

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

In the Matter of the Search of the Premises
Located at 600 Coral Way, Suite/Floor 12,
Segovia Tower, Coral Gables, Florida, 33134

TO BE FILED UNDER SEAL

**Agent Affidavit in Support of
Application for Search Warrant**

SOUTHERN DISTRICT OF FLORIDA) ss.:

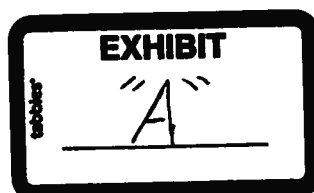
Kurt Hafer, Special Agent, United States Attorney's Office for the Southern District of New York, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am currently employed as a Special Agent in the Securities and Commodities Fraud Task Force at the United States Attorney's Office for the Southern District of New York, and I have been employed in this position since approximately February 2016. Prior to that date, I was employed as a Criminal Investigator at the United States Department of Energy's Office of Inspector General for approximately six and a half years. During my tenure with both offices, I have participated in numerous investigations of financial crimes and complex frauds, and have been investigating the current matter since approximately March 2016. I have participated in the execution of search warrants involving physical premises, electronic devices, and other electronic evidence.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises specified below (the "Subject Premises"), for the items and information, as described in Attachment A. The information contained in this affidavit is based on, among other sources of information: (i) my personal knowledge; (ii) information provided by law enforcement officers at the Internal Revenue Service



("IRS"), the Federal Bureau of Investigation ("FBI"), and the New York County District Attorney's Office participating in the same investigation; (iii) my review of publicly available OneCoin promotional materials; (iv) information that I have obtained from international law enforcement authorities pursuant to Mutual Legal Assistance Treaty ("MLAT") requests and other requests to foreign authorities; (v) my review of OneCoin's publicly available website and materials available on that website; (vi) open source research that I have conducted on the Internet; (vii) my review of digital videos posted on www.youtube.com ("YouTube") by OneCoin Ltd. and its members; (viii) my participation in various witness interviews; (ix) my review of e-mail evidence obtained pursuant to subpoenas, MLAT requests, judicially authorized search warrants, and a judicially authorized wiretap; (x) the review and analysis of various bank account records, including financial records obtained from international law enforcement authorities pursuant to MLAT requests and other requests to foreign authorities, conducted by myself, a paralegal I work with in the U.S. Attorney's Office, an IRS law enforcement agent, and officials at the New York County District Attorney's Office; and (xi) my training and experience concerning the commission of financial crimes, the use of computers in criminal activity, and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is prepared for the limited purpose of establishing probable cause, I have not set forth each and every fact I have learned in connection with this investigation. Where communications and events are referred to herein, moreover, they are related in substance and in part. Where dates, figures, and calculations are set forth herein, they are approximate.

B. The Subject Premises

3. The Subject Premises is particularly described as a residential condominium unit located on the 12th floor of Segovia Tower at 600 Coral Way, Coral Gables, Florida 33134. Segovia Tower is a terracotta-colored, 15-floor, 14-unit condominium building overlooking a golf

course and downtown Coral Gables, with a pool and gym. The Subject Premises occupies the entire 12th floor of Segovia Tower and, according to publicly-available information, is a 3850 square-foot, 4-bedroom, 3.5 bath unit with an open-air terrace. A search of public property records revealed that the Subject Premises is owned and occupied by MARK S. SCOTT, who is a defendant in a sealed Indictment, attached hereto as Exhibit 1, and a target of this ongoing investigation.

C. The Subject Offenses

4. For the reasons detailed below, I submit that there is probable cause to believe that the Subject Premises contain evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, §§ 1956(a)(1)(B)(i), 1956(a)(2)(B)(i), 1956(h), and 1344 (money laundering, conspiracy to commit money laundering, and bank fraud related activity in connection with a pyramid scheme), relating to SCOTT's laundering hundreds of millions of dollars of fraudulent proceeds of a massive international pyramid scheme involving a purported crypto-currency called OneCoin (the "Subject Offenses").

II. Probable Cause

A. Probable Cause Regarding Commission of the Subject Offenses

5. On August 21, 2018, the Government filed under seal a one-count Superseding Indictment, captioned *United States v. Mark S. Scott*, S6 17 Cr. 630 (the "Indictment"), charging SCOTT with a violation of Title 18, United States Code, § 1956(h). The Indictment is attached hereto as Exhibit 1, and is incorporated by reference herein.

Overview of SCOTT's Scheme to Launder OneCoin Fraud Proceeds

6. As described in greater detail below, in or about 2014, OneCoin Ltd. was founded by two co-conspirators not named herein ("CC-1" and "CC-2"). OneCoin Ltd. markets a purported digital cryptocurrency called "OneCoin" through a multi-level-marketing network. OneCoin

members receive commissions for recruiting others to purchase cryptocurrency packages. This multi-level marketing structure appears to have influenced rapid growth of the OneCoin member network. Records that I have obtained in the course of the investigation show that, between the fourth quarter of 2014 and the third quarter of 2016, OneCoin Ltd. generated €3.353 billion in sales revenue and earned “profits” of €2.232 billion. OneCoin continues to operate to this day.

7. As detailed below, the evidence demonstrates that OneCoin Ltd. is a pyramid fraud scheme. For example, in contrast to public representations made to investors by OneCoin Ltd., OneCoins are not “mined” by members, nor is the value of OneCoin determined by market supply and demand. Beyond these misrepresentations, OneCoin Ltd. exhibits a variety of other features, described below - including the fact that OneCoins have never been tradable on a public exchange - indicating that it is a fraud scheme and not a legitimate business.

8. SCOTT, a United States citizen and former partner of an international law firm, engaged in a scheme to launder hundreds of millions of dollars of OneCoin fraud proceeds between approximately 2016 and 2018.

9. In or about February 2016, SCOTT first met with one of the founders of OneCoin, Ltd. Shortly thereafter, SCOTT set up a series of hedge funds incorporated in the British Virgin Islands with accounts at banks located in the Cayman Islands. Between approximately June 2016 and February 2017, SCOTT’s hedge funds received the U.S. dollar equivalent of approximately \$400 million in OneCoin proceeds. SCOTT misrepresented the source of the funds to a fund administration firm and to at least one of the Cayman Islands banks. SCOTT ultimately transferred a significant portion of the funds to related bank accounts in the Republic of Ireland, again lying to the bank regarding the reason for the transfers. In one case, SCOTT issued a purported “loan” of €30 million from one of the hedge funds to an account in Hong Kong, allegedly for the purchase

of an oil field. Records obtained pursuant to a judicially authorized e-mail search suggest that €10 million of these funds were transferred to an account held by one of the founders of OneCoin Ltd. There is no evidence that the purported "loan" was ever repaid.

10. As part of the scheme, at least \$15.5 million of the OneCoin proceeds sent to the hedge fund accounts was remitted, either directly or indirectly, to bank accounts in the United States held in SCOTT's name, or controlled by SCOTT. The evidence shows that SCOTT used the monies he received from the hedge fund accounts for personal expenses and to fund large luxury purchases, including sports cars and designer watches.

Background on OneCoin Ltd.

11. Based on my review of publicly available OneCoin promotional materials, records and information that I have obtained pursuant to MLAT requests and other requests to foreign authorities, publicly available information about OneCoin, my participation in various witness interviews, my review of e-mail evidence obtained pursuant to subpoenas, MLATs, judicially authorized search warrants, and a judicially authorized wiretap, and my review and analysis of various bank account records, I have learned the following:

a. OneCoin Ltd. was founded in or about April 2014 in Gibraltar and maintains offices throughout the world, including in Bulgaria, the United Arab Emirates ("UAE"), and Hong Kong.¹ OneCoin Ltd.'s founders are CC-1 and CC-2. OneCoin Ltd. markets a digital cryptocurrency called OneCoin through a multi-level-marketing network of OneCoin members. OneCoin Ltd. has promoted various different "trader packages" priced at, for example, €110 and €55,500 euros, including "starter" packages and "tycoon trader," "premium trader," "infinity

¹ I have learned that OneCoin operates using several corporate entities and d.b.a. names, to include "OnePayments Ltd.," "OneNetwork Services Ltd.," "OneAcademy," and "OneLife." In this affidavit, I refer to these entities and d.b.a. names collectively as "OneCoin Ltd."

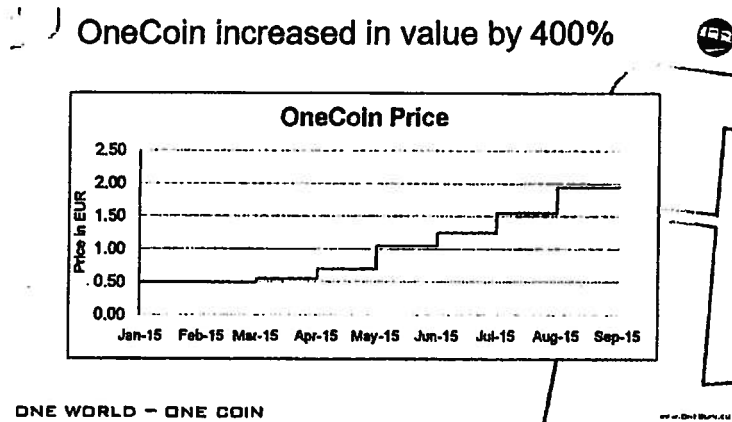
trader,” and “super combo” packages. Purchase of a trader package provides access to “educational materials” and “tokens.”

b. According to OneCoin Ltd.’s promotional materials, “tokens” are used to secure positions in OneCoin’s “mining pools,” depicted in promotional materials as computer hardware used to “mine” OneCoins.² Promotional materials also claim that OneCoin Ltd. “ensures” these mining resources and that two mining servers are located in Bulgaria and a third in Hong Kong. Consistent with other cryptocurrencies such as Bitcoin, OneCoin Ltd.’s promotional materials claim that the mining difficulty of OneCoin increases over time, as additional computer resources, and thus more tokens, are needed to mine a single OneCoin. Once a OneCoin member “mines” OneCoins using his or her tokens, the resulting OneCoins are deposited into the member’s account and may be accessed by logging in through a website operated by OneCoin Ltd.

c. OneCoin Ltd. claims that the value of OneCoin is based on market supply and demand. In or about June 2016, in a OneCoin promotional video posted on YouTube, CC-1 stated: “We discussed several times how the value of cryptocurrency comes. Cryptocurrency is not backed up. It is . . . an asset where demand and supply drive the price. Now, one of the drivers of the coin is, of course, the brand. Brand, of course, is how many people know about OneCoin? How many people use OneCoin? How spread are we worldwide?” An official press release issued by OneCoin Ltd. on or about October 1, 2016, announcing a so-called OneCoin “split,” stated in

² In the context of a legitimate cryptocurrency, “mining” refers to the process of adding carefully reviewed transaction records to the cryptocurrency’s ledger of past transactions, i.e., the “blockchain.” The primary purpose of mining is to allow the cryptocurrency’s nodes to reach a secure, tamper-resistant consensus. Mining is also the mechanism used to introduce cryptocurrency “coins” into the system. “Miners” are paid any transaction fees as well as a subsidy of newly created coins. This both serves the purpose of disseminating new coins in a decentralized manner, as well as motivating miners to provide security for the system.

part: “Cryptocurrency value is driven by supply and demand – and demand is driven by brand and usability. By doubling the coins, we will be able to bring the coin to more people and places and strengthen the brand.” Another press release, issued by OneCoin Ltd. on or about December 2, 2016, stated in part: “The value of each cryptocurrency depends on its usability, supply and demand. With over 2.7 million users OneCoin has one of the biggest user bases.” The purported value of a OneCoin has steadily grown from €0.50 to presently approximately €20.75 per coin. The chart below — which used as part of a presentation slide deck at a large OneCoin event in Macau, in or about October 2015 – plots the purported increasing value of OneCoin throughout 2015.



d. OneCoin Ltd. claims to have a private “blockchain,” or a digital ledger identifying OneCoins and recording historical transactions.³ OneCoin Ltd.’s private blockchain may be contrasted with Bitcoin’s blockchain, which is decentralized and public. At a promotional event in Dubai on or about May 15, 2015, CC-1 represented that the OneCoin blockchain was audited, stating, in part:

³ In the context of a legitimate cryptocurrency, a “blockchain” refers to the cryptocurrency’s public ledger of all past transactions. A full copy of a currency’s blockchain contains every transaction ever executed in the cryptocurrency. The blockchain serves to confirm to the rest of the cryptocurrency’s network that transactions have taken place.

We all know it is a very bad world outside. So many people making promises. So many people lying. So many people doing things and not delivering. So, what we did in the last months is we hired an auditor to audit our blockchain. And, ah, I am very proud to say that the result of the first audit is here.

CC-1 then introduced the alleged auditor of the OneCoin blockchain. The auditor subsequently provided an opinion that “all transactions are included in the blockchain (no coins are mined outside the blockchain).”

e. As noted above, OneCoin Ltd. operates a multi-level marketing structure, through which individuals are compensated for recruiting new members who purchase OneCoin trader packages. In an online video, CC-1 attributed the multi-level marketing structure plan to CC-2. CC-2 has promoted OneCoin, including at official OneCoin events, and self-identifies as OneCoin’s “Master Distributor 001.” I believe that “001” may be a reference to CC-2’s position at the top of the OneCoin Ltd. network-marketing pyramid.

f. OneCoin members receive a commission of between 10% and 25% of the value of the trader packages purchased by individuals they recruit to OneCoin. However, only 60% of commissions paid to members are withdrawable in cash; the remaining 40% are deposited in a “trading account” which may only be used to purchase either OneCoins or more tokens. OneCoin Ltd.’s multi-level marketing structure appears to have influenced rapid growth in the number of OneCoin members. OneCoin Ltd. regularly hosts large conferences in locations such as London, Bangkok, Dubai, and Macau, and presently claims to have over 3.3 million members worldwide, including approximately 48,000 members located in the United States.

g. OneCoin Ltd. continues to operate to this day.

OneCoin is a Fraudulent Scheme

12. As the result of judicially authorized search warrants, I have obtained and reviewed e-mails between CC-1 and CC-2 regarding the OneCoin scheme. I believe that the e-mail evidence

described in the paragraphs below demonstrates, among other things, that: (i) CC-1 and CC-2 conceived of and built the OneCoin business fully intending to use it to defraud investors; (ii) contrary to OneCoin Ltd.'s public representations, the value of OneCoin is determined internally and not based on market supply and demand; and (iii) contrary to OneCoin Ltd.'s public representations, OneCoins are not mined but are instead auto-generated on a monthly basis at a constant rate, and then distributed to members on an as-needed basis.

13. The following e-mails between CC-1 and CC-2, among other evidence, demonstrate that CC-1 and CC-2 conceived of and built the OneCoin business fully intending to use it to defraud investors:

a. In the summer of 2014, CC-1 and CC-2 were developing the concept and payout plan for OneCoin, which they referred to at the time in e-mail correspondence as "trashy coin." On June 11, 2014, CC-1 wrote to CC-2 concerning the OneCoin business plan:

It might not be [something] really clean or that I normally work on or even can be proud of (except with you in private when we make the money) – but . . . I am especially good in this very borderline cases [sic], where the things become gray – and you as the magic sales machine – and me as someone who really can work with numbers, legal and back you up in a good and professional way – we could really make it big – like MLM meets bitch of wall street ;-)

* * *

Your main sales argument is: **after 2 splits a member makes out of 5.000 USD 25.000 USD. You should be able to sell this ☺ . . .** I also added an **Extra Bonus for all members joining the Presales** . . . they can do actually 3 splits. Which means that they will actually **have 10x their investment**. 2 splits is 5x your money. So of course, everybody who is greedy will go in with 5.000 USD.

(bold in original). I believe this e-mail demonstrates that CC-1 developed OneCoin Ltd.'s unsustainable compensation structure for the purpose of enticing people to invest in OneCoin

trader packages, including the false promise that investors would make a five-fold or ten-fold investment return.

b. On or about August 9, 2014, CC-1 sent an e-mail to CC-2 in which CC-1 described CC-1's thoughts on the "exit strategy" for OneCoin. The first option CC-1 listed was, "Take the money and run and blame someone else for this (standard approach, see Wenyard)." I believe that by "Wenyard," CC-1 was referring to a separate multi-level marketing scheme by the same name, which multiple sources online describe as both a scam and Ponzi scheme.

14. I believe that the following evidence, including e-mails between CC-1, CC-2, and others, demonstrate that – contrary to OneCoin Ltd.'s public representations – the value of OneCoin is determined internally and not based on market supply and demand:

a. On or about June 9, 2014, in an e-mail sent by CC-1 to a representative of a blockchain development company, copying CC-2, CC-1 stated: "we are building our own cryptocurrency – and would like to set up an internal exchange service for them. We would like to be able to set the price manually and automatically and also control the traded volume."

b. On or about March 21, 2015, CC-1 wrote an e-mail to CC-2, in which CC-1 stated: "We can **manipulate the exchange** by simulating some volatility and intraday pricing." (bold in original). I believe that this e-mail refers to the intention of CC-1 and CC-2 to manipulate the price of OneCoin on OneCoin's private exchange to create the false appearance that the value fluctuated based on trading.

c. On or about August 1, 2015, CC-1 wrote an e-mail to CC-2, and included as part of a section of the e-mail entitled "Goals": "6. Trading coin, stable exchange, always close on a high price end of day open day with high price, build confidence – better manipulation so they are happy." I believe that this e-mail refers to CC-1's plan to manipulate the price of OneCoin

on OneCoin's private exchange in order to deceive investors into believing that OneCoin was a good investment.

d. Moreover, I have reviewed the graph displayed above in paragraph 11(c), showing OneCoin's purported increase in value between January 2015 through September 2015. That graph looks like a step function, with an increasing price at approximately one-month intervals. The graph is consistent with the price of the OneCoin being set – or manipulated – to increase at approximately one-month intervals, and is not consistent with the expected plot of a commodity with a price actually determined by market supply and demand.

15. I believe that the following evidence, including e-mails between CC-1 and CC-2, demonstrate that – contrary to OneCoin Ltd.'s public representations – OneCoins are not mined but are instead auto-generated on a monthly basis at a constant rate, and then distributed to members on as as-needed basis:

a. Beginning in or about August 2014, CC-1 and CC-2 developed the idea of marketing to members that tokens could be used to “mine” OneCoins. In an e-mail to CC-2 dated August 11, 2014, CC-1 proposed: “Get members to think that they are mining their OneCoin via crunching (exchanging) tokens for OneCoin. This storey [sic] is good as ppl will then not go super crazy and just try and sell tokens all the time.” CC-2 e-mailed CC-1 the following day, writing, “The concept of converting tokens into OneCoin is an important phase for validity and truth behind the OneCoin. The so called ‘mining’ of coins is a concept that is very familiar in the industry and a story we can sell to the members.” CC-1 then wrote to CC-2, “We are not mining actually – but telling people shit,” to which CC-2 responded, “how can this be investigated and found out?” and “Can any member (trying to be clever) find out that we actually are not investing in machines to mine but it is merely a piece of software doing this for us?” The fact that OneCoins are not created

using mining hardware but instead are generated using “a piece of software” is wholly inconsistent with the mining process CC-1 and CC-2 publicly represented to OneCoin Ltd. members.

b. At the end of the following week, on or about August 22, 2014, CC-1 wrote an e-mail to CC-2 summarizing progress made on various OneCoin Ltd. projects. In this e-mail, CC-1 wrote:

I am personally very unhappy – and feel that the future, regardless of what happens with onecoin is not really an exciting one – and nothing to be proud of. I have done mayn [sic] bad things in my life, many stupid things, many things that were borderline – but nothing that I was partly ashamed of – and it actually destroys part of who I am. The damage is done. I have to somehow live with it. But it is something that really upsets me.

c. On September 6, 2014, CC-1 wrote to CC-2, reporting that “last night our Indian friend got back to me on the OneCoin. Coin is ready, tmr the blockchain will be.” I believe this e-mail refers to CC-1 procuring the OneCoin code and its blockchain from a third party. In the same e-mail, CC-1 suggested CC-1 and CC-2 should decide upon the number of OneCoins to be generated every 10 minutes. Specifically, CC-1 suggested two scenarios, one of which envisioned that 10,000 OneCoins would be generated every 10 minutes. Assuming 30 days per month, this rate equates to the generation of 43,200,000 OneCoins per month. I believe this e-mail to be inconsistent with how OneCoin Ltd. marketed OneCoin mining to members, and instead corroborates CC-2’s previously described e-mail, in which CC-2 acknowledged that OneCoins were generated through software.

d. By approximately March 2015, CC-1 and CC-2 appear to have started allocating to OneCoin members coins that did not exist in the OneCoin “blockchain.” Specifically, on March 19, 2015, CC-1 e-mailed CC-2, writing: “We have an **auditor in place** – but I think I cannot start auditing, as I cheat currently on coins, I need to find a way.” (bold in original). By at

least June 2015, CC-1 and CC-2 began e-mailing one another models tabulating current and projected future trader package sales volumes, along with outstanding tokens and OneCoins. The spreadsheets identify separate lines for “mined coins,” “mined coins (real),” and “fake coins.” I believe the references to “fake coins” in these records refer to OneCoins that had been distributed to members but did not exist in the OneCoin “blockchain.” I also believe CC-1’s March 19, 2015 e-mail referring to the need to “cheat . . . on coins” is also a reference to the existence of fake coins at that time.

e. The spreadsheets that CC-1 and CC-2 shared with one another containing references to “fake coins” also describe the projected future supply of OneCoins. Analysis of the projected growth rate in these models shows that the OneCoin supply was projected to grow linearly over time, at a rate of precisely 43,200,000 OneCoins every month. This rate matches that proposed by CC-1 when CC-1 initially ordered the OneCoin software from a third-party vendor. I believe these models further demonstrate that OneCoins are not mined through use of extensive mining hardware, as is marketed to its members, but instead are automatically generated through software.

f. On or about August 6, 2015, CC-1 wrote to CC-2 an e-mail with subject line “I am afraid this is an issue,” and writing further in the body of the e-mail:

This is the implication from the big sales 4 weeks ago. 1.3 [billion] fake coins. We are fucked, this came unexpected and now needs serious, serious thinking.

g. I am not aware of any evidence that CC-1 or CC-2 ever disclosed the existence of fake OneCoins to the purported blockchain auditors or to OneCoin Ltd. investors.

16. In addition to the evidence described above, OneCoin Ltd. exhibits multiple additional features demonstrating that it is a fraudulent scheme. Specifically:

a. OneCoin Ltd. appears to be operating on an insolvent business model, if not for the restraints imposed on users to exchange OneCoins for euros. For example, in or around July 2016, OneCoin Ltd. introduced the “Ultimate Package.” In a promotional video publicly circulated online, CC-1 identified this trader package’s price as €118,000 and stated that each package would generate over two million OneCoins for its purchaser. At the time, a OneCoin was purportedly valued in excess of €5; thus, the value of this package was worth over €10,000,000. The offering and sale of such packages is not economically sustainable unless OneCoin Ltd.’s members do not exchange OneCoins for euros or the value of OneCoin collapses.

b. As noted above, OneCoin Ltd. marketed an event referred to as a “split” to entice members to purchase new or additional trading packages. When a split occurred, a member’s existing balance of tokens – directly linked to the number OneCoins the member could “mine” – would instantaneously double. In one instance, OneCoin Ltd. even doubled the balances of all members’ OneCoin balances. Such “splits” never resulted in a corresponding downward adjustment in the price of OneCoin.

c. OneCoins have never traded on an open exchange, and instead traded only briefly on OneCoin Ltd.’s private exchange, Xcoinx.com. Beginning sometime in or around January 2017, Xcoinx.com has been listed as “under maintenance” and therefore unavailable to OneCoin investors. Even when Xcoinx.com was operational, OneCoin Ltd. restrained the flow of real currency out of OneCoin Ltd. by its members. For example, OneCoin Ltd. limited sell orders to exchange OneCoins for euros to a daily maximum of 1.5% of the member’s total OneCoins. Furthermore, not all sell orders submitted to Xcoinx.com were executed. Thus, the ability to convert OneCoins into other currencies has been severely limited.

d. The ability of OneCoin Ltd. members to profit from selling OneCoins also exhibits indicators of a Ponzi scheme. Specifically, while the Xcoinx.com exchange was operating, the vast majority of OneCoin buyers apparently used so-called “trading account” funds, and not cash account funds, to purchase OneCoins. Thus, OneCoin Ltd. members’ ability to convert OneCoins into cash was dependent upon the continued flow of revenues from the sale of trader packages to new members, which resulted in the payment of commissions to such “trading accounts.”

e. Finally, multiple sources on the Internet, including established news outlets, have publicly described OneCoin Ltd. as a scam and/or Ponzi scheme. The evidence provided supporting these claims often includes one of more of the following: (i) investors’ difficulty selling OneCoins to recoup their original investments; (ii) the fact that OneCoin Ltd.’s blockchain is private and non-transparent; (iii) analysis of OneCoin “blockchain” transactional information published by OneCoin Ltd., which appears to be inconsistent with a real blockchain; and (iv) inaccurate or misleading claims made by OneCoin Ltd. principals or network leaders when marketing OneCoin trader packages to members or prospective investors.

Financial Investigation of OneCoin Proceeds

17. Based on my review and analysis of various bank account records and financial analyses performed by a U.S. Attorney’s Office paralegal and a New York County District Attorney’s Office analyst working with me on this investigation, information obtained from MLAT requests and other requests to foreign authorities, open source research that I have conducted on the Internet, my review of e-mail evidence obtained pursuant to subpoenas, MLATs, judicially authorized search warrants, and a judicially authorized wiretap, I have learned the following:

a. New OneCoin members purchase trader packages by either wiring money directly to a bank account controlled or used by OneCoin Ltd., or by paying a pre-existing OneCoin member who then transmits the funds to OneCoin Ltd. or directly to CC-1. I have discovered accounts located in Bulgaria, the UAE, Georgia, Germany, the United Kingdom, the United States, Tanzania, Hong Kong, and Singapore, which OneCoin Ltd. and its promoters have used for the purpose of receiving investment funds from members purchasing its trader packages.

b. I have obtained OneCoin Ltd. financial and accounting records detailing revenue, profits, gross margin, and other information from the fourth quarter of 2014 through the third quarter of 2016. During this period, OneCoin Ltd. purported to have generated €3.353 billion in sales revenue, and to have earned “profits” of €2.232 billion. The records show that approximately 60% of that revenue was from OneCoin members residing in China, about 18% from Europe, 15% from Australia, and the remainder from the rest of the world; according to the records, approximately 3% of that revenue came from investors in North America and the Caribbean.

c. To date, I have identified and attempted to trace approximately \$1.2 billion in OneCoin Ltd. investor funds, a substantial part of which has been laundered through financial institutions located in at least 21 different countries, including Hong Kong, Singapore, the United States, the Cayman Islands, the Republic of Ireland, and the country of Georgia. Although my tracing analysis is ongoing, I have identified multiple transactions that directly benefited CC-1 and CC-2.

d. For example, I have identified approximately \$50 million of OneCoin Ltd.-sourced funds sent through bank accounts in the United States to an international bank account (“International Account-1”). Once received in International Account-1, the funds were combined

with: (i) other OneCoin funds sourced from bank accounts in Hong Kong controlled by a Chinese OneCoin promoter; and (ii) funds from another international OneCoin Ltd. bank account. These monies were then used to credit an international bank account held by CC-2 (the "CC-2 Account") in the sums of \$39.6 million and €26.8 million. The CC-2 Account, aside from being used to make numerous personal transactions, funded outgoing wire transfers to other accounts held in CC-2's name, specifically, over €3 million crediting a second international bank account, over €4 million crediting a third international bank account, and €2 million crediting a fourth international bank account.

e. I have separately identified approximately €6.1 million of OneCoin Ltd. sourced funds sent from accounts in Bulgaria and Hong Kong to two accounts held in the name of CC-1 in the UAE. Additionally, I have identified that OneCoin Ltd. sourced funds were used at CC-1's direction to make multiple large equity investments outside of the United States.

SCOTT's Background

18. Based on my review of publicly-available documents, e-mail evidence obtained pursuant to judicially authorized search warrants, and records obtained pursuant to MLAT requests, I have learned the following:

a. SCOTT is an attorney and a member of the Florida Bar, presently in good standing, and served as a partner of an international law firm (the "Law Firm") through approximately August 2016. During all times relevant to this search warrant affidavit, SCOTT also served as the manager, registered agent, and ultimate beneficial owner of MSS International Consultants LLC ("MSSI LLC"), an entity registered with the State of Florida.

b. MSSI LLC is the owner of MSS International Consultants (BVI), Ltd. ("MSSI LTD"), an Approved Fund Manager registered in the British Virgin Islands. MSSI LTD

owned and operated a series of investment funds, including Fenero Equity Investments L.P. ("Fenero"), Fenero Equity Investments II, L.P. ("Fenero II"), and Fenero Financial Switzerland L.P. ("Fenero Switzerland"), each of which were approved funds regulated in the British Virgin Islands. MSSI LTD also owned and operated Fenero Equity Investments (Cayman) I, L.P., ("Fenero Cayman") an investment fund organized in the Cayman Islands (together with the British Virgin Islands Fenero funds, the "Fenero Hedge Funds").

c. SCOTT operated offshore bank accounts in the Cayman Islands for each of the Fenero Hedge Funds (the "Fenero Hedge Fund Accounts"). The Fenero and Fenero Switzerland accounts were held at DMS Bank and Trust Limited in the Cayman Islands ("DMS Bank"), and the Fenero Cayman and Fenero II accounts were held at Deutsche Bank (Cayman) Ltd. in the Cayman Islands.

d. SCOTT also served as the Director of Fenero Equity Investments (Ireland), Limited, an entity formed in the Republic of Ireland on April 5, 2016. SCOTT and another co-conspirator not named herein ("CC-3") additionally served as directors of two apparently related companies also formed in Ireland: Fenero Tradenext Holding Limited and Fenero Pct Holdings Limited. Information publicly available online identifies CC-3 as the head of OneCoin Ltd.'s Legal and Compliance Department.

SCOTT's Use of Fenero Hedge Funds to Launder OneCoin Proceeds

19. Based on my own review and analysis of various bank account records and financial analysis performed by the New York County District Attorney's Office, information obtained from MLAT requests and other requests to foreign authorities, and my review of e-mail evidence obtained pursuant to subpoenas, MLATs, and judicially authorized search warrants, I have learned the following:

a. On September 30, 2015, SCOTT was introduced to CC-1 via e-mail.

b. On January 31, 2016, CC-1 e-mailed SCOTT, writing, "As time is ticking, what are the next steps and how can we move pls? If we want to meet – I am in London from 5.2-15.2 . . . Cindy has sent you the phone – contact me when you have it." I understand 5.2-15.2 to refer to February 5th through 15th, 2016. Travel records indicate that that SCOTT traveled from Miami to London on February 9, 2016, and returned on February 14, 2016. I believe that the phone sent to SCOTT by Cindy referenced in this e-mail was an encrypted telephone used to communicate with CC-1. I know from review of e-mails that CC-1 communicates with individuals using special encrypted telephones, in an effort to avoid interception by law enforcement.

c. On or about February 29, 2016, SCOTT registered MSSILTD in the British Virgin Islands. The following day, Fenero was registered as a Limited Partnership Company in the British Virgin Islands. On April 27, 2016, Fenero Cayman was registered in the Cayman Islands. And on May 5, 2016 and June 8, 2016, Fenero II and Fenero Switzerland were respectively registered in the British Virgin Islands.

d. After bank accounts were opened in the names of each of the Fenero Hedge Funds, between June 2016 and February 2017, the Fenero Hedge Fund Accounts collectively received wire transfers totaling approximately €364 million and \$10 million. These wire transfers originated from approximately 10 different bank accounts—held in the names of various entities, including International Marketing Services Pte ("IMS-1"), International Marketing Services GmbH ("IMS-2"), B and N Consult Ltd. ("B&N"), Fates Group ("Fates"), and Star Merchant Inc. Ltd ("Star Merchant")—at banks located in Singapore, Germany, Hong Kong, the United

Kingdom, and the United States.⁴ Through financial tracing, I have learned that eight of these 10 bank accounts—held by IMS-1, IMS-2, B&N, and Fates—received, either directly or indirectly, monies sent to OneCoin Ltd. by members purchasing trader packages.⁵ I have further identified documents and e-mail correspondence demonstrating that the Star Merchant bank account is associated with CC-1.

e. After receiving the above-described deposits sourced from OneCoin Ltd., between approximately August 2016 and February 2017, the Fenero Hedge Fund Accounts funded approximately €273 million in wire transfers benefitting three accounts held at Bank of Ireland in the Republic of Ireland (“Bank of Ireland”), each listed in the name of “Fenero Equity Investments Ireland.” Bank records for these accounts show that SCOTT controlled each of these accounts. In response to a MLAT request to the Republic of Ireland, I have obtained a partial set of records evidencing the disposition of some of these funds sent to Bank of Ireland.

SCOTT's Lies to Effectuate Transactions Sourced With OneCoin Funds

20. Based on my review of information obtained from MLAT requests and other requests to foreign authorities, my review of e-mail evidence obtained pursuant to subpoenas and MLATs, and my interview of relevant individuals, I have learned that SCOTT, in the course of operating the Fenero Hedge Funds, provided false information to banks and a fund administration firm concerning the source of funds and the purpose of various wire transfers.

⁴ These banks included: (i) United Overseas Bank and OCBC Bank in Singapore; (ii) Commerzbank and Deutsche Bank in Germany; (iii) DBS Bank in Hong Kong; (iv) Barclays and DSK Bank in the United Kingdom; and (v) Morgan Stanley and Sabadell United Bank in the United States.

⁵ For example, based on open source research that I have conducted on the internet, I have learned that at least three of the bank accounts from which funds were wired into the Fenero Hedge Fund Accounts were publicly advertised online as bank accounts into which OneCoin investors could wire money to purchase OneCoin packages.

SCOTT's Misrepresentations to a Fund Administration Firm

21. As described below, I believe that SCOTT misrepresented to a fund administration firm the source of funds and the purpose of wire transfers in order to conceal and disguise the nature, location, source, ownership, and control of OneCoin fraud proceeds. More specifically:

a. In or around April 2016, SCOTT contacted Apex Fund Services ("Apex"), a fund administration firm with offices in the Cayman Islands, Ireland, the United Kingdom, and the United States to inquire about services that Apex may be able to provide related to the administration of Fenero.

b. On or about April 29, 2016, SCOTT provided a Managing Director of Apex (the "Apex Director") with a document describing Fenero, its mission, investment strategy, and investor base. According to this document:

Fenero Equity Investments, L.P., is the first of a series of \$100,000,000 open ended investment funds located in the British Virgin Islands (the "Fund" or "Fenero"), focusing on investments in the financial services industry in Europe. . . . Due to its small investor base of wealthy families and middle market companies (the "Initial Investors") and its narrow investment strategy, the Fund requires very little staff. . . . Fenero will always fully control its capital and conduct its own stringent "KYC" on investors and final due diligence on any target companies internally.

Fenero has been created at the request of a select group of European based families and companies The Fund will basically be administered and managed in [the] form of a multi "Family Office" by MSS International Consultants (BVI), Ltd. . . . which is ultimately owned by Mark S. Scott . . . [who] currently is the Managing Partner of [the Law Firm], an Amlaw 50 firm, in Miami. The initial Investors of Fenero have been represented legally by Mr. Scott ranging from three (3) to twelve (12) years and have closed on in excess of \$2,100,000,000 in transactions under Mr. Scott's business and legal guidance.

c. I believe the above statement SCOTT provided to Apex to be false because:

(i) all of the money sent to Fenero and Fenero Switzerland was sourced from OneCoin Ltd.;

(ii) SCOTT did not know CC-1 for a period of three to twelve years, as he apparently was introduced to CC-1 via e-mail approximately eight months earlier; and (iii) I can find no evidence SCOTT ever closed in excess of \$2.1 billion in transactions with OneCoin Ltd., CC-1, or related persons.

d. On or about May 10, 2016, SCOTT, acting on behalf of Fenero and MSSI LTD, executed an agreement with Apex that described the services to be performed by Apex for Fenero, including carrying out relevant anti-money laundering (“AML”) requirements. Beginning on or about June 7, 2016, SCOTT contacted Apex about Fenero Switzerland, for which Apex also agreed to provide administrative services.

e. Apex facilitated the opening of bank accounts at DMS Bank for Fenero and Fenero Switzerland. While under the administration of Apex, the Fenero and Fenero Switzerland accounts received approximately €155 million in deposits sourced by wire transfers from OneCoin-related bank accounts in Singapore, Germany, and Bulgaria. An analyst in the New York County District Attorney’s Office reviewed records produced by the Bank of New York Mellon (“BNY Mellon”), which revealed that 11 wire transfers sent between May 30, 2016 and July 29, 2016 from OneCoin-related bank accounts in Singapore to the Fenero account at DMS Bank, totaling €55 million, were transacted through a correspondent account held at BNY Mellon. The New York County District Attorney’s Office analyst contacted BNY Mellon and learned that these wire transfers transacted through BNY Mellon’s correspondent account located in New York County. The OneCoin-related bank accounts in Singapore were held by a Singapore company operating under the name “International Marketing Services Pte” (“IMS-1”).⁶

⁶ An associated company, operating in Germany under the name “International Marketing Services GmbH” (“IMS-2,” and together with IMS-1, the “IMS Companies”), held additional OneCoin-related bank accounts in Germany.

f. SCOTT told Apex that all the funds sent to the Fenero and Fenero Switzerland hedge funds were actually deposits to accounts held at the hedge funds by another company named B and N Consult Ltd (“B&N”). SCOTT provided documents to Apex, which identified CC-3 as the beneficial owner of B&N. As noted above, CC-3 has served as the head of OneCoin Ltd.’s legal and compliance department. SCOTT never shared with Apex this fact, nor the fact that CC-3 was employed by or associated with OneCoin Ltd.

g. Concerning the source of monies funding the Fenero and Fenero Switzerland hedge funds, SCOTT told the Apex Director that CC-3 was a tech inventor and that B&N had licensed certain technology to the IMS Companies. SCOTT claimed that in return for licensing this technology from B&N, the IMS Companies wired funds to the Fenero and Fenero Switzerland hedge funds crediting B&N’s investment accounts. For example, on or about June 17, 2016, after the Fenero bank account received a €5 million wire transfer from IMS-1, SCOTT wrote to Apex, “we received another Euro 5,000,000 from IMS on behalf of B&N.”

h. In early July 2016, SCOTT e-mailed the Apex Director informing him that Fenero would issue a €30 million short-term loan to CryptoReal Investments Trust Ltd. (“CryptoReal”), which was allegedly purchasing an oil field from Barta Holdings Limited (“Barta”).⁷ SCOTT informed the Apex Director that a person (“Individual-1”), who SCOTT identified as a relative of two former United States Presidents, was the authorized representative of Barta, and stated “We will try hard not to ask for further KYC as to that part of the transaction.” SCOTT also e-mailed the Apex Director a letter from the purported beneficial owner of

⁷ Based on my review of CryptoReal’s website, I believe that CryptoReal is OneCoin Ltd.’s investment trust.

CryptoReal, and further advised that Individual-1 would sign the share purchase agreement concerning the sale of the oil field.

i. SCOTT requested that the €30 million loan be wired directly from Fenero to Barta's bank account held at bank located in Hong Kong. On or about July 13, 2016, SCOTT e-mailed the Apex Director a copy of the stock purchase agreement concerning the sale of the oil field. This agreement does not bear the signature of Individual-1, as SCOTT had previously represented to the Apex Director. Instead, it is signed by citizen of Madagascar on behalf of Barta, and by CC-1 on behalf of CryptoReal. On or about July 13, 2016, €30,000,000 was wired from the Fenero account to Barta's account in Hong Kong. Records produced by BNY Mellon show that this wire transacted through a correspondent account held at BNY Mellon, located in New York County.

j. I have obtained other records from a judicially authorized search warrant of an e-mail account, which indicate that Barta's Hong Kong bank account was used to fund a €10 million transaction benefiting CC-2. I am not aware of any evidence demonstrating that the loan from Fenero to Barta was ever repaid. For these reasons, I believe that the €30 million purported "loan" from Fenero to Barta was arranged by SCOTT to launder OneCoin Ltd. proceeds to CC-2.

k. On or about July 30, 2016, SCOTT apparently inadvertently forwarded an e-mail chain to Apex that included an e-mail originating from CC-3, identifying CC-3's e-mail address domain as onecoin.eu. According to the Apex Director, this e-mail address was noticed by Apex, representing the first time that Apex established a definite connection between the monies being received by SCOTT's hedge funds and OneCoin.

l. On or about August 2, 2016, in the course of conducting additional due diligence on the source of funds deposited into Fenero and Fenero Switzerland, the Apex Director

e-mailed SCOTT, stating that Apex required “a clear trail from the companies that pay IMS money[,] the services provided for that money and then the corresponding bank payments.”

m. On or about August 8, 2016, SCOTT e-mailed Apex copies of contracts between the two IMS Companies and OneCoin Ltd. The first contract, between IMS-1 and OneCoin Ltd. stated that IMS-1 would provide OneCoin Ltd. “financial handling” services and would charge a fee of 22% on “all incoming Client funds weekly.” The second contract, between IMS-2 and OneCoin Ltd. was similarly worded, but the fee was 20% rather than 22%. The terms of the two contracts appear designed to provide support for the volume of payments - purportedly for the purpose of licensing technology - made by the IMS Companies to Fenero Hedge Funds accounts held by B&N. However, I have reviewed the contracts and note that they are facially suspect, as they both suffer from multiple formatting abnormalities and obvious typographical errors.⁸

n. On or about August 10, 2016, Apex e-mailed SCOTT stating, “The first mention of OneCoin to Apex was only yesterday morning as the counterparty to a contract with IMS. This now opens more Enhanced Due Diligence questions around the flow of money from IMS to OneCoin particularly as there is a large amount of information on the internet raising concerns about OneCoin, its beneficial owners, and the number of investigations by different

⁸ In response to an MLAT request sent to Germany, I have obtained copies of the actual contracts between OneCoin Ltd. and the two IMS Companies. I understand that these contracts were seized by German law enforcement while executing a search warrant on IMS-2’s place of business. I believe these contracts to be the real contracts, because: (i) they were obtained directly from IMS-2; and (ii) they do not have the same formatting abnormalities and typographical errors present in the versions SCOTT provided to Apex. Both of these contracts allow for the IMS Companies to charge a 1% fee on handling incoming client funds, and not the fees of 20% and 22% set forth in the contracts provided by SCOTT to Apex.

regulators.” Later that day, SCOTT terminated MSSI LTD’s and Fenero’s engagement with Apex.

SCOTT’s Misrepresentations to DMS Bank

22. As described below, I believe that SCOTT also misrepresented to DMS Bank the source of funds and the purpose of wire transfers to and from the Fenero hedge funds in order to conceal and disguise the nature, location, source, ownership, and control of OneCoin fraud proceeds. More specifically:

a. On or about August 10, 2016, SCOTT contacted a banker at DMS Bank and stated that he had no further interest in working with Apex and needed a new firm that was more understanding of his business needs.

b. On or about September 21, 2016, SCOTT requested that DMS Bank wire €17 million apparently to a Fenero Equity Investments Ireland account held at Bank of Ireland. The next day, SCOTT explained to DMS Bank via e-mail that, “I am simply shifting Euro 15,000,000 [sic] to one of our subsidiaries in Ireland to somewhat reduce our Euro risk and expense. Fenero Securities was formed to hold a trading account in the UK. In order to obtain such account I need to have the funds ready.” Bank records show that this wire transfer was executed on or about September 22, 2016, in the amount of €17 million, crediting an account at Bank of Ireland (“Ireland Account-1”).

c. On or about October 13, 2016, an employee of MSSI LLC (the “MSSI Employee”) e-mailed DMS Bank, copying SCOTT, and requested that €40 million be wired to a Fenero Equity Investments Ireland account, adding that “these funds are ultimately being sent to our brokers in London.” Bank records show that this wire transfer was executed on or about October 14, 2016, in the amount of €40 million, crediting Ireland Account-1.

d. Similarly, on or about January 27, 2017, the MSSI Employee e-mailed DMS Bank, copying SCOTT, and requested that €20 million and €10 million, respectively, be wired to a Fenero Equity Investments Ireland account. The purpose of this transfer was described as “Internal Transfer to Brokerage Account.” Bank records show both of these wires were executed, crediting a second account at Bank of Ireland (“Ireland Account-2”).

e. I have reviewed records related to Ireland Account-1 and Ireland Account-2, obtained in response to a MLAT request sent to the Republic of Ireland. These records evidence that, at most, €10 million of the aforementioned €17 million, €40 million, €20 million and €10 million wire transfers to Ireland Account-1 and Ireland Account-2 was sent to a brokerage account, and that this €10 million was apparently only temporary held at the brokerage firm. More specifically, on January 23 and 24, 2017 Ireland Account-1 sent approximately €10 million to a financial services firm located in London offering investment brokerage services (“Firm-1”), but this money was apparently returned via an approximately €10 million wire from Firm-1 sent to Ireland Account-1 on April 7, 2017.

f. Working with the U.S. Department of Justice Office of International Affairs (“OIA”), I requested that Cayman Island authorities interview DMS Bank employees, to include a managing director (the “DMS Bank Director”) who worked with SCOTT and managed the Fenero and Fenero Switzerland accounts. I provided certain questions and requested they be posed to the DMS Bank Director.

g. OIA received from the Cayman Islands the DMS Bank Director’s responses to my questions, dated May 16, 2018. The information provided included the following:

What were you told was the source of funds transferred into the Fenero Cayman Accounts?

DMS was told the source of funds transferred into the Fenero Cayman accounts was Family Offices from Europe, primarily Switzerland. DMS understood from speaking to Mark Scott and [the MSSI Employee] that Mr Scott was a private equity lawyer in Germany for many years and had built a network of investor contacts there.

Apex, a FCA regulated fund administrator, was fully appointed at the time of investor subscriptions and, as is standard banking practice, this enabled DMS to take comfort in its internal KYC checks on individual investors.

What were you told was the disposition of the funds transferred to the Fenero Irish Accounts?

DMS were advised that the disposition of the funds transferred to the Fenero Irish accounts was to fund a broker account.

h. Based on the evidence I have reviewed, I believe that SCOTT's representations to DMS Bank about the source of the funds deposited in the Fenero and Fenero Switzerland DMS Bank accounts were false. The funds did not originate from family offices in Switzerland, nor did they originate from private equity deals that SCOTT had negotiated in Europe. Rather, the funds represented proceeds of the OneCoin fraud scheme.

23. Based on financial tracing conducted by myself and an analyst with the New York County District Attorney's Office, I have learned that between approximately February and April 2016, SCOTT received into a United States bank account held in his name, three wires totaling approximately \$1 million from the IMS Companies. I have further learned that at least \$15.5 million of the original €364 million and \$10 million sent to the Fenero Hedge Fund Accounts was remitted either directly, or indirectly through intermediary accounts, to bank accounts in the United States held in the name of SCOTT or MSSI LLC. As described further below, many of these transfers involved accounts held in the name of Nicole J. Huesmann. SCOTT used the monies he

received from the Fenero Hedge Fund Accounts for personal expenses and to fund large luxury purchases. For example:

a. On or about September 6, 2016, approximately \$279,000 was remitted from a Fenero bank account at DMS Bank to a bank account in the United States held by SCOTT. On or about September 6, 2016, SCOTT made a payment of \$26,500 from the account to a designer watch retailer. Between approximately September 7, 2016 and September 26, 2016, SCOTT made payments totaling approximately \$65,000 from the account to a credit card company.

b. On or about November 2, 2016, \$1 million was remitted from a Fenero bank account at Bank of Ireland to an intermediary bank account in the United States. On or about November 7, 2016, \$250,000 was wired from the intermediary account to a United States bank account held in the name of MSSI LLC, over which SCOTT maintained sole signatory authority (the "MSSI LLC Account"). On or about November 8, 2016, SCOTT made a payment of approximately \$250,000 from the MSSI LLC Account to a luxury car dealership in Florida (the "Florida Dealership") for a 2011 Ferrari 599 9TB.

c. On or about February 1, 2017, \$325,000 was remitted from a Fenero bank account to the MSSI LLC Account. On or about February 10, 2017, SCOTT made a payment of approximately \$120,000 from the MSSI LLC Account to the Florida Dealership for a 2017 Porsche 911 Turbo S.

d. On or about March 9, 2017, over \$3.1 million was remitted from a Fenero bank account at Bank of Ireland to a bank account in the United States held by SCOTT.

24. Based on financial tracing conducted by me and an analyst at the New York County District Attorney's Office, I have also identified property that was purchased by or for SCOTT with funds originally sourced from OneCoin-derived or OneCoin-related proceeds, to wit:

- a. A diamond bracelet from Buchwald Jewelers;
- b. An emerald-cut engagement ring from Buchwald Jewelers;
- c. An Hermes Black Etoupe 40 bag;
- d. An Hermes Orange Poppy Birkin 35 bag;
- e. An Hermes cut clutch bag;
- f. A Big Pilot Le Petit Prince Rose Gold watch;
- g. A Panerai PAM 598 watch with blue strap;
- h. A Panerai PAM 530 watch;
- i. A Panerai PAM 421 watch;
- j. A Panerai PAM 582 barometer wall clock;
- k. A Panerai PAM 583 thermometer;
- l. A Panerai PAM 584 hygrometer watch; and
- m. A Panerai PAM 585 wall clock.

25. Moreover, review of financial records conducted by an analyst at the New York County District Attorney's Office, related to bank accounts controlled by SCOTT and Nicole J. Huesmann has demonstrated that Huesmann has assisted SCOTT in repatriating OneCoin fraud proceeds for SCOTT's personal use.⁹ For example, I have learned that:

- a. Between October 2016 and June 2017, Huesmann received 11 wire transfers totaling \$5,600,000 from Fenero-related accounts.
- b. Between November 2014 and March 2017, Huesmann received nine wire transfers totaling \$2,416,955 from accounts in the name of SCOTT and/or MSSl.

⁹ Based on my review of publicly-available attorney certification records, I have learned that Nicole J. Huesmann is an attorney admitted to practice in Florida, with an office address in Coral Gables, Florida.

c. On November 20, 2014, SCOTT sent a \$40,000 payment to Huesmann related to a “condo purchase.”

d. On January 14, 2015, SCOTT sent a \$150,000 payment to Huesmann related to “closing costs.”

e. On October 3, 2016, Fenero Tradenext sent \$250,000 to an account controlled by Huesmann in connection with “escrow property partial payout of BN loan facility.”

f. On November 2, 2016, Fenero Tradenext transferred \$250,000 to an account controlled by Huesmann in connection with “Acquisition funds MSSSI.”

g. On November 7, 2016, Huesmann transferred \$250,000 from an account she controlled to MSSSI LLC.

h. On February 1, 2017, Fenero Tradenext transferred to Huesmann \$350,000.00; the wire instructions for this transfer stated “(Equity and pot loan) for Mumbelli deal. Returnable at MSSSI.”¹⁰

i. On February 15, 2017, an account controlled by Huesmann transferred \$130,000 to Galati Yacht Sales LLC as an “escrow deposit for 2016 Sunseeker Predator 5757 for MSSSI Consultants.”¹¹

j. On February 17, 2017, Huesmann sent \$3,000 to Daniel Fernandez for “57 Sunseeker, MSSSI, legal fee.”

k. On March 9, 2017, a Huesmann-controlled account transferred \$144,712.11 to Braman Motorcars.¹²

¹⁰ Florida Department of Corporations records reflect that Mumbelli Group LLC was registered as a corporation, with Huesmann serving as its agent.

¹¹ According to open source information, the “Sunseeker Predator 57” is a yacht.

¹² According to publicly-available information, Braman Motorcars is a luxury car dealership located in West Palm Beach, Florida.

l. On March 21, 2017, a Huesmann-controlled account transferred \$1,127,000 to Nautikos Florida LLC in connection with a Sunseeker.

m. On June 19, 2017, Fenero Tradenext sent Huesmann \$250,000.00 in connection with "Additional cap contribution for Railroad/Barnstable Property development."

26. I have additionally learned that SCOTT transferred OneCoin fraud proceeds from the Fenero Hedge Fund Accounts to Huesmann in connection with his purchase of a multi-million-dollar beach-front property in Cape Cod, Massachusetts. On October 12, 2016, Fenero Tradenext transferred \$500,000 to Huesmann; the wire details of that transaction referenced "Escrow 133SL Additional retainer."¹³ On October 17, 2016, Fenero Tradenext transferred another \$500,000 to Huesmann; the wire details of that transaction referenced "Escrow property 2nd payment. Total 1,000,000." Massachusetts real estate public records reflect that on October 24, 2016, a property located at 133 Sunset Lane, Barnstable, Massachusetts, was deeded to 133 Sunset LN Acquisition Limited c/o Huesmann, for the amount of \$2,850,000. I have reviewed Massachusetts public corporation records and learned that 133 Sunset LN Acquisition Limited is a BVI company registered in Massachusetts as a foreign business on December 11, 2017. According to the public corporate registration records for 133 Sunset LN Acquisition Limited, the entity was organized in the BVI on October 3, 2016, and SCOTT serves at its director, with the Subject Premises as his address.

27. Based on the above-referenced financial records and publicly-available information, I believe that Huesmann has (i) participated in transfers of OneCoin Scheme

¹³ Based on the information set forth later in this paragraph, I believe that "Escrow 133SL Additional retainer" refers to a payment related to the purchase of 133 Sunset Lane, Barnstable, Massachusetts.

proceeds; (ii) assisted SCOTT in real estate transactions funded by proceeds of the OneCoin Scheme; and (iii) facilitated SCOTT's purchase of boats.

B. Probable Cause Justifying Search of the Subject Premises

28. Based on the evidence gathered in the investigation, there is probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses, as set forth in Attachment A, are located at the Subject Premises and in containers present therein, including on computers, cell phones, and other electronic devices.

29. As noted above, the Subject Premises is owned by SCOTT. Based upon my review of property records relating to the Subject Premises, I have learned that SCOTT has owned the Subject Premises since on or about January 12, 2015. Additionally, based on my review of property records related to the Subject Premises, I have learned that SCOTT obtained a mortgage on the property on or about August 19, 2016, and that mortgage is currently outstanding. The property records related to the Subject Premises reflect that Huesmann represented SCOTT in the purchase of and obtaining a mortgage for the Subject Premises.

30. Based upon my review of Florida Division of Corporations public records, I have learned that the Subject Premises is listed as both the principal address and mailing address for MSSSI LLC, the Florida company that controls the Fenero Hedge Funds. Florida Division of Corporations records further reflect that SCOTT is the sole managing member and registered agent of MSSSI LLC, and that SCOTT filed an annual report for MSSSI LLC as recently as February 2018 listing the Subject Premises as both the principal address and mailing address for MSSSI LLC.

31. Based upon my review of a 2016 Request for Taxpayer Identification Number and Certification Form W-9 filed with the IRS on behalf of MSSSI LLC, I have learned that the Subject Premises is listed on that Form W-9 as the address for MSSSI LLC.

32. I have reviewed several e-mails between SCOTT and Apex in connection with the mailing of certain materials related to the Fenero Hedge Funds to SCOTT. In these emails, dated August 2016, SCOTT requested that Apex mail the materials to him at the Subject Premises. These emails also contain two shipping receipts reflecting that two boxes of materials related to the Fenero Hedge Funds were in fact mailed to the Subject Premises, the first in August 2016, and the second in October 2016.¹⁴

33. Based on my review of emails containing invoices related to professional services provided to MSSI LLC and the Fenero Hedge Funds, I have learned that those invoices, dated approximately June 2016 to August 2016, were addressed to MSSI LLC at the Subject Premises. Notably, the invoices included professional fees related to the establishment of and advice provided to the Fenero Hedge Funds, as well as professional fees related to the MSSI LLC.

34. Based on the facts described in this affidavit and in the Superseding Indictment, it appears that SCOTT received documents and correspondence relating to the OneCoin Scheme and laundering of its proceeds at the Subject Premises. Based upon my training and experience investigating white-collar offenses, I know that individuals routinely maintain business records, including corporate documents, financial records, and communications, at their places of business and/or residences, and retain those documents for long periods of time. Indeed, businesses are often required to retain certain records and documents for a prolonged period of time for various regulatory and administrative purposes, including tax audits. I submit that there is probable cause to believe that SCOTT engaged in the Subject Offenses and that evidence of this

¹⁴ While tracking records evidenced both these deliveries, SCOTT nevertheless claimed not to have received one of these boxes.

criminal activity, including records relating to the OneCoin Scheme and laundering of its proceeds, is likely to be found at the Subject Premises.

C. Probable Cause Justifying Search of ESI

35. Based on the facts described above, and detailed in the Superseding Indictment, it appears that SCOTT used email to send and receive documents and communications related to the OneCoin Scheme and his laundering of the proceeds from that scheme. Based upon my training and experience in similar investigations, I submit that there is probable cause to believe that there will be computers and other electronic devices belonging to SCOTT at the Subject Premises and that those devices will contain electronic files and data relating to the Subject Offenses.

36. Based on my training and experience, I also know that, where computers, cellphones, and electronic devices are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because, among other things:

- a. Electronic files can be stored on a hard drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.
- b. Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is “deleted” on a computer or electronic device, the data contained in the file does not actually disappear, but instead remains on the hard drive, in “slack space,” until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or “cache,” which is only overwritten as the “cache” fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was

created or viewed than on a particular user's operating system, storage capacity, and computer habits.

c. In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or external hard drives.

37. Based on the foregoing, I respectfully submit there is probable cause to believe that SCOTT engaged in the Subject Offenses and that evidence of this criminal activity is likely to be found at the Subject Premises and on computers, cellphones, and other electronic devices and media contained in the Subject Premises.

III. Procedures for Searching ESI

A. Execution of Warrant for ESI

38. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review." Consistent with Rule 41, this Application requests authorization to seize any computer devices and storage media, and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

a. First, because of the volume of data on computers, cellphones (including iPhones), other electronic devices, and storage media, it is typically impractical for law enforcement personnel to review the data in its entirety at the search location.

b. Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized

software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.

c. Third, there are so many different types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.

d. Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

B. Review of ESI

39. Following seizure of any computers, cellphones, electronic devices, or storage media, and/or the creation of forensic image copies, law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant, as set forth in Attachment A.

40. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- Surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

- Conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “Scanning” storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and
- Performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation¹⁵; and
- Reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

41. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

C. Return of ESI

42. If the Government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

¹⁵ Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

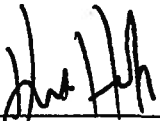
IV. Additional Screening Procedures

43. Additionally, because SCOTT is an attorney, the review of evidence seized from the Subject Premises and any electronic devices will be conducted pursuant to established screening procedures to ensure that the law enforcement personnel involved in the investigation, including attorneys for the Government, collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege. As appropriate, the procedures will include use of a designated "filter team," separate and apart from the investigative team, in order to review potentially privileged communications and determine which communications to release to the investigation and prosecution team.

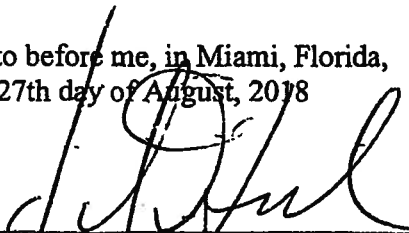

V. Conclusion and Ancillary Provisions

44. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this Affidavit and to the Warrant.

45. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.


 KURT HARER
 Special Agent
 United States Attorney's Office, Southern District of
 New York

Sworn to before me, in Miami, Florida,
 on this 27th day of August, 2018


 JOHN O'SULLIVAN
 UNITED STATES MAGISTRATE JUDGE
 Steven M. Larimore, Clerk,
 U.S. District Court
 Southern District of Florida
 By 
 Deputy Clerk
 Date 8/27/18

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - - X
:
UNITED STATES OF AMERICA
:
- v. - : SEALED INDICTMENT
:
MARK S. SCOTT, : S6 17 Cr. 630
:
Defendant. :
:
- - - - - X

COUNT ONE
(Conspiracy to Commit Money Laundering)

The Grand Jury charges:

1. From at least in or about 2016 through in or about 2018, in the Southern District of New York and elsewhere, MARK S. SCOTT, the defendant, and others known and unknown, knowingly did combine, conspire, confederate, and agree together and with each other to commit money laundering, in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 1956(a)(2)(B)(i).

2. It was a part and an object of the conspiracy that MARK S. SCOTT, the defendant, and others known and unknown, knowing that the property involved in certain financial transactions represented the proceeds of some form of unlawful activity, would and did conduct and attempt to conduct such financial transactions which in fact involved the proceeds of specified unlawful activity, to wit, approximately \$400 million

in proceeds of a pyramid scheme involving a purported cryptocurrency known as "OneCoin," knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a) (1) (B) (i).

3. It was further a part and an object of the conspiracy that MARK S. SCOTT, the defendant, and others known and unknown, would and did transport, transmit, and transfer, and attempt to transport, transmit, and transfer a monetary instrument and funds from a place in the United States to and through a place outside the United States, and to a place in the United States from and through a place outside the United States, knowing that the monetary instrument and funds involved in the transportation, transmission, and transfer represented the proceeds of some form of unlawful activity and knowing that such transportation, transmission, and transfer was designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, to wit, approximately \$400 million in proceeds of a pyramid scheme involving a purported cryptocurrency known as "OneCoin," in violation of Title 18, United States Code, Section 1956(a) (2) (B) (i).

(Title 18, United States Code, Section 1956(h).)

FORFEITURE ALLEGATION

4. As a result of committing the offense alleged in Count One of this Indictment, MARK S. SCOTT, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), any and all property, real and personal, involved in said offense, or any property traceable to such property, including but not limited to a sum of money in United States currency representing the amount of property involved in said offense.

Substitute Asset Provision

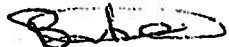
5. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property

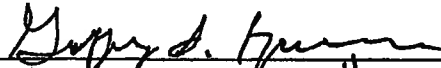
of the defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Section 982;
Title 21, United States Code, Sections 853; and
Title 28, United States Code, Section 2461.)



FOREPERSON

August 31, 2018



GEOFFREY S. BERMAN *JB*
United States Attorney
Southern District of New York

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

MARK S. SCOTT,

Defendant.

SEALED INDICTMENT

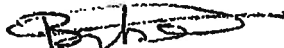
S6 17 Cr. 630

(18 U.S.C. § 1956(h).)

GEOFFREY S. BERMAN

United States Attorney.

A TRUE BILL



Foreperson.

ATTACHMENT A

I. Premises to be Searched—Subject Premises

A. The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:

The Subject Premises is particularly described as a condominium located at 600 Coral Way, Suite/Floor 12, Segovia Tower, Coral Gables, Florida, 33134, and Any Closed Containers/Items Contained Therein. The Subject Premises occupies the entire floor.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Attachment A. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

Additionally, review of the items described in this attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege. Because the owner and resident of the Subject Premises is an attorney, the procedures shall include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privilege issues.

II. Items to Be Seized—Evidence, Fruits, and Instrumentalities of the Subject Offenses

A. Items to Be Seized

The items to be seized from the Subject Premises include the following evidence, fruits, and instrumentalities of Title 18, United States Code, §§ 1956(a)(1)(B)(i), 1956(a)(2)(B)(i), 1956(h), and 1344 (money laundering, conspiracy to commit money laundering, and bank fraud), related to the OneCoin business and derived funds (the “Subject Offenses”), described as follows:

a. Evidence of the Subject Offenses, including but not limited to: (i) documents and communications relating to the administration of the OneCoin business, and the transfer and/or laundering of criminal proceeds; (ii) drafts or different versions of the same; and (iii) documents and communications making reference to or containing discussion of the commission of those offenses, including those referencing the following individuals and/or entities:

- Apex Fund Services Ltd.
- B and N Consult Ltd
- Bank of Ireland
- Barclays Bank
- Barta Holdings Limited
- City National Bank
- Commerzbank
- Cryptoreal
- Deutsche Bank (Germany)
- Deutsche Bank (Cayman) Ltd.
- DBS Bank
- DMS Bank and Trust Ltd.
- DSK Bank
- Fates Group
- Fenero Equity Investments L.P.
- Fenero Equity Investments II, L.P.
- Fenero Equity Investments (Ireland), Limited
- Fenero Equity Investments (Cayman) I, L.P.
- Fenero Financial Switzerland L.P.
- Fenero Pct Holdings Limited
- Fenero Tradenext Holding Limited
- Morgan Stanley
- Mumbelli Group LLC
- Nicole Huesmann
- International Marketing Services GmBH
- International Marketing Services Pte
- MSS International Consultants (BVI), Ltd.

- MSS International Consultants LLC (together with MSS International Consultants (BVI), Ltd., "MSSI")
- OCBC Bank
- OneCoin Ltd.
- Sabadell United Bank
- Star Merchant Inc. Ltd
- United Overseas Bank

and other individuals and entities involved in the administration of OneCoin and the transfer/laundering of OneCoin fraud proceeds, covering the period of July 2015 to the present;

b. Financial agreements – including loan agreements and other documents representing purported financial contracts or obligations – memoranda and other communications, spreadsheets, ledgers, summaries, and logs relating to, or containing information regarding, transactions involving the individuals and entities described above and transactions involving any OneCoin-derived or OneCoin-related funds, covering the period of July 2015 to the present;

c. Financial records, including agreements, bank account records, corporate organization documents, ledgers, and memoranda relating to any MSSI-related and/or Fenero-related entity, covering the period of July 2015 to the present;

d. Communications constituting crimes, including emails, chats, memoranda, and/or other communications relating to the transfer and/or laundering of criminal proceeds and the transmission of funds without a license, covering the period of July 2015 to the present;

e. Communications with co-conspirators, including emails that demonstrate the relationships among co-conspirators, covering the period of July 2015 to the present;

f. Evidence concerning the identity or location of any co-conspirators;

g. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

h. Evidence sufficient to identify Mark S. Scott's use of electronic accounts, including but not limited to e-mail accounts, social media accounts, and Internet cloud storage accounts; and

i. Any items purchased by or for Mark S. Scott with funds originally sourced from OneCoin-derived or OneCoin-related proceeds, to wit:

- (1) A diamond bracelet from Buchwald Jewelers;
- (2) An emerald-cut engagement ring from Buchwald Jewelers;
- (3) An Hermes Black Etoupe 40 bag;
- (4) An Hermes Orange Poppy Birkin 35 bag;
- (5) An Hermes cut clutch bag;
- (6) A Big Pilot Le Petit Prince Rose Gold watch;
- (7) A Panerai PAM 598 watch with blue strap;
- (8) A Panerai PAM 530 watch;
- (9) A Panerai PAM 421 watch;
- (10) A Panerai PAM 582 barometer wall clock;
- (11) A Panerai PAM 583 thermometer;
- (12) A Panerai PAM 584 hygrometer watch; and
- (13) A Panerai PAM 585 wall clock.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises include any computers, cellphones, electronic devices, and storage media that may contain any electronically stored information ("ESI") falling within the categories set forth above, including, but not limited to, desktop and laptop computers, cellphones (including iPhones and other smartphones), tablets (such as iPads), external hard drives, and thumb drives. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.
4. Any items or records needed to access the data stored on any seized or copied computers, cellphones, electronic devices, or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
5. Any items or records that may facilitate a forensic examination of the computers, cellphones, electronic devices, or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

6. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computers, cellphones, electronic devices, or storage media.

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Southern District of FloridaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)THE PREMISES LOCATED AT 600 CORAL WAY,
SUITE/FLOOR 12, SEGOVIA TOWER, CORAL
GABLES, FLORIDA 33134

Case No. 18-3283 JJO

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Southern District of Florida
(Identify the person or describe the property to be searched and give its location):the premises located at 600 Coral Way, Suite/Floor 12, Segovia Tower, Coral Gables, Florida 33134, and any closed
containers/items contained therein, as further described in Attachment A.I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (Identify the person or describe the property to be seized):

See Attachment A.

YOU ARE COMMANDED to execute this warrant on or before 9/10/18 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to the duty Magistrate Judge
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued: 8/27/18 @ 2:30 PM

City and state: Miami, Florida

Certified to be a true and correct copy of the document on file with the court.	
John O'Sullivan, U.S. District Court, Southern District of Florida	
By	Deputy Clerk
Date	

MC 115A0 00000440

ATTACHMENT A

I. Premises to be Searched—Subject Premises

A. The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:

The Subject Premises is particularly described as a condominium located at 600 Coral Way, Suite/Floor 12, Segovia Tower, Coral Gables, Florida, 33134, and Any Closed Containers/Items Contained Therein. The Subject Premises occupies the entire floor.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Attachment A. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

Additionally, review of the items described in this attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege. Because the owner and resident of the Subject Premises is an attorney, the procedures shall include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privilege issues.

II. Items to Be Seized—Evidence, Fruits, and Instrumentalities of the Subject Offenses

A. Items to Be Seized

The items to be seized from the Subject Premises include the following evidence, fruits, and instrumentalities of Title 18, United States Code, §§ 1956(a)(1)(B)(i), 1956(a)(2)(B)(i), 1956(h), and 1344 (money laundering, conspiracy to commit money laundering, and bank fraud), related to the OneCoin business and derived funds (the “Subject Offenses”), described as follows:

a. Evidence of the Subject Offenses, including but not limited to: (i) documents and communications relating to the administration of the OneCoin business, and the transfer and/or laundering of criminal proceeds; (ii) drafts or different versions of the same; and (iii) documents and communications making reference to or containing discussion of the commission of those offenses, including those referencing the following individuals and/or entities:

- Apex Fund Services Ltd.
- B and N Consult Ltd
- Bank of Ireland
- Barclays Bank
- Barta Holdings Limited
- City National Bank
- Commerzbank
- Cryptoreal
- Deutsche Bank (Germany)
- Deutsche Bank (Cayman) Ltd.
- DBS Bank
- DMS Bank and Trust Ltd.
- DSK Bank
- Fates Group
- Fenero Equity Investments L.P.
- Fenero Equity Investments II, L.P.
- Fenero Equity Investments (Ireland), Limited
- Fenero Equity Investments (Cayman) I, L.P.
- Fenero Financial Switzerland L.P.
- Fenero Pct Holdings Limited
- Fenero Tradenext Holding Limited
- Morgan Stanley
- Mumbelli Group LLC
- Nicole Huesmann
- International Marketing Services GmBH
- International Marketing Services Pte
- MSS International Consultants (BVI), Ltd.

- MSS International Consultants LLC (together with MSS International Consultants (BVI), Ltd., "MSSI")
- OCBC Bank
- OneCoin Ltd.
- Sabadell United Bank
- Star Merchant Inc. Ltd
- United Overseas Bank

and other individuals and entities involved in the administration of OneCoin and the transfer/laundrying of OneCoin fraud proceeds, covering the period of July 2015 to the present;

b. Financial agreements – including loan agreements and other documents representing purported financial contracts or obligations – memoranda and other communications, spreadsheets, ledgers, summaries, and logs relating to, or containing information regarding, transactions involving the individuals and entities described above and transactions involving any OneCoin-derived or OneCoin-related funds, covering the period of July 2015 to the present;

c. Financial records, including agreements, bank account records, corporate organization documents, ledgers, and memoranda relating to any MSSI-related and/or Fenero-related entity, covering the period of July 2015 to the present;

d. Communications constituting crimes, including emails, chats, memoranda, and/or other communications relating to the transfer and/or laundrying of criminal proceeds and the transmission of funds without a license, covering the period of July 2015 to the present;

e. Communications with co-conspirators, including emails that demonstrate the relationships among co-conspirators, covering the period of July 2015 to the present;

f. Evidence concerning the identity or location of any co-conspirators;

g. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

h. Evidence sufficient to identify Mark S. Scott's use of electronic accounts, including but not limited to e-mail accounts, social media accounts, and Internet cloud storage accounts; and

i. Any items purchased by or for Mark S. Scott with funds originally sourced from OneCoin-derived or OneCoin-related proceeds, to wit:

- (1) A diamond bracelet from Buchwald Jewelers;
- (2) An emerald-cut engagement ring from Buchwald Jewelers;
- (3) An Hermes Black Etoupe 40 bag;
- (4) An Hermes Orange Poppy Birkin 35 bag;
- (5) An Hermes cut clutch bag;
- (6) A Big Pilot Le Petit Prince Rose Gold watch;
- (7) A Panerai PAM 598 watch with blue strap;
- (8) A Panerai PAM 530 watch;
- (9) A Panerai PAM 421 watch;
- (10) A Panerai PAM 582 barometer wall clock;
- (11) A Panerai PAM 583 thermometer;
- (12) A Panerai PAM 584 hygrometer watch; and
- (13) A Panerai PAM 585 wall clock.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises include any computers, cellphones, electronic devices, and storage media that may contain any electronically stored information ("ESI") falling within the categories set forth above, including, but not limited to, desktop and laptop computers, cellphones (including iPhones and other smartphones), tablets (such as iPads), external hard drives, and thumb drives. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized from the Subject Premises also include:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.
4. Any items or records needed to access the data stored on any seized or copied computers, cellphones, electronic devices, or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
5. Any items or records that may facilitate a forensic examination of the computers, cellphones, electronic devices, or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

6. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computers, cellphones, electronic devices, or storage media.