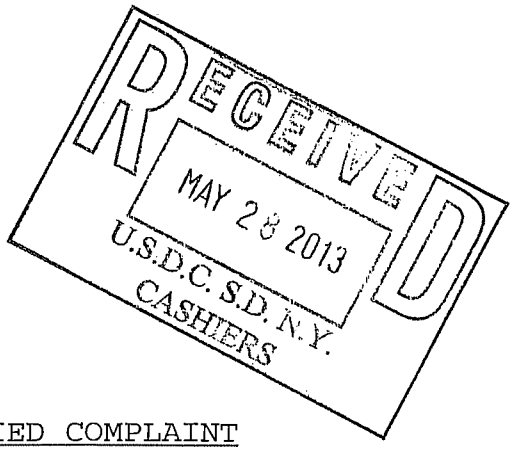
JUDGE [redacted]

PREET BHARARA
United States Attorney for
the Southern District of New York
By: [redacted]

Assistant United States Attorneys
One St. Andrew's Plaza
New York, New York 10007
Tel. [redacted]

13 CIV 3565



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - - - - - - - - - - - - - - - - -x

UNITED STATES OF AMERICA, :

Plaintiff, : VERIFIED COMPLAINT

- v. - : 13 Civ.

THE FOLLOWING DOMAIN NAMES: :

WM-CENTER.COM; :
E-NAIRA.COM;
ECARDONE.COM; :
EBUYGOLD.COM;
GETEMONEY.COM; :
EPAYMONSTER.COM;
INSTANTGOLDNG.COM; :
JTGOLD.COM;
GOLDNAIRAEXCHANGE.COM; :
SUPERCHANGE.RU;
WEBMONEY.CO.NZ; :
M-GOLD.COM;
GOLDMEDIATOR.COM; :
ABSOLUTEXCHANGE.EU;
MEWAHGOLD.COM; :
CENTREGOLD.CA;
ELECTRUMX.COM; :
TUKARDUID.COM;
ENTELNOVA.COM; :
TACOAUTHORIZED.COM;
INTEXCHANGE.COM; :
UKRNETMONEY.COM;
WMIRK.COM; :
NIGERIAGOLDEXCHANGER.COM;
EDEALSPOT.COM; :
DUYDUYCHANGER.COM;
MAGNETIC-EXCHANGE.COM; :
MONEYEXCHANGE.VN;

ABC-EX.NET; :
MI-BILLETERA.COM;
NICCIEXCHANGE.COM; :
EXHERE.COM;
ALERTEXCHANGER.COM; :
VELAEXCHANGE.COM;
GOLDEXPAY.COM; :

Defendants-in-rem. :

- - - - - - - - - - - - - - - - - - -x

Plaintiff United States of America, by its attorney, Preet Bharara, United States Attorney for the Southern District of New York, for its verified complaint alleges, upon information and belief, as follows:

I. JURISDICTION AND VENUE

1. This action is brought by the United States of America pursuant to Title 18, United States Code, Section 981(a)(1)(A), seeking the forfeiture of the following domain names: WM-CENTER.COM; E-NAIRA.COM; ECARDONE.COM; EBUYGOLD.COM; GETEMONEY.COM; EPAYMONSTER.COM; INSTANTGOLDNG.COM; JTGOLD.COM; GOLDNAIRAEXCHANGE.COM; SUPERCHANGE.RU; WEBMONEY.CO.NZ; M-GOLD.COM; GOLDMEDIATOR.COM; ABSOLUTEXCHANGE.EU; MEWAHGOLD.COM; CENTREGOLD.CA; ELECTRUMX.COM; TUKARDUID.COM; ENTELNOVA.COM; TACOAUTHORIZED.COM; INTEXCHANGE.COM; UKRNETMONEY.COM; WMIRK.COM; NIGERIAGOLDEXCHANGER.COM; EDEALSPOT.COM; DUYDUYCHANGER.COM; MAGNETIC-EXCHANGE.COM; MONEYEXCHANGE.VN; ABC-EX.NET; MI-BILLETERA.COM; NICCIEXCHANGE.COM; EXHERE.COM; ALERTEXCHANGER.COM;

VELAEXCHANGE.COM; and GOLDEXPAY.COM (collectively the "Defendant Domain Names").

2. This Court has jurisdiction over this action pursuant to Title 28, United States Code, Section 1355(b)(1), which provides that a forfeiture action or proceeding may be brought in the district court for the district in which any of the acts or omissions giving rise to the forfeiture occurred.

3. Venue is proper pursuant to Title 28, United States Code, Section 1395(a) because the cause of action accrued in the Southern District of New York, and the Defendant Domain Names are found in the Southern District of New York, in that they were accessed by computers located in the Southern District of New York.

4. Venue is further proper pursuant to Title 28, United States Code, Section 1395(b) because the property that the United States seeks to forfeit is found in the Southern District of New York, in that the Defendant Domain Names were accessed by computers located in the Southern District of New York.

II. THE DEFENDANT DOMAIN NAMES ARE FORFEITABLE PROPERTY

Background

5. For years, Liberty Reserve S.A. ("Liberty Reserve"), a company incorporated in Costa Rica in 2006, operated one of the world's most widely used digital currencies. Through its website, www.libertyreserve.com, Liberty Reserve provided its

users with what it described as "instant, real-time currency for international commerce," which can be used to "send and receive payments from anyone, anywhere on the globe." Liberty Reserve also touted itself as the Internet's "largest payment processor and money transfer system," serving "millions" of people around the world, including the United States. At no time, however, did Liberty Reserve register with the United States Department of the Treasury as a money transmitting business.

6. Arthur Budovsky ("Budovsky"), Vladimir Kats ("Kats"), Ahmed Yassine Abdelghani ("Yassine"), Azzeddine El Amine ("El Amine"), Allan Esteban Hidalgo Jimenez ("Hidalgo"), Mark Marmilev ("Marmilev"), and Maxim Chukharev ("Chukharev") intentionally created, structured, and operated Liberty Reserve as a criminal business venture, one designed to help criminals conduct illegal transactions and launder the proceeds of their crimes. Liberty Reserve was designed to attract and maintain a customer base of criminals by, among other things, enabling users to conduct anonymous and untraceable financial transactions.

7. Liberty Reserve emerged as one of the principal means by which cyber-criminals around the world distributed, stored, and laundered the proceeds of their illegal activity. Indeed, Liberty Reserve became a financial hub of the cyber-crime world, facilitating a broad range of online criminal activity, including credit card fraud, identity theft, investment fraud,

computer hacking, child pornography, and narcotics trafficking. Virtually all of Liberty Reserve's business derived from suspected criminal activity.

8. The scope of Liberty Reserve's criminal operations was staggering. Estimated to have had more than one million users worldwide, with more than 200,000 users in the United States, Liberty Reserve processed more than 12 million financial transactions annually, with a combined value of more than $1.4 billion. Overall, from 2006 to May 2013, Liberty Reserve processed an estimated 55 million separate financial transactions and is believed to have laundered more than $6 billion in criminal proceeds.

9. To use Liberty Reserve's digital currency, commonly referred to as "LR," a user first was required to open an account through the Liberty Reserve website. In registering, the user was required to provide basic identifying information, such as name, address, and date of birth. However, unlike traditional banks or legitimate online payment processors, Liberty Reserve did not require users to validate their identity information, such as by providing official identification documents or a credit card. Accounts could therefore be opened easily using fictitious or anonymous identities.

10. Once a user established an account with Liberty Reserve, the user could then conduct transactions with other

Liberty Reserve users. That is, the user could receive transfers of LR from other users' accounts, and transfer LR from his own account to other users - including any "merchants" that accepted LR as payment. Liberty Reserve charged a one-percent fee every time a user transferred LR to another user through the Liberty Reserve system, up to a maximum fee of $2.99 per transaction. In addition, for an additional "privacy fee" of 75 cents per transaction, a user could hide his own Liberty Reserve account number when transferring funds, effectively making the transfer completely untraceable, even within Liberty Reserve's already opaque system.

11. To add an additional layer of anonymity, Liberty Reserve did not permit users to fund their accounts by transferring money to Liberty Reserve directly, such as by issuing a credit card payment or wire transfer to Liberty Reserve. Nor could Liberty Reserve users withdraw funds from their accounts directly, such as through an ATM withdrawal. Instead, Liberty Reserve users were required to make any deposits or withdrawals through the use of third-party "exchangers," thus enabling Liberty Reserve to avoid collecting any information about its users through banking transactions or other activity that would leave a centralized financial paper trail.

12. Liberty Reserve's "exchangers" were third-party entities that maintained direct financial relationships with

Liberty Reserve, buying and selling LR in bulk from Liberty Reserve in exchange for mainstream currency. The exchangers in turn bought and sold this LR in smaller transactions with end users in exchange for mainstream currency. Thus, in order to fund a Liberty Reserve account, a user was required to transmit mainstream currency in some fashion (through a money remitter, for example) to an exchanger. Upon receiving the user's payment, the exchanger credited the user's Liberty Reserve account with a corresponding amount of LR, by transferring LR from the exchanger's Liberty Reserve account to the user's account. Similarly, if a Liberty Reserve user wished to withdraw funds from his account, the user was required to transfer LR from his Liberty Reserve account to an exchanger's Liberty Reserve account, and the exchanger then made arrangements to provide the user a corresponding amount of mainstream currency.

13. The Liberty Reserve website recommended a number of "pre-approved" exchangers, among which were the exchangers that use the Defendant Domain Names for their websites. These exchangers tended to be unlicensed money transmitting businesses operating without significant governmental oversight or regulation, concentrated in Malaysia, Russia, Nigeria, and Vietnam. The exchangers charged transaction fees for their services, typically amounting to five percent or more of the funds being exchanged. Such fees were much higher than those

charged by mainstream banks or payment processors for comparable money transfers.

The Related Criminal Case

14. On May 20, 2013, a grand jury in the Southern District of New York returned a sealed indictment charging Liberty Reserve, Budovsky, Kats, Yassine, El Amine, Hidalgo, Marmilev, and Chukharev with conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h) (Count One); conspiracy to operate an unlicensed money transmitting business, in violation of 18 U.S.C. § 371 (Count 2); and operation of an unlicensed money transmitting business, in violation of 18 U.S.C. §§ 1960 and 2 (Count Three). See United States v. Liberty Reserve, et al., 13 Cr. 368 ([redacted]) (the "Indictment"). The Indictment alleges, among other things, that the defendants operated an international online digital currency service and money transfer system through the website www.libertyreserve.com that was designed to attract and maintain a customer base of criminals and, in fact, became the online service preferred by cyber-criminals around the world for distributing, storing, and laundering the proceeds of their criminal activity, in violation of 18 U.S.C. § 1956(h). Furthermore, as alleged in the Indictment, by operating the Liberty Reserve website, the defendants operated, and engaged in a conspiracy to operate, an unlicensed money transmitting business, in violation of 18 U.S.C.

§§ 1960, 371, and 2. A true and correct copy of the Indictment is attached hereto as Exhibit A and is incorporated by reference as if fully set forth herein.

15. As part of the criminal case against Liberty Reserve et al., on May 23, 2013, the United States obtained a post-indictment seizure warrant (the "Seizure Warrant"), pursuant to 21 U.S.C. § 853(e) and (f), for the domain name LibertyReserve.com, as well as for the domain names used by four online exchangers owned or controlled by certain of the individuals charged in the Indictment (the "Seized Domain Names").[1] The Honorable [redacted], United States District Judge, found probable cause to believe that the Seized Domain Names were property subject to seizure and criminal forfeiture pursuant to 18 U.S.C. § 982(a)(1). A true and correct copy of the Seizure Warrant is attached hereto as Exhibit B and is incorporated by reference as if fully set forth herein. A true and correct copy of the Declaration of Special Agent [redacted] of the United States Secret Service (the "[redacted] Decl.") submitted in support of the Government's application for the Seizure Warrant is annexed hereto as Exhibit C and is

[1] The four exchanger domain names that were subjects of the Seizure Warrant (ExchangeZone.com, Swiftexchanger.com, MoneyCentralMarket.com, and AsianaGold.com) are not named as in rem defendants in this action.

incorporated by reference as if fully set forth herein. The Seizure Warrant was executed on May 24, 2013.

16. Also on May 24, 2013, Budovsky, El Amine, Marmilev, Kats and Chukharev were arrested on the charges in the Indictment.

17. As further part of the criminal investigation, the United States obtained seizure warrants or restraining orders for 45 bank accounts located in the United States, Costa Rica, Cyprus, Australia, Morocco, Spain, Hong Kong, China, Latvia, and Russia, which have already resulted in the seizure or restraint of approximately $25 million. In addition, pursuant to court-authorized warrants, more than 45 searches and seizures have been carried out in multiple countries, including the United States, Costa Rica, Sweden, Switzerland, and the Netherlands.

Domain Names in General

18. Domain names operate as follows:

a. A domain name is a simple, easy-to-remember way for people to identify computers on the Internet. For example, "www.google.com" and "www.yahoo.com" are domain names.

b. The Domain Name System ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label to the left

specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain. For example, the domain name "www.example.com" means that the computer assigned that name is in the ".com" top-level domain and the "example" second-level domain, and is a web server (denoted by the "www").

c. DNS servers are computers connected to the Internet that convert domain names that are easy for people to remember into Internet Protocol ("IP") addresses, which are unique machine-readable numeric addresses that computers use to identify each other on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer connection to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. DNS servers can be said to "resolve" or "translate" domain names into IP addresses.

d. For each top-level domain (such as ".com"), there is a single company, called a "registry," that determines which second-level domain resolves to which IP address. For example, the registry for the ".tv," ".net," and ".com" top-level domains is VeriSign, Inc.

e. If an individual or business wants to purchase a domain name, they buy it through a company called a

"registrar." Network Solutions LLC ("Network Solutions") and GoDaddy.com Inc. ("GoDaddy") are two well-known examples of registrars, although there are hundreds of registrars on the Internet. The registrar, in turn, communicates this purchase to the relevant registry. The individual or business who purchases, or registers, a domain name is called a "registrant."

f. Registrants control the IP address, and thus the computer, to which the domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world simply by changing the IP address at the registry.

g. Registries and/or registrars maintain additional information about domain names, including the name and contact information of the registrant.

The Defendant Domain Names

19. In connection with the investigation, and based on their review of the various webpages that are accessible via the Defendant Domain Names, federal law enforcement agents learned the following:

20. The Liberty Reserve website, before it was shut down by federal law enforcement on May 24, 2013, displayed a list of "pre-approved" online exchangers, which included the websites affiliated with the Defendant Domain Names. As explained above, individuals wishing to use Liberty Reserve's anonymous digital

currency system were required to use an online exchanger in order to convert their LR digital currency into real currency, and vice-versa.

21. In or about May 2013, a federal law enforcement agent visited the sites affiliated with the Defendant Domain Names and took numerous "screen shots" of the sites, capturing what the websites looked like to one visiting the site on the Internet at that time. The websites all described their services as electronic currency exchange, e-currency exchange or digital currency exchange, and most also specifically advertised that they served as exchangers for Liberty Reserve.

22. For example, the website associated with E-NAIRA.COM, the defendant, held itself out as, "The leading Liberty Reserve exchanger located in Africa." The website associated with EPAYMONSTER.COM, the defendant, touted itself as, "One of Nigeria's largest and most trusted accredited Liberty Reserve exchangers." The website associated with GOLDNAIRAEXCHANGE.COM, the defendant, advertised that it was "Nigeria's First and Largest Liberty Reserve Exchanger." The website associated with EDEALSPOT.COM, the defendant, claimed that it "exclusively support[s] Liberty Reserve with the best rates."

23. Furthermore, the websites associated with the Defendant Domain Names provided exchanger services for users of

Liberty Reserve. This was determined by various methods, including reviewing bank records, analyzing server data, engaging in undercover transactions, and reviewing email correspondence.

III. PROBABLE CAUSE FOR FORFEITURE

24. As explained above and as alleged in the Indictment, Liberty Reserve and its principals engaged in a money laundering conspiracy by operating a digital currency website that catered to cyber-criminals. The exchanger websites associated with the Defendant Domain Names were directly involved in Liberty Reserve's money laundering operation, in at least two ways. First, they allowed users of Liberty Reserve's digital currency to exchange their real currency for LR, and their LR for real currency. In other words, the Defendant Domain Names were used to fund Liberty Reserve's Operations; without them, there would not have been money for Liberty Reserve to launder. Second, the Defendant Domain Names were used to add another layer of anonymity to each transaction processed through Liberty Reserve, thus directly appealing to cyber-criminals who were looking to launder the proceeds of their criminal activities.

25. Because the websites associated with the Defendant Domain Names bought and sold LR for real currency, they were involved in and facilitated Liberty Reserve's primary function, which was to launder money. Accordingly, the Defendant Domain Names are property involved in the money laundering conspiracy

charged in the Indictment, and are subject to forfeiture to the United States under 18 U.S.C. § 981(a)(1).

26. In sum, there is probable cause to believe that the Defendant Domain Names constitute property involved in a conspiracy to commit money laundering, or property traceable to such property, in violation of Title 18, United States Code, Section 1956(h). Accordingly, the Defendant Domain Names are subject to forfeiture to the United States of America pursuant to Title 18, United States Code, Section 981(a)(1)(A).

IV. CLAIM FOR FORFEITURE

27. Paragraphs 1 through 26 of this Complaint are repeated and realleged as if fully set forth herein.

28. Pursuant to 18 U.S.C. § 981(a)(1)(A), "[a]ny property, real or personal, involved in a transaction in violation of section 1956 [or] 1960 . . . of [Title 18], or any property traceable to such property," is subject to forfeiture.

29. Pursuant to Title 18, United States Code, Section 1956, commonly known as the "money laundering" statute, a person who:

> (a)(1) . . . knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity -

(A)(i) with the intent to promote the carrying on of specified unlawful activity; or

(ii) with intent to engage in conduct constituting a violation of section 7201 or 7206 of the Internal Revenue Code of 1986; or

(B) knowing that the transaction is designed in whole or in part -

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

(ii) to avoid a transaction reporting requirement under State or Federal law,

shall be guilty of a crime.

30. Title 18, United States Code, Section 1956 further provides, in pertinent part, that

(a)(2) Whoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States -

(B) knowing that the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part -

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity

shall be guilty of a crime.

31. Title 18, United States Code, Section 1956(h) further provides that "[a]ny person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy."

32. By reason of the above, the Defendant Domain Names are subject to forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(A).

WHEREFORE, plaintiff United States of America prays that process issue to enforce the forfeiture of the Defendant Domain Names and that all persons having an interest in the Defendant Domain Names be cited to appear and show cause why the forfeiture should not be decreed, and that this Court decree forfeiture of the Defendant Domain Names to the United States of America for disposition according to law, and that this Court grant plaintiff such further relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Dated: May 28, 2013
New York, New York

PREET BHARARA
United States Attorney for the
Southern District of New York

By: [redacted]

[redacted]

Assistant United States Attorneys
One Saint Andrew's Plaza
New York, New York 10007
Tel.: [redacted]
Facsimile: [redacted]

VERIFICATION

STATE OF NEW YORK)
COUNTY OF NEW YORK)
SOUTHERN DISTRICT OF NEW YORK)

[redacted], being duly sworn, deposes and says that he is a Special Agent with the United States Secret Service, and, as such, has responsibility for the within action; that he has read the foregoing complaint and knows the contents thereof, and that the same is true to the best of his own knowledge, information, and belief.

The sources of the deponent's information and the grounds for his belief are his personal knowledge and the official records and files of the United States Government.

Dated: New York, New York
May 28, 2013

[redacted]
Special Agent
United States Secret Service

Sworn to before me this
28th day of May, 2013

[redacted]
Notary Public

[redacted]
Notary Public, State of New York
No. [redacted]
Qualified in Nassau County
My Commission Expires May 6, 2014