a California criminal case as the perpetrator of numerous SIM swap frauds. In a December 2018 hearing in Truglia's case, the prosecution cited an investigatory report revealing that Truglia had used telephone accounts obtained through SIM swap to register new cryptocurrency accounts, including accounts on Coinbase, Gemini, and Binance. Truglia also engaged in money laundering efforts after his SIM swaps by moving his stolen cryptocurrency through multiple addresses, breaking up the stolen amounts into multiple segments of smaller amounts, structuring his transactions to avoid reporting requirements, and otherwise taking steps to avoid due diligence and suspicion. Truglia has boasted about his

cybercrimes to many friends.

43. Likewise, Pinsky has been identified as Truglia's partner in multiple SIM swap frauds. In 2018, after the Terpin hack but prior to his arrest, Truglia implicated Pinsky in several conversations recorded by a friend. In a declaration under penalty of perjury, Chris David quoted the following admissions by Truglia in a September 2018 conversation:

- (a) How Pinsky and he hacked Terpin to steal his \$24 million worth of Cryptocurrency holdings;
- (b) How Pinsky and he laundered cryptocurrency holdings out of the blockchain into cash;
- (c) Truglia has an account at the Gemini exchange and took out \$1,200,000;
- (d) Truglia committed tax fraud;
- (e) Truglia saw records indicating that in December 2017, Pinsky had \$70 million; and
- (f) One of their victims, Plaintiff, is too "dumb" to be able to figure out what happened and trace the laundered cryptocurrency holdings.

44. In another conversation on September 9, 2018, Truglia related the following to a mutual friend:

- (a) He will never be caught hacking/stealing because he is so good at it—literally, "how are they going to prove that my story [his defense] wrong?";
- (b) "Nobody can get me in trouble. Nobody can put me in jail. I would bet my life on it, actually"; and
- (c) As of September 2018, Truglia had \$60 million of Bitcoin.

45. In still another 2018 conversation, Truglia admitted:

- (a) He told the police that he had \$60 million when they came to his apartment;
- (b) He had stolen all his money and had not legitimately accumulated his wealth;
- (c) He was a computer hacker and stole his victims' cryptocurrency holdings and that this was thrilling for him—"the thrill of the game"—which he would never stop doing—even if there were no money involved; it was all "a mind game";
- (d) His partner was named Ellis Pinsky, and Pinsky had stolen between \$70 and \$80 million through hacking;
- (e) He, Truglia, is a "Robin Hood" who robs from the rich but does not give to the poor;
- (f) Pinsky and he do hacking and SIM swapping by Truglia locating the victims through social engineering and Pinsky intercepting 2FA messages to find out information about accounts;
- (g) Truglia's "biggest" SIM swap was Plaintiff Michael Terpin for \$24 million, and Pinsky was his partner; and
- (h) Pinsky took proceeds from the \$24 million.

46. In mid-August of last year, Truglia further admitted his guilt for purloining Plaintiff's \$24 million of coins. Remarkably, on his public Twitter account (@erupts) at Twitter.com, Truglia admitted six times that he "Stole 24 million," referring to Plaintiff's cryptocurrency holdings.

47. Pinsky himself also has admitted that he is a cybercriminal. He has told friends that, since he was 13, he has stolen over \$100 million worth of cryptocurrency through scores of hacks, and boasted of hundreds of thousands of cash stored in his bedroom in his mother's home. Indeed, when Pinsky repaid in 2019 a portion of the sum that had been stolen from Plaintiff, it included a cash payment consistent with Pinsky's boast.

48. Pinsky fancies himself as some kind of Super Boy who is beyond the reach of the law and impervious to Plaintiff's efforts to hold him liable for the \$24 million heist. This brash egoist has texted:

"You think I'm fucking dumb . . . I'm not fucking stupid . . . I threw out all my shit [computers] . . . Fuck that attorney [Terpin's lawyer]. They don't have shit on me. . . You think I'm dumb enough to keep all my money in America . . . [Truglia] is a dumb ass . . . and got caught."

49. In the same text session where he is declaring himself invincible, Pinsky demonstrated the wisdom of the adage that "pride comes before a fall." A wannabe Master of the Universe, Pinsky wrote to an African-American: "I'm well off I'm good I don't need extra money I'm set for life . . . You're a dumb nigger I could buy you and all your family . . . **I have 100 million dollars.**"

50. More recently, after being confronted by Plaintiff about his involvement, Pinsky (with the advice of sophisticated legal counsel) sent cryptocurrency, cash, and a watch to Plaintiff without any conditions. As Pinsky and Plaintiff have no other connection to one another other than as stated herein, there was no other reason to repatriate these items—worth roughly \$2 million at the time—other than to make a partial repayment of what he had stolen from Terpin. Pinsky has thereby further admitted his complicity.



### **TERPIN'S DAMAGES**

51. Terpin's cryptocurrency holdings that are the subject of this proceeding are valued in the sum of at least \$23,808,125 consistent with applicable damages law.

52. Plaintiff is entitled at a minimum to interest on the losses, if not greater losses as a result of his inability to use his cryptocurrency holdings to invest the proceeds.

53. In seeking to recover his money, Plaintiff will have incurred substantial attorney's fees, costs, and expenses in a sum to be proven at trial, and in any event no less than \$1,000,000.

54. Plaintiff is entitled to recover from Defendants at least \$23,808,125 (before trebling or punitive damages), subject to credits given consistent with applicable law for any amounts recovered by Plaintiff, plus interest and attorneys' fees consistent with applicable law.

### **NECESSITY OF INJUNCTIVE RELIEF**

55. As noted above, Pinsky has admitted that he has \$100 million of stolen money, presumably in a mix of cash and cryptocurrency. He also reportedly had substantial cash stashed in his bedroom, which was reconfirmed by his inclusion of at least some portion of that cash with the partial sum that he repaid in 2019.

56. Defendants have proven to be skillful professionals at using the internet for stealing and laundering coins and money. They are as dangerous with a computer as armed bank robbers are with guns.

57. Due to the nature of cryptocurrency and Defendants' mastery of cybercrime, Pinsky's assets, including the amounts taken from Plaintiff, could readily be dissipated and lost absent injunctive and other relief preventing any transfer.

## **FIRST CLAIM FOR RELIEF**

### **(Against All Defendants for Violations of Section 1962(c) of the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. § 1962(c))**

58. Plaintiff realleges and incorporates by reference the allegations of Paragraphs 1 through 57 above as if fully set forth herein.

59. This claim for relief arises under 18 U.S.C. § 1962(c) and is asserted against Defendants Pinsky and DOES 1-20.

60. Each of the Defendants, for purposes of this particular cause of action, is or has been a “person” employed by or associated with an enterprise engaged in, or the activities of which affect, foreign or interstate commerce (the “Enterprise”), and as such, has conducted or participated, directly or indirectly, in the conduct of such Enterprise’s affairs through a pattern of racketeering activity as described below.

61. For the purpose of this particular cause of action under Section 1962(c), the Enterprise consists of Defendants Pinsky, non-Defendant Truglia, and DOES 1-20.

62. Since at least 2017, Defendants Pinsky, non-defendant Truglia, and DOES 1-20 and other Enterprise members, knowingly, intentionally, and unlawfully, aided and abetted, and conspired with each other, to devise, or intend, the scheme to defraud cryptocurrency investors and others (including Plaintiff), by which they were to illegally steal their victims’ identities and to illegally obtain and acquire control of victims’ cryptocurrency and other accounts, and to illegally keep those assets for their own benefit and interest.

63. In furtherance of its scheme to defraud, and in order to achieve its objectives, the Enterprise knowingly, intentionally, and unlawfully aided and abetted to commit, attempted to commit, conspired to commit, did commit, and caused to be committed, the below enumerated

overt and/or predicate acts of racketeering activity to illegally steal money from victims, including Plaintiff, through SIM swaps and other subterfuges and to subsequently retain such money.

64. From at least 2017 to the present, for the purpose of executing the Enterprise's scheme to defraud, Defendants Pinsky, non-Defendant Truglia, and DOES 1-20 unlawfully obtained information about victims' mobile phone accounts, including information about security codes and other personal information. The Enterprise then used such information, in combination with false identifications and information obtained through phishing or the Dark Web, to port over a victim's telephone number to a phone under its control. The Enterprise then used their phones to intercept messages to the victim, including 2FA messages, and accessed the victim's accounts to obtain information about cryptocurrency holdings, including private keys. Through this scheme, the Enterprise gained control of victims' online accounts, including cryptocurrency wallets or other accounts, and exfiltrated victims' cryptocurrency to accounts under their own control. The scheme perpetrated on Terpin by Defendants Pinsky, non-defendant Truglia, and DOES 1-20, as alleged in this complaint, is typical of the Enterprise's *modus operandi*.

65. The scheme perpetrated by Defendants Pinsky, non-defendant Truglia, and DOES 1-20 took place in interstate commerce within the United States. Through the conduct described above, in furtherance of the scheme to defraud Terpin and other victims, the members of the Enterprise knowingly, intentionally, and unlawfully, aided and abetted and conspired with each other to violate, and did violate 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1030(a)(4) (Computer Fraud and Abuse Act); New York Penal Law §§ 156.05 (unauthorized use of a computer), 156.10 (computer trespass), 156.27 (computer tampering in the first degree), 156.30

(unlawful duplication of computer related material in the first degree), and 156.35 (criminal possession of computer related material), and other provisions of the New York Penal Law, including New York Penal Law §165.54 (criminal possession of stolen property in the first degree).

66. Through the conduct described above, Defendants Pinsky, non-defendant Truglia, and DOES 1-20 and other Enterprise members, knowingly, intentionally and unlawfully, aided and abetted, conspired to, and each of them in fact did, conduct or participate, directly or indirectly, in the conduct of the Enterprise's affairs, through a pattern of unlawful access to computers in violation of 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1030(a)(4), (Computer Fraud and Abuse Act); New York Penal Law §§ 156.05 (unauthorized use of a computer), 156.10 (computer trespass), 156.27 (computer tampering in the first degree), 156.30 (unlawful duplication of computer related material in the first degree), and 156.35 (criminal possession of computer related material), and other provisions of the New York Penal Law, including New York Penal Law §165.54 (criminal possession of stolen property in the first degree).

67. As a proximate cause of the Defendants' violations, Plaintiff was injured in his property inasmuch he has been the object of theft of his property in violation of law.

68. The injuries suffered by Plaintiff Michael Terpin are reasonably estimated to be in the amount of at least \$23,808,125, with interest accruing from the date each component of said sum was converted by Defendant, subject to credits given consistent with applicable law for any amounts recovered by Plaintiff.

69. Pursuant to 18 U.S.C. § 1964(c), Plaintiff shall recover threefold the damages sustained in an amount of at least \$71,415,375 (*i.e.*, \$23,808,125x3), with interest accruing consistent with applicable law, subject to credits given consistent with applicable law for any

amounts recovered by Plaintiff. In 2019, a Los Angeles County Superior Court Judge assessed such treble damages against Truglia for his participation in the theft of Plaintiff's cryptocurrency in a \$75.8 million judgment.

70. Pursuant to 18 U.S.C. § 1964(c), Plaintiff Michael Terpin is entitled to reasonable attorneys' fees, expenses, and costs in a sum to be proven at trial, and in any event no less than \$1,000,000.

## **SECOND CLAIM FOR RELIEF**

### **(Against All Defendants for Conversion and Conspiracy to Commit Conversion)**

71. Plaintiff realleges and incorporates by reference the allegations contained in Paragraphs 1 through 70 above as if fully set forth herein.

72. At all times mentioned above, Plaintiff was, and still is, the owner and was, and still is, entitled to the possession of cryptocurrency valued in the sum of at least \$23,808,125 consistent with applicable damages law.

73. On or about January 7, 2018, Defendants Pinsky, non-defendant Truglia and DOES 1-20 took and conspired to take the property described above from Plaintiff's possession in the manner described above and converted the same to their own use.

74. As a proximate result of the wrongful conduct of Defendants Pinsky, non-defendant Truglia, and DOES 1-20 as alleged above, Terpin has been damaged in the sum to be proven at trial, but at least \$23,808,125, with interest accruing from the date each component of said sum was converted by Defendant, subject to credits given consistent with applicable law for any amounts recovered by Plaintiff.

75. As a further proximate result of the Defendants' acts alleged above, Terpin has also expended substantial sums of time and money in pursuit of the sums converted by

Defendants. Terpin is presently incurring such amounts in an attempt to recover his converted property. The full amount and extent of those damages are presently unknown. Plaintiff will seek leave to amend this complaint when the full extent and amount of said damages have been ascertained.

76. Defendants Pinsky and DOES 1-20 have engaged in despicable conduct as alleged above with an intent to injure Terpin and to subject him to cruel and unjust hardship in conscious disregard of his rights, and these actions were done fraudulently, maliciously and oppressively. Terpin is therefore entitled to punitive or exemplary damages against Defendants in an amount sufficient to punish and make a public example of each of the Defendants.

### **THIRD CLAIM FOR RELIEF**

#### **(Against All Defendants for Money Had and Received)**

77. Plaintiff realleges and incorporates by reference the allegations of Paragraphs 1 through 76 above as if fully set forth herein.

78. Pinsky and DOES 1-20 received money belonging to Terpin in the amount of a sum to be proven at trial, but at least \$23,808,125 at that time. Defendants Pinsky and DOES 1-20 benefitted from the receipt of that money. Under principles of equity and good conscience, Defendants should under no circumstances whatsoever be permitted to keep that money.

79. The whole of this sum has not been paid back to Plaintiff, and there is now due, owing, and unpaid – as money had and received – the sum to be proven at trial, which is at least \$23,808,125, with interest accruing from the date each component of said sum was converted by Defendant, subject to credits given consistent with applicable law for any amounts recovered by Plaintiff.

#### **FOURTH CLAIM FOR RELIEF**

##### **(Against All Defendants for Replevin)**

80. Plaintiff realleges and incorporates by reference the allegations of Paragraphs 1 through 79, above, as if fully set forth herein.

81. Plaintiff is, and at all times material herein was, the owner of personal property described as the cryptocurrency holdings identified above.

82. Plaintiff is, and at all times material herein was, entitled to immediate and exclusive possession of his cryptocurrency holdings.

83. During and as a direct and proximate result of Defendants' wrongful possession and retention of his cryptocurrency holdings, Plaintiff has suffered the loss of the use and enjoyment of them as well as additional damages in an amount to be proven at trial but in no event less than \$23,808,125, with interest accruing from the date each component of said sum was converted by Defendant, subject to credits given consistent with applicable law for any amounts recovered by Plaintiff.

84. Plaintiff is entitled to immediate return and possession of his cryptocurrency holdings.

85. In doing the acts alleged above, Defendants acted with oppression, fraud, and malice and with the intent to defraud Plaintiff. Accordingly, Plaintiff is entitled to an award of punitive and exemplary damages against Defendants in a sum to be proven at time of trial.

#### **FIFTH CLAIM FOR RELIEF**

##### **(Against All Defendants for Violation of the Computer Fraud and Abuse**

##### **Act, 18 U.S.C. § 1030(a)(4))**

86. Plaintiff realleges and incorporates by reference the allegations of Paragraphs 1

through 85 above as if fully set forth herein.

87. By committing and aiding and abetting the SIM swap described above, Defendants knowingly and intentionally accessed through interstate commerce Plaintiff's mobile telephone and accounts accessible through his mobile device, all of which are protected computers, without authorization and in violation of Plaintiff's rights in his property and privacy.

88. Defendants' activities described above constitute a violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(4). Plaintiff may maintain a civil action against Defendants for violations of the CFAA pursuant to 18 U.S.C. § 1030(g).

89. As a result of the unauthorized activities, Defendants caused a loss to Plaintiff of at least \$23,808,125 in cryptocurrency, with interest accruing from the date each component of said sum was converted by Defendant, subject to credits given consistent with applicable law for any amounts recovered by Plaintiff.

90. Plaintiff has additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy and identity theft.

91. The unlawful access to Plaintiff's mobile computer and online accounts has also caused Plaintiff irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiff's remedy at law is not adequate to compensate him for these inflicted and threatened injuries, entitling Plaintiff to remedies, including injunctive relief as provided by § 1030(g).

#### **SIXTH CLAIM FOR RELIEF**

##### **(Against All Defendants for a Preliminary and Permanent Injunction)**

92. Plaintiff realleges and incorporates by reference the allegations of Paragraphs 1 through 91 as if fully set forth herein.



93. Defendants' possession and control of Plaintiff's cryptocurrency holdings and money, and the substantial threat of loss through transfers to unknown accounts or persons, is causing and will continue to cause Plaintiff great and irreparable harm, for which Plaintiff has no adequate remedy at law.

94. Plaintiff is therefore entitled to a preliminary and permanent order enjoining and restraining Defendants Pinsky and DOES 1-20, and their agents, servants, employees, confederates, co-conspirators, aiders and abettors, and representatives from engaging in, committing, or performing, directly or indirectly, any and all of the following acts: accessing, expending, disbursing, transferring, assigning, pledging, encumbering, concealing, laundering, washing, or in any manner whatsoever disposing of the whole or any part of the cryptocurrency holdings and cash belonging to Plaintiff.

#### **DEMAND FOR JUDGMENT**

WHEREFORE, Plaintiff prays for judgment against Defendants, and each of them, as follows:

1. For the value of the property converted in the sum to be proven at trial, but at least \$23,808,125, subject to credits given consistent with applicable law for any amounts recovered by Plaintiff;
2. For interest thereon at the legal rate from the date of the conversion of each component of the foregoing sum;
3. For additional damages for time and money properly expended in pursuit of the converted property, according to proof;
4. For an order requiring Defendants Pinsky and DOES 1-20, jointly and severally, to return to Plaintiff all assets, funds, and other property derived from such transactions, as well

as any benefits or profits derived therefrom, and to pay Plaintiff any consequential damages caused by these transactions;

5. For an order compelling Defendants Pinsky and DOES 1-20 to reconvey legal title of Plaintiff's cryptocurrency holdings to Plaintiff;

6. For an order requiring Defendants Pinsky and DOES 1-20, and their agents, servants, employees, confederates, co-conspirators, aiders and abettors, and representatives to be enjoined during the pendency of this action, and then permanently enjoined after conclusion of this action, from engaging in, committing, or performing, directly or indirectly, any and all of the following acts: accessing, expending, disbursing, transferring, assigning, pledging, encumbering, concealing, or in any manner whatsoever disposing of the whole or any part of the cryptocurrency holdings and cash belonging to Plaintiff;

7. For punitive or exemplary damages in an amount sufficient to punish Defendants Pinsky and DOES 1-20 and make a public example of them;

8. For treble damages pursuant to 18 U.S.C § 1964(c);

9. For attorney's fees pursuant to 18 U.S.C. § 1964(c);

10. For costs of suit incurred herein; and

11. For such other and further relief as this Court may deem just and proper.

///

///

///

///

///

**DEMAND FOR JURY TRIAL**

Plaintiff demands trial by jury on all claims for relief for which a jury trial is appropriate.

DATED: May 7, 2020

CHEHEBAR DEVENEY & PHILLIPS

and

GREENBERG GLUSKER FIELDS CLAMAN &  
MACHTINGER LLP

By:  (CM-3544)  
CORNELIUS P. MCCARTHY (CM-3544)

By:  (PO-5724)/cm  
PIERCE O'DONNELL ( PO-5724)

Attorneys for Plaintiff  
MICHAEL TERPIN