PIERCE O'DONNELL (SBN 081298)
PODonnell@GreenbergGlusker.com
TIMOTHY J. TOOHEY (SBN 140117)
TToohey@greembergGlusker.com
PAUL BLECHNER (SBN 159514)
PBlechner@GreenbergGlusker.com
GREENBERG GLUSKER FIELDS CLAMAN &
MACHTINGER LLP
1900 Avenue of the Stars, 21st Floor
Los Angeles, California 90067-4590
Telephone: 310.553.3610
Fax: 310.553.0687

Attorneys for Plaintiff
MICHAEL TERPIN

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF LOS ANGELES

CENTRAL DISTRICT

MICHAEL TERPIN,

Plaintiff,

v.

NICHOLAS TRUGLIA,

Defendant.

Case No. 18STCV09875

Honorable Barbara M. Scheper
Dept. 30

DECLARATION OF MICHAEL TERPIN IN SUPPORT OF PLAINTIFF'S EX PARTE MOTIONS FOR TEMPORARY RESTRAINING ORDER, WRIT OF ATTACHMENT, TEMPORARY PROTECTIVE ORDER AND EXPEDITED DISCOVERY

Date: December 31, 2018

Dept:

Time: 8:30 a.m.

I, MICHAEL TERPIN, hereby declare and state as follows:

1. I am the Plaintiff in this lawsuit. I have a residence in Los Angeles County, California. I obtained wireless services from AT&T Mobility, Inc. ("AT&T") in Los Angeles County in or about the mid-1990s. At all times relevant to this lawsuit, I received wireless

services from AT&T for a telephone number with a Southern California area code.

Cryptocurrency

2. I have been active with cryptocurrency and in the cryptocurrency community. I have been a cryptocurrency investor for numerous years and have been a thought leader and publicist in the blockchain sector. I co-founded the first angel group for bitcoin investors, BitAngels, in early 2013, and the first-ever digital currency fund, the BitAngels/Dapps Fund, in March 2014. I am currently a senior advisor to Alphabit Fund, one of the world's largest digital currency hedge funds. I have worked with more than 100 cryptocurrency token crowdsales, including Augur, Bancor, Ethereum, Gnosis, Golem, MaidSafe, Neo and Qtum. I am the founder and CEO of Transform Group, the leading PR and advisory company for the public blockchain industry and have organized the long-running CoinAgenda global investor conference series and monthly TokenMatch investor events.

3. I am very familiar with cryptocurrency, with cryptocurrency transactions and exchanges, and with the phenomenon of SIM swaps from my extensive involvement in the industry and through personal experience.

4. Cryptocurrency (also known as "crypto," "coins" or "tokens") is digital or virtual currency which can be used as a medium of exchange in which encryption techniques verify the transfer of funds through an encrypted and decentralized ledger called a "blockchain." The blockchain records transactions and manages any issuance of new units of currency within a consensus algorithm. Cryptocurrency is typically decentralized, operates independently of a central bank or other regulatory authority, and is often traded by parties through centralized businesses called "exchanges" (similar to an online stock brokerage, but for cryptocurrency). Once a transfer of cryptocurrency has occurred outside of an exchange, it is difficult to trace and impossible to reverse the transaction without possession of certain "private" key numbers held only by the transferor.

5. In recent years, the cryptocurrency community has been hit with thefts by hackers that occur through the process of "SIM swaps." A "SIM swap" is a practice whereby a hacker gains access to a victim's telephone account to intercept communications, including text

messages, to the mobile telephone, effectively putting them in control of the target's digital life. A perpetrator of a SIM swap typically arranges through bribery of someone (such as an employee or contractor of a telephone carrier) with access to customer information 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 victim's phone number, now under the hacker's control, to impersonate the victim with service providers, such as e-mail providers and cryptocurrency exchanges, 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.

6. Perpetrators of SIM swap fraud frequently intercept 2FA or "2-Factor Authentication" messages (where the second factor is a text message sent to the user's telephone number listed on the account) sent to the victim's telephone number. 2FA is frequently used as a security mechanism for authentication purposes. Perpetrators of SIM swaps intercept the messages to gain access to the accounts owned by the victim, including cryptocurrency accounts or other accounts that provide 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. At this point, it is impossible to reverse the transfer.

7. The perpetrators of SIM swap fraud specifically target victims owning cryptocurrency because of the nature of cryptocurrency transactions. The digital assets embodied by cryptocurrency are a medium of exchange that uses 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 paired with a public key using a long-standing technology known as "public key cryptography," is used to write in the public ledger to transfer cryptocurrency but is not displayed publicly. The private key is a secret number, which is typically filed in a "wallet." Because the key can be used to "spend" cryptocurrency, owners of cryptocurrency typically keep such keys secure. Such keys are complex. For example, in Bitcoin a private key is a 256-bit number, which translates to 64 characters.

8. Holders of cryptocurrency frequently store their private keys in a cryptocurrency

"wallet." One type of wallet is a "hardware wallet" which stores the user's private keys in a secure hardware device. "Trezor" is a type of hardware wallet for handling cryptocurrency private keys. A Trezor device may be used to transfer cryptocurrency without exposing private keys to online and offline risks.

9. Once a transfer of cryptocurrency has occurred, it cannot be reversed. Although the transaction is displayed in a public ledger, it is not easy to identify the transferor or transferee without knowing the parties' private keys. Cryptocurrency thus makes an attractive target for perpetrators of SIM swap fraud because the perpetrators can transfer stolen digital assets to other addresses or wallets in transactions that are not readily traced and are irreversible. Moreover, the transferred cryptocurrency can then be accessed anywhere in the world free from government regulation or inspection

My January 7, 2018 SIM Swap

10. On January 7, 2018, my phone with my AT&T wireless number went dead. As I later learned from my discussions with AT&T, an AT&T employee on that date had ported over my wireless number to an imposter on a new SIM card. Through the hack, the thief or thieves gained control over my accounts and stole nearly $24 million worth of cryptocurrency from me on January 7 and 8, 2018.

11. I have discovered in recent weeks that the primary perpetrator of my SIM swap on January 7, 2018 was Defendant Nicholas Truglia.

12. Through this hack, I lost at least $23,808,125 worth of crypto currency. Because cryptocurrency has a fluctuating value, I believe that I am entitled under California law to the highest market value of the currencies that were stolen or later converted to Bitcoin. I have always been a strategic investor in cryptocurrency and would have pursued other investment opportunities to protect my gains from market fluctuations. Based on prices from coinmarketcap.com, which averages exchange prices, and actual exchanges, such as Bittrex or Binance, I calculate my losses as follows:

Currency	**# Coins**	**Price at Conversion**	**Conversion Date**	**Highest Price**	**Date of High**	**Loss in USD**
Triggers	3,000,000	$7.577	1/7/18	$7.577	1/7/18	$22,731,000.00
Sky	20,000	$48.41	1/7/18	$49.55	1/10/18	991,000.00
Steem	12,500	$6.48	1/7/18	$6.89	1/25/18	86,125.00
TOTAL						**$23,808,125.00**

The "Currency" column in this chart corresponds to the types of cryptocurrency stolen from me on January 7-8, 2018. The "# Coins" column is the amount of that currency that I held, the "Conversion Date" is the date that the SIM swap occurred, and the "Loss in USD" corresponds to the approximate US dollar value of the cryptocurrency at its highest point at or after the conversion. Although I strongly believe that I am entitled to the value using the highest interim price, this legal argument does not substantially impact the total calculation and I note that that value of the stolen cryptocurrency using the price on the date of conversion was $23,780,200.00. I also note that I may be entitled to costs and attorney fees in the action that I am bringing against Nicholas Truglia, but that for purposes of these motions, I am limiting my attachment to $23,780,200.00, without in any way waiving my right to obtain additional amounts, including attorney fees and costs for the claims set forth in my complaint.

13. I am informed that, at Truglia's bail hearing on December 18, 2018, the Court read on the record from a filing submitted by the prosecution that indicate that there had been a forensic search of Truglia's iCloud backup file and that the prosecution had found a number of documents that include: (a) texts in 2017 in which Truglia was complaining to his dad about a lack of money and requesting for money for food, train tickets, and other items, (b) a text from Truglia to his dad on January 7, 2018 (the day my SIM card was swapped and my hack began) in which Truglia stated that he had just made money and that important things were happening, (c) a text on the same day from Truglia to another individual that Truglia had stolen a wallet that has at least $20 million in it, (d) a text by Truglia to another person stating that Truglia is a millionaire, that he isn't kidding, and he has 100 Bitcoin, and (e) a text by Truglia in January 2018 in which he states that his life changed forever and offers to take this person to the Superbowl. I expect to

be able to secure all of these texts and other documents similar in nature, which corroborate and further support the evidence submitted at this time in showing Truglia's central involvement in the theft of my cryptocurrency in January 2018.

14. A Trezor is a small, hand-held computer-type device on which the owner holds cryptocurrency and can be used to transfer and sell those cryptos through the internet. A Trezor can be likened to a private safe or safety deposit box at a financial institution. When Truglia was arrested, the police seized one of his Trezors containing a substantial amount of cryptos worth millions of dollars. That Trezor is in the possession of the Santa Clara District Attorney or Sheriff.

15. I have brought this lawsuit as part my ongoing effort to recover my losses caused by the perpetrators of the January 7, 2018 theft. Based on the evidence as it now stands without discovery, particularly the Declaration of Chris David, I believe that Truglia has assets, including US dollars, cash, and cryptos, that are held in various accounts at JP Morgan, TD Ameritrade, and Gemini, among others, and on his Trezor mentioned above. On the same basis, I believe that there is a substantial risk that Truglia will transfer and seek to conceal this money and assets unless they are immediately attached and frozen pending the outcome of this litigation.

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

Executed in San Juan, Puerto Rico on December 30, 2018.

MICHAEL TERPIN