

FILED

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
FORT MYERS DIVISION

2017 AUG 21 PM 3:42

CLERK, US DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
FORT MYERS FLORIDA

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case No. 2:17-cv-474-FHM - 38MRM

ASSET IDENTIFIED IN
PARAGRAPH ONE OF
VERIFIED COMPLAINT,

Defendant.

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

In accordance with Rule G(2) of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions, Plaintiff United States of America brings this complaint and alleges upon information and belief as follows:

NATURE OF THE ACTION

1. This is a civil action *in rem*, to forfeit to the United States the following

Defendant Property:

\$450,000 of the \$524,390.32 obtained from the sale of the real property located on Southwest 25th Place in Cape Coral, Florida ("Cape Coral property").

VENUE AND JURISDICTION

2. Venue properly lies in the Middle District of Florida pursuant to 28 U.S.C. § 1395, because the property lies within the district. 28 U.S.C. § 1395(b).

3. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1345, which provides the Court with jurisdiction over all civil actions commenced by the United States, and pursuant to 28 U.S.C. § 1355, which provides the Court with jurisdiction over actions to recover or enforce forfeitures.

4. This Court has *in rem* jurisdiction over the Defendant Property because pertinent acts giving rise to the forfeiture occurred in the Middle District of Florida. 28 U.S.C. § 1355(b)(1)(A). In addition, the Defendant Property was found in the Middle District of Florida. 28 U.S.C. § 1395(b).

5. Because the Defendant Property is in the government's possession, custody, and control, the United States requests that the Clerk of Court issue an arrest warrant *in rem*, upon the filing of the complaint, pursuant to Supplemental Rule G(3)(b)(1). The United States will then execute the warrant on the property pursuant to 28 U.S.C. § 1355(d) and Supplemental Rule G(3)(c).

STATUTORY BASIS FOR FORFEITURE

6. The Defendant Property purchased is traceable to proceeds of wire fraud offenses, in violation of 18 U.S.C. §§ 1343 & 1349. Accordingly, the United States is entitled to forfeit the Defendant Property pursuant to 18 U.S.C. § 981(a)(1)(C). Section 981(a)(1)(C) provides for the civil forfeiture of any property, real or personal, which constitutes or is derived from proceeds from any offense constituting "specified unlawful activity" as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such offenses. 18 U.S.C. § 981(a)(1)(C). A "specified unlawful activity," as defined in 18 U.S.C. § 1956(c)(7)(A) includes any act or activity constituting an offense listed in 18 U.S.C. § 1961(1). Section 1961(1) contains wire fraud violations.

FACTS

7. Specific facts supporting the forfeiture of the Defendant Property have been provided by Homeland Security Investigations (HSI) Special Agent (SA) Michael P. Adams, who has been a Special Agent with HSI since July 2011. Prior to Joining HSI, SA Adams was employed as a SA with the United States Secret Service (USSS)

from June 2000 through July 2011. SA Adams investigates violations of federal law relating to financial crimes and the cross-border flow of money and goods. His investigations have included numerous cases involving patterns of conduct similar to that described in this complaint. SA Adams has received training by HSI and USSS on detecting and investigating the use and manufacture of counterfeit credit cards and false identification documents, money laundering, unlicensed money remitting, racketeering, and wire fraud. He personally participated in this investigation and is thoroughly familiar with the information contained in this complaint.

8. The facts contained in this complaint are based on SA Adams' personal knowledge, knowledge obtained from law enforcement officers, review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein (including participants), and information gained through his training and experience and the training and experience of others. The following summary of the facts is intended to establish reasonable cause that the United States can meet its burden of proof at trial. It does not attempt to provide every detail of this investigation.

I. **SUMMARY OF ALLEGATIONS**

9. This case involves an investigation of fraudulent online investment vehicles known as "High-Yield Investment Programs," or "HYIPs." HYIPs are a common form of internet-based fraud scheme. A typical HYIP advertises itself as a legitimate investment opportunity offering extraordinarily lucrative returns. Instead of investing depositor funds as promised, however, the HYIP's operators divert the money for their personal enrichment.

10. Since at least 2003, Brian and Edward Krassenstein, two brothers who reside in the Middle District of Florida, have owned and operated websites devoted to the promotion of fraudulent HYIPs. In particular, the Krassenstein-run sites "talkgold.com" and "moneymakergroup.com" are discussion forums in which HYIP operators advertise and promote their fraud schemes to potential victims. Over the 13 years of these sites' existence, they have generated tens of thousands of complaints by victims of fraudulent HYIPs. Based on this fact, along with other facts set forth below, there is reasonable cause to believe that the Krassensteins would have known that the HYIPs being promoted on their sites were fraudulent. There is also reasonable cause to believe that, by partnering with the operators of these fraudulent HYIPs for the purpose of promoting the fraudulent HYIPs, Brian and Edward Krassenstein have conspired to commit wire fraud.

11. Brian and Edward Krassenstein have derived substantial revenues from their HYIP-related websites. This revenue primarily takes the form of "advertising fees" paid by HYIP operators in exchange for promotion on the sites. These payments from HYIP operators to the Krassensteins are the proceeds of wire fraud. Given the duration and depth of the Krassensteins' involvement in the world of HYIPs, there is reasonable cause to believe that the Krassensteins would have known that these funds were criminally derived.

II. BACKGROUND OF INVESTIGATION

A. Liberty Reserve and Perfect Money

12. Liberty Reserve was an underworld cyber-banking system that laundered hundreds of millions of dollars in illicit proceeds for criminals around the world. Liberty Reserve was designed to protect its users from the scrutiny of law enforcement: its founders promoted the currency as being fully anonymous and untraceable, and moved

the organization from the United States to Costa Rica in an attempt to escape the jurisdiction of U.S. law enforcement. Despite these efforts, Liberty Reserve's founders were indicted and have pleaded guilty in the Southern District of New York to offenses including conspiracy to commit money laundering (case no. 1:13cr368).

13. After the takedown of Liberty Reserve, its users migrated to other digital currencies including "Perfect Money." Perfect Money was Liberty Reserve's chief competitor at the time of the Liberty Reserve takedown. Perfect Money shared many of the features which made Liberty Reserve attractive to cybercriminals, including: 1) a high degree of anonymity and minimal account verification; and 2) the absence of a mechanism for law enforcement to obtain transaction records.

14. Both Liberty Reserve and Perfect Money structured their business models so as to minimize direct contact with their end-users. An individual or entity could not directly purchase digital currencies from either Liberty Reserve or Perfect Money. Instead, the individual/entity was required to transact through an "exchanger" in order to exchange real-world currency (e.g., U.S. Dollars) for digital currency (e.g., Liberty Reserve). Often, multiple layers of exchangers would separate the Liberty Reserve and Perfect Money organizations from the ultimate users of the digital currencies. This multi-tiered system was designed to insulate the leaders of Liberty Reserve and Perfect Money from law enforcement scrutiny and provide them a measure of plausible deniability if confronted with the illegal nature of their users' transactions.

15. Prior to its demise, a substantial portion of Liberty Reserve transactions related to online criminal activity, including HYIPs. Since the Liberty Reserve takedown, Perfect Money appears to be filling the void as the predominant digital currency used in HYIP-related transactions. Open-source internet searches revealed that Perfect Money

was a frequent topic of discussion on a website named "talkgold.com." And searches run by SA Adams from 2015 to 2016 revealed that Perfect Money and its exchangers have advertised on the website "talkgold.com" and a similar website "moneymakergroup.com," both of which are discussed below.

B. The "Talkgold.com" and "Moneymakergroup.com" HYIP Forums

16. Talkgold.com and moneymakergroup.com are publicly accessible websites dedicated primarily to the discussion and promotion of HYIPs. Research of the talkgold.com and moneymakergroup.com websites revealed that they are owned by Brian and Edward Krassenstein and operated under their business "E & B Advertising." The domain name "talkgold.com" was registered by Brian Krassenstein on January 2, 2003. The domain name "moneymakergroup.com" was registered by Jason Tucker in July 2004, but transferred to E & B Advertising sometime prior to November 2010.

17. HYIPs are a form of investment fraud similar to a "Ponzi scheme," "pyramid scheme," or "multi-level marketing scheme."

- a. A typical HYIP lures "investors" (*i.e.*, victims) by promising extraordinarily high rates of return on investments or dividends, sometimes tied as an incentive to the recruitment of other "investors." The perpetrators usually disclose little or no detail about the underlying management, location, or other aspects of how the funds are being invested. HYIPs often pay out apparent "returns" or "dividends" during the early stages of the scheme in order to create the appearance of legitimacy. These "dividends" are, in reality, taken from the money "invested" by new victims. Investment fraud experts refer to such payments as "lulling payments." HYIP schemes conclude when the perpetrators delete their websites, empty their accounts, and abscond with their victims' money.
- b. In order to evade prosecution, HYIP organizers often operate through shell corporations established in countries with lax enforcement of fraud laws. They also use so-called "bulletproof" internet hosting providers who shield the HYIP organizers from victim complaints and law enforcement scrutiny.

- c. Among those who are knowledgeable about and experienced with HYIPs, there are some who "invest" in the programs with the awareness that they are Ponzi schemes. They do so with the belief that, if they enter the scheme early enough, they can reap a profit before the scheme terminates and the payments stop. Such individuals are aided in this practice by "monitor sites" which are established to publicize which HYIPs are currently paying and which are not. As discussed below, Brian and Edward Krassenstein have maintained HYIP monitor sites including "goldrater.com."
- d. Prior the takedown of Liberty Reserve, HYIP organizers required investors/victims to transmit funds utilizing Liberty Reserve in order to participate in the HYIP. Since the Liberty Reserve prosecution, Perfect Money appears to be filling the void left by Liberty Reserve and has become the dominant method of transferring funds in and out of the HYIPs advertised on talkgold.com and moneymakergroup.com.
- e. The fraudulent nature of HYIPs is well known to regulators. The Financial Industry Regulatory Authority (FINRA) maintains an "Investor Alert" webpage dedicated to warning investors that "virtually every HYIP [the agency] has seen has the hallmarks of fraud." The page lists warning signs including "high, unsustainable yields" and "unclear methodology for achieving returns." It also explains that the "HYIP world" involves: 1) sites which rank HYIPs, 2) sites which "teach" investors about HYIPs, and 3) digital currency systems which are the means for transferring money in and out of HYIPs.

18. Both talkgold.com and moneymakergroup.com are structured as discussion forums in which users can post and respond to "threads," or conversations, on various topics. The description below applies to talkgold.com, but moneymakergroup.com is similar in content and organization:

- a. Discussion threads on talkgold.com are organized by category. The largest and most popular category is titled "HYIPs - High Yield Investment Programs." Samples of discussion threads in this category dating back to 2005 have been reviewed. Each thread is devoted to a particular HYIP, and begins with a post describing the HYIP and the promised rates of return. As is typical for HYIPs, the advertised rates are extraordinarily high. For example, a thread dedicated to the "Reprofinance" HYIP, posted on June 6, 2010, advertised rates of 1.9% per day for 180 days (that is, a total gain of 342% over 180 days of simple interest, or significantly more if the

revenues are "reinvested," as is offered by some HYIPs). Subsequent posts to the thread consist of discussion of the HYIP by investors/victims and others. Early in a thread, users often post that they are receiving payments from the HYIP. As time goes on, however, users begin to complain that their money has been taken and that the HYIP is a scam. As of July 27, 2016, the "HYIPs" category contained 47,345 threads.

- b. A second discussion category on talkgold.com is titled "Closed Programs and Scam Warnings." This category is home to threads which were moved from the HYIPs category after they were identified by users as failing to pay returns. Once an HYIP thread attracts enough such user complaints, one of the site's administrators moves it into the "Closed Programs and Scam Warnings" category. As of July 27, 2016, the "Closed Programs and Scam Warnings" category contained 13,638 threads. A sampling of older threads from the "HYIPs" category, however, showed that many threads in that category received scam complaints but were never moved to the "Scams" category. It is therefore likely that the number of HYIP threads containing scam complaints is significantly greater than 13,638.
- c. Talkgold.com also offers a category titled "HYIP - AutoSurf Program Admin Talk." This category is a forum for the "administrators" of the "investment programs" (that is, the perpetrators of the frauds) to discuss business with one another. For example, in a thread titled "HYIP industry almost dead!" posted by user "currencymarket" on March 20, 2014, users discuss the difficulties faced by HYIPs in the wake of the Liberty Reserve takedown.
- d. Talkgold.com contains other discussion categories, such as "Bitcoin Games / Gambling" and "Debit Cards." However, the three HYIP-related categories described above represent a majority of the site's activity. As of June 29, 2016, they contain a total of 4,177,073 posts, or 80% of the site's total non-archived posts.
- e. In order to post on talkgold.com, users must register accounts with the forum. Each user account is granted a certain level of status. Some levels of status, including "Administrator," "Moderator," and "Super-Moderator," allow the user to perform tasks like moving threads from one category to another or "banning" users who have violated the rules of the forum. The highest status, "Administrator," belongs to only three of the site's 268,128 users.
- f. The investigation indicates that one of the "Administrator" accounts, "talkgold," appears to belong to Brian Krassenstein and/or Edward Krassenstein. The investigation has determined that: 1) the "talkgold" account's existence dates back to the founding of the

website; 2) the very first posts on the website were made by the account; 3) the account username, "talkgold," is the same as the name of the website; 4) the account is one of only three to hold the highest account status, "Administrator;" and 5) posts authored by the account are sometimes signed "brian."

- g. Analysis of posting activity by the account "talkgold" indicates that Brian Krassenstein and/or Edward Krassenstein have remained highly active in the day-to-day operation of the talkgold.com forums. As of July 27, 2016, the "talkgold" account has made roughly 19,000 posts, or an average of roughly four posts per day over the life of the forum.

19. Besides offering a forum for the promotion and discussion of HYIPs, talkgold.com and moneymakergroup.com also offer paid advertising space on their websites. On numerous occasions, these sites have been found to contain advertisements that usually promote HYIPs. For example, on talkgold.com in June 2016, the most prominent banner advertisement was for "Coince," a purported "British investment company" promising daily returns of 3%. Talkgold.com and moneymaker.com publish the rates charged for such advertisements. These rates are dramatically in excess of those ordinarily paid by legitimate businesses. For example, in the fall of 2016, talkgold.com charged \$399 per day, \$1997 per week, or \$7699 per month for its most prominent advertising spot. By comparison, another forum website run by the Krassensteins, "filesharingtalk.com," charges \$50 per week or \$150 per month for its most expensive advertising spot.

20. The talkgold.com site includes a "disclaimer" which purports to immunize the site from any liability. The disclaimer reads, in part: "Sites which ask you for money as an investment are extremely risky. They are not verified for legitimacy by talkgold.com since this is virtually impossible to do. It is possible that some of the sites advertising on talkgold.com are built on a Pyramid foundation or are outright scams. . . . Before investing

in any of these programs, please understand that they are a gamble, as it is almost impossible to determine the legitimacy of online investments. . . . By clicking on any ads you hereby agree to have taking all legal and financial risks upon yourself."

21. Publicly available records obtained via "whois" lookup indicate that Brian and Edward Krassenstein operate multiple other HYIP-related websites in addition to talkgold.com and moneymakergroup.com:

- a. At various times, the Krassensteins owned and operated HYIP "monitor sites." These sites purported to track the performance of HYIPs and rate them based on their soundness as investment vehicles. HYIP monitor sites maintained by the Krassensteins included "goldrater.com," "gamesofgold.com," "rankhyips.com," and "web-life.org." The front page of web-life.org claimed, "We monitor programs based on investments that we have in programs, inside info that we receive from Web Life Members, admin updates and general opinion from around all the HYIP forums. If you believe that a program is not rated correctly or is listed as paying and in your opinion is not, please PM edward [Edward Krassenstein] on the forum and advise of the details and if necessary the rating will be promptly changed." Web-life.org also contained a flashing banner claiming that the site was "the ONLY safelist for HYIP."
- b. At various times, the Krassensteins owned and operated web hosting services marketed to HYIPs, including "smileyhosting.com" and "gold-hosting.com." These sites offered server space used by HYIP operators to publish their websites on the internet.
- c. At various times, the Krassensteins owned and operated other HYIP-related sites and services, including "HYIPMailer," a mailing list for information on HYIPs, and "hyipbanners.com," a site that offered to sell banner advertising space to HYIP operators.
- d. The Krassensteins' various HYIP-related websites overlapped extensively in their functionality. For example, talkgold.com and moneymakergroup.com served substantially identical functions, and goldrater.com and web-life.org served substantially identical functions. To the casual visitor, it would have appeared that these sites were being operated independently from one another. For example, smileyhosting.com was promoted on talkgold.com by user "Salpou," who signed his post "Mario." However, "whois" data for the domain www.smileyhosting.com revealed that it was registered to Edward Krassenstein. The Krassensteins' network of apparently

unrelated HYIP sites promoted the appearance of a thriving HYIP "industry" with numerous independent players. In reality, however, the apparent community of HYIP sites was the product of a concerted effort by the Krassensteins, designed to ensure a continuous supply of new HYIP fraud victims and the continued enrichment of Brian Krassenstein, Edward Krassenstein, and their coconspirators.

22. Based on their more than ten years of experience with HYIPs - including maintaining multiple discussion forums devoted to HYIPs, posting actively on those forums, establishing a "scams" category which has grown to more than 13,000 threads, operating sites to rate and track HYIPs, offering server hosting services for HYIPs, and maintaining a mailing list dedicated to HYIPs - there is reasonable cause to believe that Brian and Edward Krassenstein would have known that virtually all, if not all, HYIPs are fraud schemes and not legitimate investment vehicles.

C. THE HYIPS

23. As discussed above, both talkgold.com and moneymakergroup.com were internet forums where HYIPs were promoted, discussed, and advertised. Tens of thousands of HYIPs have been discussed in dedicated discussion threads on talkgold.com and moneymakergroup.com. Again, as discussed above, HYIPs are typically operated as online Ponzi schemes, and are by nature fraudulent. The following paragraphs describe in more detail five HYIPs that were discussed and promoted through dedicated threads on talkgold.com. These HYIPs are typical and representative of the HYIPs that were promoted, discussed, and advertised on talkgold.com and moneymakergroup.com.

a. The "Leopard Fund" HYIP

24. On November 25, 2005, the Administrator account "talkgold" posted a thread titled "The Leopard Fund - theleopardfund.com" to the talkgold.com HYIP forum,

apparently on behalf of the operators of the "Leopard Fund." The post included the text, "This thread is for the discussion of theleopardfund. It pays 5% per month. Please discuss this program in this thread." Posts on the thread discussing the Leopard Fund HYIP suggested that the HYIP was active through at least March 2007.

25. The Leopard Fund and affiliated HYIPs were the subject of an investigation by the FBI. That investigation ultimately resulted in the conviction by jury of the Leopard Fund's operator, David Boyner Prince, for five counts of wire fraud (N.D. Cal. case no. 3:10cr153). Evidence at Prince's trial, including expert testimony by a FINRA analyst, showed that the Leopard Fund and related schemes were run as Ponzi schemes in which investor funds were used to pay supposed "dividends" and ultimately diverted for the personal enrichment of Prince and his coconspirator.

b. The "PanaMoney" HYIP

26. The talkgold.com forum contained a thread titled "PanaMoney Technologies - PanaMoney.net," begun on September 23, 2008 by user "SilverA." "SilverA," purporting to be an investor in the PanaMoney HYIP, wrote statements including the following (all emphasis in original):

- a. "Just a few weeks ago I found PanaMoney.net, a managed Forex trading company. I invested the minimum and got the maximum!"
- b. "Now I get up to 2.8% DAILY and all I do is check my account and watch REAL TIME Forex trading sessions."
- c. "In addition, I just CAN'T HAVE ANY LOSS with the company as they cover possible trading losses."

27. Posts on the PanaMoney thread at talkgold.com revealed that the HYIP was using Liberty Reserve account XXXX7259 to accept investor funds and pay "dividends." SA Adams reviewed records from that account, which revealed the following activity:

- a. XXXX7259 received 14,361 deposits between September of 2008 and May of 2010. These deposits totaled \$5,276,290. The "memo" lines of these transactions indicate that a substantial portion, if not all, of them were deposits from investors in the HYIP.
- b. XXXX7259 made transfers totaling \$25,017 to Liberty Reserve account XXXX6552, registered to "Talkgold Advertising" in the name of Brian Krassenstein. XXXX7259 also made transfers totaling \$2,948 to Liberty Reserve account XXXX3299, registered to "MMG ads" in the name of Edward Krassenstein. Based on SA Adams' training and experience, and knowledge of the investigation, these transfers were payments for the advertisement of the HYIP on talkgold.com and moneymakergroup.com, respectively.
- c. XXXX7259 made transfers totaling \$30,083 to Liberty Reserve account XXXX3022, with the account name "server4sale." Server4Sale is an Internet Service Provider and server rental business. Based on SA Adams' training and experience, this transfer was payment for the rental of web servers used to host the panamoney.net website.
- d. XXXX7259 made transfers totaling \$1,017,692 to Liberty Reserve accounts in the names of "Tori Musashi" and "Masioke Tisura." Each transfer into these accounts was almost immediately redirected to Liberty Reserve account XXXX4858. Funds in that account were subsequently withdrawn, often with the notation "exchange into wire" and occasionally specifying a destination bank in Cyprus or Latvia. Based on SA Adams' training and experience, the "Musashi" and "Tisura" accounts were used by the operators of the PanaMoney HYIP to launder the scheme's proceeds into account XXXX4858, after which time the funds were converted to cash overseas for the personal enrichment of the scheme's organizers.

28. The PanaMoney thread on talkgold.com was moved to the "Scams" forum in approximately May of 2010.

c. The "CSMFinance" HYIP

29. The talkgold.com forum contained a thread titled "CSMFinance Group - CSMFinance.com," started by user "varens" on September 20, 2009. The post advertised "1.7% daily interest for 200 days!" and "Initial deposit refund!"

30. SA Adams reviewed the Liberty Reserve account database for references to "CSM Finance." This search revealed that Liberty Reserve account XXXX5592 was registered to email address "contact@csmfinance.com." A majority of the money deposited into that account (64.5%) came from Liberty Reserve account XXXX2055, which had the account name "CSM Finance Group Ltd." Analysis of transaction records suggests that the accounts were used jointly to manage a Ponzi-style HYIP scheme. For example:

- a. XXXX5592 received 3,494 deposits, totaling \$963,043, from 2,281 unique Liberty Reserve accounts. The large number of unique depositors, coupled with the relatively small amount of each deposit (an average of \$305.66 per deposit), indicates that XXXX5592 was used to collect "investments" from victims of the HYIP. This interpretation is corroborated by posts to the CSMFinance thread on talkgold.com in which users reported that they had invested in the HYIP by sending money to Liberty Reserve account XXXX5592. (Other investors reported on the thread that they had invested in the HYIP by sending money to a separate Liberty Reserve account, XXXX0617, suggesting that CSMFinance's gross receipts were substantially in excess of the \$963,043 deposited into XXXX5592.)
- b. XXXX2055 made 72,481 withdrawals, totaling \$1,221,901, to 2,741 unique Liberty Reserve accounts. The large number of unique recipients, coupled with the relatively small amount of each withdrawal (an average of \$16.86 per withdrawal), indicates that XXXX2055 was used to make "lulling payments" to the HYIP's victims, as described in paragraph 17.a. above. This interpretation is corroborated by posts to the CSMFinance thread on talkgold.com in which investors reported that they had received payments from XXXX2055.
- c. XXXX5592 made 21 transfers, totaling \$114,533, to a Liberty Reserve account owned by "YourOwnSurf.com." XXXX2055 made 26 transfers, totaling \$77,161, to a Liberty Reserve account owned by "Intexchange." SA Adams knows both "YourOwnSurf.com" and "Intexchange" to be Liberty Reserve "exchangers" of the kind discussed in paragraph 14 above. As previously explained, the use of such exchangers was the only way for a Liberty Reserve user to transform the digital currency into real-world currency. These transfers represent the diversion of investor funds for the personal enrichment of the HYIP's operators.

- d. There was no evidence in either of the Liberty Reserve accounts that any funds had been used to purchase securities or otherwise directed to legitimate investment channels.
- e. In SA Adams' training and experience, based upon the cash flows in and out of the Liberty Reserve accounts, the cost of expenses such as the server rental, and the amount of money diverted to the operators of the HYIP, it would have been impossible for investors in CSMFinance to recover the principal they had invested, let alone the extraordinary rates promised by the HYIP's organizers.

31. According to posts on talkgold.com, during the operation of the CSMFinance HYIP, its operators posted a software application on the CSMFinance website and encouraged investors to download it. CSM Finance promised an enhanced user experience via this new program. Posts on the "talkgold.com" forum indicated that unsuspecting investors who downloaded the program later learned the computer program was a virus which gave the CSM Finance operators the ability to transfer funds from victims' Liberty Reserve accounts.

32. The CSMFinance thread on talkgold.com began showing a significant volume of fraud complaints in approximately March 2010, and was ultimately moved to the "Scams" forum.

d. The "Reprofinance" HYIP

33. The talkgold.com forum contained a thread titled "ReProFinance - ReProFinance.com," started by user "skyLineGTR" on June 6, 2010. The post claimed that the HYIP was run by "the most successful and perspective [sic] corporation in its field of activity." The post advertised rates of return including "1.5/1.9% daily for 90/180 days."

34. SA Adams reviewed the Liberty Reserve account database for references to "Reprofinance." This search revealed that Liberty Reserve account XXXX6408 was registered to email address "reprofinance@gmail.com." Virtually all of the funds

transferred into that account (99.6%) came from Liberty Reserve account XXXX8513, which was registered to email address "keeper@reprofinance.com." Analysis of transaction records suggests that the accounts were used jointly to manage a Ponzi-style HYIP scheme. For example:

- a. XXXX6408 received 9,174 deposits, totaling \$1,707,398, from 5,085 unique Liberty Reserve accounts. The large number of unique depositors, coupled with the relatively small amount of each deposit (an average of \$186.11 per deposit), indicates that XXXX6408 was used to collect "investments" from victims of the HYIP. This interpretation is corroborated by posts to the Reprofinance thread on talkgold.com in which users reported that they had invested in the HYIP by sending money to Liberty Reserve account XXXX6408.
- b. XXXX6408 made 90,654 withdrawals, totaling \$1,053,415, to 4,122 unique Liberty Reserve accounts. The large number of unique recipients, coupled with the relatively small amount of each withdrawal (an average of \$11.62 per withdrawal), indicates that XXXX6408 was used to make "lulling payments" to the HYIP's victims. This interpretation is corroborated by posts to the ReproFinance thread on talkgold.com in which investors reported that they had received payments from XXXX6408.
- c. XXXX6408 made a \$3,000 transfer to Liberty Reserve account XXXX8076. SA Adams knows this account to be controlled by an entity that provides web hosting services to HYIPs and other entities engaged in unlawful activities. The notation for this transaction read, "payment for server - reprofinance." Based on SA Adams' training and experience, this transfer was payment for the rental of web servers used to host the Reprofinance website.
- d. XXXX6408 made withdrawals totaling \$808,701 into ten accounts which SA Adams knows to be owned by Liberty Reserve "exchangers" of the kind discussed in paragraph 14 above. As previously explained, the use of such exchangers was the only way for a Liberty Reserve user to transform the digital currency into real-world currency. These transfers represent the diversion of investor funds for the personal enrichment of the HYIP's operators.
- e. There was no evidence in either of the Liberty Reserve accounts that any funds had been used to purchase securities or otherwise directed to legitimate investment channels.
- f. In SA Adams' training and experience, based upon the cash flows in and out of the Liberty Reserve accounts, the cost of expenses such

as the server rental, and the amount of money diverted to the operators of the HYIP, it would have been impossible for investors in Reprofinance to recover the principal they had invested, let alone the extraordinary rates promised by the HYIP's organizers.

35. The ReproFinance thread on talkgold.com began showing a significant volume of fraud complaints in approximately January 2012, and was ultimately moved to the "Scams" forum.

e. The "Safe Depositary" HYIP

36. The talkgold.com forum contained a thread titled "safedepository - safedepository.com," started by user "hothyip" on August 9, 2010. The post advertised four "funds" — the "Virtax Fund," the "Rovasion Fund," the "Orston Fund," and the "Grand Fund" — promising daily interest rates between 1.6% and 2.3%.

37. SA Adams reviewed the Liberty Reserve account database for references to "Safe Depositary." This search revealed that Liberty Reserve account XXXX0421 was registered to email address "safedepository@yahoo.com." Virtually all of the funds transferred into that account (97.7%) came from Liberty Reserve account XXXX4597, which was registered to email address "safedepository@safe-mail.net." Analysis of transaction records suggests that the accounts were used jointly to manage a Ponzi-style HYIP scheme. For example:

- a. XXXX4597 received 10,304 deposits, totaling \$3,149,489, from 5,655 unique Liberty Reserve accounts. The large number of unique depositors, coupled with the relatively small amount of each deposit (an average of \$305.66 per deposit), indicates that XXXX4597 was used to collect "investments" from victims of the HYIP. This interpretation is corroborated by posts to the Safe Depositary thread on talkgold.com in which users reported that they had invested in the HYIP by sending money to Liberty Reserve account XXXX4597.
- b. XXXX0421 made 131,782 withdrawals, totaling \$2,625,617, to 4,557 unique Liberty Reserve accounts. The large number of unique recipients, coupled with the relatively small amount of each

withdrawal (an average of \$19.92 per withdrawal), indicates that XXXX0421 was used to make "lulling payments" to the HYIP's victims. This interpretation is corroborated by posts to the Safe Depository thread on talkgold.com in which investors reported that they had received payments from XXXX0421.

- c. XXXX4597 made withdrawals totaling \$129,472 into accounts which, based upon their account names, appear to be under the control of operators of HYIP monitoring sites of the kind discussed in paragraph 17.c. above. These payments were made for the purpose of promoting the HYIP to potential victims.
- d. XXXX4597 made withdrawals totaling \$441,942 into fifteen accounts which SA Adams knows to be owned by Liberty Reserve "exchangers" of the kind discussed in paragraph 14 above. These transfers represent the diversion of investor funds for the personal enrichment of the HYIP's operators.
- e. There was no evidence in either of the Liberty Reserve accounts that any funds had been used to purchase securities or otherwise directed to legitimate investment channels.
- f. In SA Adams' training and experience, based upon the cash flows in and out of the Liberty Reserve accounts, the cost of expenses such as the server rental, and the amount of money diverted to the operators of the HYIP, it would have been impossible for investors in Safe Depository to recover the principal they had invested, let alone the extraordinary rates promised by the HYIP's organizers.

38. The Safe Depository thread on talkgold.com began showing a significant volume of fraud complaints in approximately October 2011, and was ultimately moved to the "Scams" forum.

III. FINANCIAL ANALYSIS

A. Purchase of the Cape Coral Property

39. The Cape Coral property was purchased jointly by Brian and Edward Krassenstein on July 14, 2009. Attorney Joseph Troiano conducted the escrow for the sale. A search of the Lee County Assessor's records, as well as documents obtained from the title agent conducting the closing of the property on November 9, 2016, show that the property was purchased by the Krassensteins for \$450,000.00. Bank records

indicate that on July 13, 2009, days prior to the close of escrow, \$465,000.00 was sent via wire transfer to Joseph A. Troiano Esq. from Bank of America Checking Account Number XXXXXXXX5167 held by Brian and Edward Krassenstein ("BOA -5167").

1. *Funding of BOA -5167*

40. BOA -5167 was opened on August 31, 2001. The signature card lists Brian and Edward Krassenstein as joint account holders and the only authorized signers on the account.

41. An analysis was conducted on the source of funds deposited into BOA -5167 by a financial investigator to determine if fraud proceeds were used to make the purchase of the property. The analysis revealed that the only source of funds deposited into BOA -5167 between June 11, 2009 and July 13, 2009 (date of \$465,000 wire to purchase the property), were:

- a. \$200,000 transfer from Bank of America Savings Account Number XXXXXXXX2548 held by Brian and Edward Krassenstein ("BOA -2548");¹
- b. CD redemption for \$365,956.47;²

¹ BOA -2548 is a savings account and the only deposits and withdrawals into this account during 2009 were transfers to/from Bank of America Checking Account Number XXXXXXXX7497 held by E&B Advertising ("BOA -7497"), plus interest. Between January 5, 2009 and June 11, 2009, the deposits into BOA -7497 totaled \$424,576.68. Of this total, only 6.75% of the total deposits into the account were found to be from what appear to be "clean sources," *i.e.*, legitimate fees earned by E&B advertising.

² Based upon SA Adams' review of the Krassenstein's financial records, and a review of the money they earned from operating websites devoted to the promotion of fraudulent HYIPs, SA Adams believes that the vast majority of the funds comprising the CD are traceable to proceeds obtain from the wire fraud offenses described herein.

- c. three deposits totaling \$15,587 from Alertpay Inc.³ and Technocash Inc⁴ (advertising fees associated with the promotion of the fraudulent HYIPs);
 - d. \$6,900 from Bank of America Checking Account Number XXXXXXXX7497 held by E&B Advertising ("BOA -7497");⁵ and
 - f. miscellaneous deposits totaling \$1,338.74.
2. *Sale of Cape Coral Property*

42. On August 22, 2016, Brian and Edward Krassenstein contracted with innocent third parties to purchase the Cape Coral property for \$575,000. The closing took place on November 9, 2016. The Krassensteins received approximately \$524,390.32 from the sale of the Cape Coral property. However, law enforcement seized the funds from the title company (located in the Middle District of Florida) conducting the closing of the property before the money was paid to the Krassensteins as the sale proceeds were traceable to the proceeds of the offenses described herein.

³ AlertPay, Inc. was rebranded and currently does business under the brand name Payza. Payza operates as a money transfer service and is listed as a method of payment that the Krassensteins accept to pay for advertisement fees on talkgold.com or moneymakergroup.com websites. Because Payza is listed as an accepted payment method to pay for advertising fees, it appears that these funds are from individuals who are renting advertisement space on the talkgold.com or moneymakergroup.com websites.

⁴ Technocash was an online wire transfer service located in Australia that ceased operation in June 2013 in the wake of the Liberty Reserve takedown. Technocash was listed in a suit filed by the Securities and Exchange Commission ("SEC") against a Ponzi scheme called Profitable Sunrise. In the suit, the SEC detailed that the proceeds from the Profitable Sunrise scheme were transferred via Technocash. A search revealed that Profitable Sunrise was the subject of an HYIP thread on talkgold.com.

⁵ Between January 5, 2009 and June 11, 2009, the deposits into this account totaled \$424,576.68. Of this total, only 6.75% of the total deposits into the account were found to be from what appear to be "clean sources," i.e., legitimate fees earned by E&B advertising

43. Because the property was purchased with wire fraud proceeds, the property, and the proceeds obtained from the sale of the property are subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

44. On or about August 18, 2017, the United States entered into a settlement agreement with Brian and Edward Krassenstein. Pursuant to the terms of the settlement agreement, the Krassensteins consented to the forfeiture of \$450,000 of the \$524,390.32 obtained from the sale of the Cape Coral property. See Composite Exhibit A, Brian and Edward Krassenstein's Consents to Forfeiture.

CONCLUSION


WHEREFORE, pursuant to Supplemental Rule G, Plaintiff United States requests that this Court issue an arrest warrant *in rem* pursuant to Supplemental Rule G(3)(b)(1), initiate a process of forfeiture against the Defendant Property, and duly notice all interested parties to appear and show cause why the forfeiture should not be decreed. The United States further requests the Court order the Defendant Property be forfeited to

the United States for disposition according to law and grant the United States such further relief as this case may require.

Dated: August 21, 2017

Respectfully submitted,

W. STEPHEN MULDROW
Acting United States Attorney

By: 
NICOLE M. ANDREJKO
Assistant United States Attorney
Florida Bar Number 0820601
400 W. Washington Street, Suite 3100
Orlando, Florida 32801
(407) 648-7500 – telephone
(407) 648-7643 – facsimile
E-mail: nicole.andrejko@usdoj.gov

VERIFICATION

Pursuant to 28 U.S.C. § 1746, I, Michael P. Adams, declare under penalty of perjury that:

I am a Special Agent with Homeland Security Investigations. I have read the foregoing Verified Complaint for Forfeiture *in Rem* and know the contents thereof, and that the matters contained in the Verified Complaint are true to my own knowledge and belief.

I have acquired my knowledge in this matter through my personal experience, observation, and investigation, and through information conveyed to me by other law enforcement officers, as well as information contained in the official files and records of the United States.

Executed this 18 day of August 2017.



Michael P. Adams, SA
Homeland Security Investigations

JS 44 (Rev. 11/15)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the clerk of court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

RECEIVED
 21 AUG 21 PM 3:43
 U.S. DISTRICT COURT
 NORTHERN DISTRICT OF FLORIDA
 PORTLAND, OREGON

I. (a) PLAINTIFFS
 United States of America

(b) County of Residence of First Listed Plaintiff _____
 (EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

DEFENDANTS
 Assets Identified in Paragraph One of Verified Complaint

County of Residence of First Listed Defendant _____
 (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

1 U.S. Government Plaintiff

2 U.S. Government Defendant

3 Federal Question (U.S. Government Not a Party)

4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

	PTF	DEF		PTF	DEF
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input type="checkbox"/> 4
Citizen of Another State	<input type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input checked="" type="checkbox"/> 690 Other	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
<input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement	<input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act	<input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g))	<input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609

V. ORIGIN (Place an "X" in One Box Only)

1 Original Proceeding 2 Removed from State Court 3 Remanded from Appellate Court 4 Reinstated or Reopened 5 Transferred from Another District (specify) 6 Multidistrict Litigation

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
 18 U.S.C. Sections 1343 and 1349

Brief description of cause:
 wire fraud offenses

VII. REQUESTED IN COMPLAINT: CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$ _____ CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY (See instructions): JUDGE _____ DOCKET NUMBER _____

DATE: 8/21/17 SIGNATURE OF ATTORNEY OF RECORD: *Ducob M. Quacy*

FOR OFFICE USE ONLY: RECEIPT # W AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

2:17-cv-474-fm-38MRM