

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

**AFFIDAVIT IN SUPPORT OF COMPLAINT FOR FORFEITURE**  
(18 U.S.C. §§ 981, 1957, 1960)

I, Roy Dotson, state as follows:

1. I am a Special Agent (“SA”) of the United States Secret Service (“USSS”), and have been so employed for approximately three and one half years. I am currently assigned to the Orlando Field Office. Among my duties as an SA, I am charged with the investigation of financial crimes, including check fraud, identity fraud, credit card fraud, bank and wire fraud and the manufacturing, possession and passing of counterfeit United States currency. Prior to my employment with the USSS, I was employed by the Brevard County Sheriff’s Office for nine years. My last assignment was that of a Federal Task Force Agent with the Drug Enforcement Administration. Among my duties as a Task Force Agent, I was charged with investigating large criminal organizations that distributed and sold controlled substances and financial crimes involving money laundering. Several of the investigations resulted in the seizures of criminally derived property, including, but not limited to, monetary instruments.

2. An investigation into the E-GOLD operation is being conducted jointly by the United States Secret Service, the Federal Bureau of Investigation, and the Internal Revenue Service. Information obtained as a result of the investigative efforts of each agency are being shared with agents from the other agency and have been incorporated into this affidavit. The facts set forth in this affidavit are based on my own personal knowledge; knowledge obtained from other 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; and information gained through my training and experience and the training and experience of others.

3. This affidavit is being submitted in support of a verified Complaint for Forfeiture *In Rem* against property seized from in the E-GOLD accounts listed below, all of which constitutes property involved in money laundering and the operation of an unlicensed money transmitting business, and thus is subject to forfeiture based upon 18 U.S.C. § 981(a)(1)(a), and is further property traceable to proceeds of “specified unlawful activity,” and thus is subject to forfeiture based on 18 U.S.C. § 981(a)(1)(c). The E-GOLD accounts listed below contain property that falls into one of three categories: (1) property involved in laundering the proceeds of child pornography; (2) property involved in laundering the proceeds of credit card fraud; and (3) property involved in laundering the proceeds of wire (investment) fraud. All of these accounts contain the digital currency “e-gold” that is allocated and transferred among accounts by e-gold, Ltd. The physical precious metals that are “backing” the e-gold are controlled by the E-GOLD operation and by Douglas Jackson and Barry Downey. The specific property is:

a. Property involved in laundering the proceeds of child pornography:

Name	Account number
lolitalist.info	4181605

b. Property involved in laundering the proceeds of access device fraud:

Name	Account number
“Maksik”	1751848
“Segvec”	3584940

c. Property involved laundering the proceeds of wire (investment) fraud:

Name	Account number
Legisi Holdings LLC	2636005, 2825136 and 2828872
Miguel Jimenez	3921533
Nawaaz Meerun	1359767 and 1424543
IFF "ULWES"	3830833 and 2094836
Sime Securities	1922141
World Investment Group	3931825, 3814228, 3751783, 3781244, 3711356, 3599523, 3729709, and 3686876
e-gold-invest.us	3297330
VIP Invest Club	3900642, 3900899, 3414996, 2739290, 2739330, 3744230, 3724455, 3777270, 3910742, 3622583, 3034142, and 4055663
Phoenix Surf	3114779
Freeland Ops	1141305, 1142733, 1146912, 1338640, 1426358, and 817253
ExpInvest International	2353188
E-Gold Daily Pro (EGDP)	2319629

d. Property involved in money laundering

Name	Accounts
1mdc	808080, 808081, and 808082

4. Based upon the evidence uncovered, there is reasonable cause to believe that the property contained in the above- identified E-GOLD accounts is involved in money laundering in violation of Title 18, United States Code, Section 1956, and is therefore subject to seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A), or is identical property found in the same place

or account, within one year, as the property involved in the offense giving rise to forfeiture, and therefore subject to seizure for forfeiture as provided by 18 U.S.C. § 984(a)(2), or property involved in a money laundering conspiracy, or involved in the operation of an unlicensed money transmitting business.

5. The transactions occurring in, and the total value of, the accounts described in this Affidavit for seizure are presented below in both grams of gold and U.S. dollars to reflect the way in which the owners and operators of the e-gold system record the transactions occurring in the e-gold accounts in their databases, as discussed more fully in paragraphs 18 and 19. To obtain the value subject to seizure in these accounts pursuant to the requested seizure warrant, it will be necessary to require e-gold, Ltd. and/or Gold & Silver Reserve, Inc. to convert the “e-gold” in the accounts specified to United States dollars or physical precious metals before turning the property over to the United States. Otherwise, the property in the accounts will remain as e-gold and thus entirely under the unsupervised control of e-gold, Ltd. and Gold & Silver Reserve, Inc. (defendants in the related criminal case), could be easily dissipated, and would be essentially without value should e-gold, Ltd. and or Gold & Silver Reserve, Inc., and other exchangers decide not to provide exchange services. Further, given that the United States is seeking the seizure of the e-gold accounts of some of those entities, exchange services may be partially, if not entirely unavailable after the seizure warrants are executed.

6. I have not included every detail of every aspect of the investigation for this affidavit. Rather, it only includes the information necessary to establish that reasonable cause exists to believe that the defendant property is subject to forfeiture.

### *Background on Digital Currency Issuers and Exchangers*

7. A “digital currency” is a medium of exchange offered over the Internet that is purportedly backed by precious metals and offers users another option for conducting on-line funds transfers. Digital currencies are generally marketed as offering global acceptance without the need for conversion between national currencies, and are valued at fluctuating rates tied to the price of a particular precious metal, especially gold. Digital currency is used for on-line commerce or for funds transfers between individuals for private purposes. While technically speaking, the owner of digital currency could have some right to acquire the actual metal behind the currency, digital currency users typically convert their value into a national currency when they want to take value out of the on-line system.

8. One of the earliest issuers of digital currency was e-gold, Ltd. (“E-GOLD”), which operates via the Internet using the domain name [www.e-gold.com](http://www.e-gold.com), and began offering the digital currency “e-gold” in 1996. E-GOLD appears as the most popular and prominent digital currency available on-line. e-gold is widely accepted as a payment mechanism for transactions involving credit card and identification fraud, high yield investment programs and other investment scams, and child exploitation. e-gold is not widely accepted by large or mainstream vendors.

9. There are four primary steps involved in a financial transaction using e-gold: (i) opening a digital currency account with E-GOLD; (ii) converting national currency into e-gold to fund the account; (iii) using e-gold to buy or sell a good or service or transfer funds to another person; and (iv) exchanging the e-gold back into national currency. E-GOLD needs two additional parties to complete these steps: (i) digital currency exchangers; and (ii) merchants or

individuals that are willing to accept e-gold for the payment of goods and services or to use the e-gold operation to transfer funds.

10. Digital currency exchangers take national currency from customers and exchange it into e-gold for purposes of funding a new E-GOLD account, or increasing the value of an existing account.

11. Exchangers also exchange e-gold back into national currency and are typically the only method by which users can obtain the value out of an E-GOLD account, short of taking possession of the precious metal itself, which is not always possible and practically never done. Each exchanger set its own terms and conditions on the types and amounts of national currency that it accepts for exchange. Some only accept transfers from banks or credit card accounts. Others accept cash and money orders. Most exchangers (including all of the domestic exchangers investigated) operate out of their home by using an Internet website to service customers, bank accounts for accepting cash and other deposits, and post office boxes for receipt of checks and other mailings.

12. The exchangers are an integral part of the e-gold operation. Some of these exchangers are sponsored by E-GOLD on its website and receive discounted rates for the e-gold they purchase to operate their businesses. While, generally, these exchangers also convert national currency to other online digital currencies, e-gold is the most prominent and extensively-used digital currency.

13. Individuals using digital currency exchangers typically incur fees on a per transaction basis. Fees/percentages incurred per transaction depend largely on the exchanger used. In some instances, the exchanger would charge up to 6% of the amount of funds

transferred. These fees assessed by the exchanger are referred to as “service fees.”

14. Users around the world can register for a free E-GOLD account via the E-GOLD website and fund their account through a third party digital currency exchanger or through E-GOLD’s own exchange service, which it called “OmniPay.” Once open and funded, account holders can access their accounts through the Internet and conduct transactions with other parties anywhere in the world. E-GOLD advertises on its website that it is “an alternative Internet payment system” that “empowers people to use gold as money.” E-GOLD advertises its service as “Better Money,” and “Internet Payments 100% backed by Gold.”

15. The digital currency e-gold can be traded among online account holders using the Internet. With only a valid e-mail address, each account holder is issued an e-gold account, which can be used to send and receive any amount of e-gold to/from other e-gold account holders anywhere in the world anonymously, instantaneously, and irreversibly. E-GOLD, in combination with other unregistered money service businesses, has become a preferred funds transfer mechanism for a multitude of criminal financial transactions.

### **The E-Gold Operation**

16. The e-gold operation consists of two entities, e-gold, Ltd. (“E-GOLD”) and Gold & Silver Reserve, Inc. (“GSR”), and three individuals, Douglas Jackson, Barry Downey, and Reid Jackson (collectively the “e-gold operation”). As described above, E-GOLD is the issuer of the digital currency known as “e-gold,” which functions as an alternative payment system, is purportedly backed by stored physical gold, and operates via the Internet using the domain name www.e-gold.com. GSR describes itself as the operator of E-GOLD and its respective website, and offers a digital currency exchange service (known as OmniPay) for individuals wishing to

purchase, transfer, and/or sell e-gold. OmniPay operates via the Internet using the domain name www.omnipay.com. While E-GOLD was incorporated in Nevis, the e-gold operation is located entirely in Florida, including its physical business location at 175 E. Nasa Blvd., Suite 300, Melbourne, Florida (including management, employees, and records) and computer servers that conduct its on-line operations. All e-gold transactions take place through the e-gold server and database located in Florida. All e-gold accounts and balances are maintained there as well. The e-gold operation's owners/operators include Douglas Jackson, Barry Downey, and Reid Jackson.

17. Ownership of e-gold. According to the e-gold website, the gold bullion allegedly backing the digital currency e-gold is physically held in allocated storage in overseas vaults by three repositories (*i.e.*, custodians) on behalf of the e-gold Bullion Reserve Special Purpose Trust. Also according to the e-gold website, the e-gold Bullion Reserve Special Purpose Trust was established for holding title for the gold collectively on behalf of the e-gold account holders. The e-gold Account User Agreement provides that an "e-metal balance is accounted by weight and constitutes title to that precise fine weight of metal." As such, the beneficiaries of the e-gold Bullion Reserve Special Purpose Trust are purportedly the account holders of e-gold accounts (collectively) and e-gold account holders purportedly hold title to the "precise fine weight of metal" backing the amount of e-gold in their account. However, the account holders' right to claim the physical gold in exchange for their e-gold is severely circumscribed by the user agreement's conditional right of redemption, which provides, among other things, that the minimum quantity for redemption would "in no case ... be less than the fine weight of the smallest bullion items held in storage." According to the e-gold website, E-GOLD's lowest ounce bar is a 32 ounce bar, worth approximately \$21,248. As a result, at a minimum, an

account holder can only exchange \$21,248 worth of e-gold in order to take physical possession of the gold. Finally, the e-gold website also provides that “[N]o metal may be removed from storage or any other disposition made without the signatures of both e-gold Ltd. and a third party Escrow Agent of good reputation.” This further conditions an e-gold account holder’s ability to obtain physical possession of any gold.

**Examination of E-GOLD Customer Account Database**

18. Search warrants were conducted on the business location of the e-gold operation as well as the location of the operation’s computer servers in December of 2005. Approximately three terabytes of digital evidence (three quadrillion characters of information) and 100 boxes of documentary evidence (approximately 288,000 pages) were seized.

19. Evidence regarding the transactions and account activity of e-gold account holders and its customers was obtained through examination the e-gold operation’s computer databases. The e-gold operation maintains Microsoft SQL server databases housing customer profiles and transaction histories of e-gold account holders, as well as OmniPay customers. Your Affiant obtained copies of these databases by imaging servers located at AT&T in Orlando, Florida<sup>1</sup> and seizing back-up tapes at the Melbourne offices of the e-gold operation pursuant to a December 16, 2005 search warrant issued by a Magistrate Judge in Orlando, Florida. The e-gold operation also provided an additional update of the database information (by copying the database to hard drives) for the period of November 2005 through October 2006 in response to grand jury subpoenas issued on May 22, 2006 and October 25, 2006. The e-gold operation provided a

---

<sup>1</sup> Both the e-gold and OmniPay websites and corresponding customer databases are run from servers co-located at AT&T in Orlando, Florida, approximately 100 miles from GSR’s physical business location in Melbourne, Florida.

second update of the database information (by copying the database to an external hard drive) for the period of October 2006 through March 2007 in response to a grand jury subpoena issued on March 6, 2007.

20. From these images of the servers and copies of the databases, I was able to reconstruct the customer profiles and transaction histories for e-gold account holders by transferring the database information on each account holder into a Microsoft Excel spreadsheet.

The following specific information was available for each e-gold account:

- a. Customer profile: point of contact information for the e-gold account holder, including account name, mailing address, and email address supplied by the customer.
- b. Transaction history: list of transactions demonstrating e-gold being transferred into and out of the account. For each transaction, the history contains, among other things, the date of the transaction, the type of transaction (e.g., whether e-gold is being transferred into or out of the account), the e-gold account number of the other party to the transaction (also known as the “counteraccount”), the amount of the transaction, the Internet Protocol (IP) address of the transferor of e-gold, and a place for the customer to make a notation about the purpose of the transaction (also known as the “memo” field).
- c. Value limits: The e-gold operation had a policy of placing a “value-limit” on accounts that it believed to be engaged in criminal activity or where bogus contact information had been entered by the account holder. An account holder with a “value limit” placed on his or her account was restricted from receiving any

further e-gold into his or her account, although s/he continued to be free to spend or transfer any e-gold out of his or her account. When a “value-limit” was placed on an account, a notation of the basis for the “value-limit” (such as for “child porn,” “scammer,” or “cc fraud”) was entered in the user’s account profile in the e-gold database and would appear, along with the date the value limit was placed, in the transaction history information.

21. From these images of the servers and copies of the databases I was able to perform various searches of the database, including, for example:
  - a. Searches for particular terms used in the “memo” fields in the customer transaction histories, such as “lolita,” “IDs” or “HYIP” to indicate that “e-gold” was being used for the purchase and sale of contraband or otherwise used for criminal purposes.
  - b. Searches for particular e-mail addresses of known criminals or criminal entities that may have been used to create an e-gold account.
  - c. Searches for particular names or nicknames of known criminals or criminal entities that may have been used to create an e-gold account.
  - e. Searches for notations of the basis for the e-gold operation placing “value-limits” on particular accounts, such as for “child porn,” “scammer,” or “cc fraud”.

**Property Involved in Money Laundering:**  
**Child Pornography Proceeds**

---

22. Child Pornography is defined pursuant to Title 18, United States Code, Section 2256(8) as “any visual depiction, including any photography, film, video, picture or computer or

computer generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or ©) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.”

23. The term “visual depiction,” as used herein, is defined pursuant to Title 18, United States Code, Section 2256(5) as including “undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.” The term “minor,” as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1), as “any person under the age of eighteen years.” The term “sexually explicit conduct,” as used herein, is defined pursuant to Title 18, United States Code, Section 2256(2) as “actual or simulated (A) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (B) bestiality; ©) masturbation; (D) sadistic or masochistic abuse; or (E) lascivious exhibition of the genitals or pubic area of any person.” Factors to be considered in determining if an image constitutes “lascivious exhibition” include 1) whether the focal point of the depiction is the child’s genitalia or pubic area; 2) whether the setting is sexually suggestive, i.e., in a place or pose generally associated with sexual activity; 3) whether the child is depicted in an unnatural pose or in inappropriate attire, considering the age of the child; 4) whether the child is full or partially clothed or nude; 5) whether the depiction suggest sexual coyness or a willingness to engage in

sexual activity; 6) whether the depiction is intended or designed to elicit a sexual response in the viewer.”

24. The term “child erotica,” as used herein, means “any material, relating to children, that serves a sexual purpose for a given individual.” See Kenneth V. Lanning, *Child Molesters: A Behavioral Analysis* (2001) at 65. Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

25. This investigation has revealed that e-gold is widely used in the child pornography market, and is often the only payment mechanism available to purchase child pornography images and videos on certain websites. Further, investigation has revealed a number of e-gold accounts being used by sellers of child pornography to collect, hide, and distribute the proceeds of their illegal sales. Typically, one e-gold account is used to collect fees for the purchase of child pornography from numerous linked websites. The account number changes frequently as it is identified by law enforcement or by the e-gold operation, and the operators of the websites simply open new e-gold accounts to proceed with their activities.

**e-gold account 4181605  
(lolitalist.info)**

26. On February 22, 2007 SA Cordero, operating in an undercover capacity, signed onto the internet and typed [www.lolitalist.info](http://www.lolitalist.info) into the Universal Resource Locator (“URL”) address line. SA Cordero was directed to a web page which displayed the following:

"Welcome to "LOLITA LIST"  
This is link pages only. Only direct links.  
Following sites does not contain illegal or pedo pictures.  
They contain art pictures only.

". . . If you fight against child porno you must love this link pages, because here you can find many sites that you can abuse."

**So please, if you are a pedo fighter use these links like a reference materials.**

27. Based upon the experience of SA Cordero and other agents within the FBI's Innocent Images Unit, it was determined that this website was designed as a "Personal Portal" to access a variety of other web sites. A Personal Portal is a site on the World Wide Web that typically provides personalized capabilities to its visitors, providing a pathway to other content. It is designed to use distributed applications, different numbers and types of middleware and hardware to provide services from a number of different sources. In addition, business portals are designed to share collaboration in workplaces. A further business-driven requirement of portals is that the content be able to work on multiple platforms such as personal computers, personal digital assistants (PDAs), and cell phones.

28. After activating the "ENTER" hyperlink, SA Cordero was directed to web address <http://lolalist.info/index1.html?enter=ENTER>". The banner of this web page stated the following:

THE BEST UNDERGROUND PAYSITES ALL OVER THE NET  
LOLALIST.INFO  
SITES OVERVIEW PRICES & JOIN WHAT IS E-GOLD?

Under the header "LOLALIST.INFO" were the Visa, MasterCard, American Express, Discover, e-gold and Paypal logos indicating that memberships could be purchased via these methods to the advertised websites. A warning statement was then displayed which indicated that the "Cards-1" (described below) payment method was temporarily off-line and to "CLICK HERE FOR MORE INFO." The web page then displayed a banner listing "PAGE #01" through "PAGE

#12", each equipped with a hyperlink. SA Cordero accessed each of these twelve pages by activating the hyperlinks and reviewed 199 preview page thumbnail images which included the name and description of the "Lolitas Sites" which were available for membership purchases. SA Cordero determined that all 199 thumbnails contained images of child pornography and/or child erotica.

29. SA Cordero then activated the "CLICK HERE FOR MORE INFO" hyperlink located under the above-mentioned warning statement and was redirected to a web address identified as <http://pay.bestquickbuy.com/portal/prices.php>. This web page was divided into nineteen (19) text tables representing nine (9) unique web sites which contain, advertise and offer memberships to content that is child pornography. The tables listed 199 various "Plans" that were available for purchase, the "Site Title", the "Status" and the E-Gold price with a "Buy Now" hyper-link. The table also contained the credit card price, represented as "Cards-1" and "Cards-2" and a "Buy Now" hyper-link. SA Cordero activated the E-Gold "Buy Now" hyperlink for web site title "BD MAGAZINE issue #01" and was redirected to URL <http://pay.bestquickbuy.com/portal/payform.php?mp=BD-basic001>. This web page described in detail how to purchase this membership utilizing e-gold. The potential customer was instructed to log into their e-gold account, click "Spend," type the e-gold account number "4018318" in the memo field or go directly to account "4018318" by typing in the URL address line <http://4018318.e-gold.com/>. SA Cordero randomly activated the "E-Gold Buy Now" hyperlink of 25 of the above referenced "Plans" and determined that the e-gold account listed for payment for all of the sites was 4018318. Analysis of account 4018318 shows that funds in this account were received from individuals for the purchase of child pornography, and that funds were then

either transferred to other e-gold accounts controlled by the owner of account 4018318 or exchanged out for cash.

30. As of April 23, 2007, the www.lolalist.info child pornography site had stopped using e-gold account number 4018318 (in the account name of ONLYBEST and individual name of Diogo Ferreira) and had begun using account number 4181605 (in the account name of BEST+ and individual name of Andy Woren) in exactly the same manner.

**Access Device Fraud (Credit Card Fraud and Identity Theft)**

31. During the month of December 2003, the USSS became aware of the extent to which e-gold was being used to fund criminal transactions in its investigation of Shadowcrew, an international criminal organization of approximately 4,000 members that promoted and facilitated a wide variety of criminal activities including, among others, electronic theft of personal identifying information, credit card and debit card fraud, and the production and sale of false identification documents. During the investigation, the USSS monitored several websites dedicated to the promotion of criminal activities listed above, including but not limited to; www.shadowcrew.com, www.carderplanet.com, and www.stealthdivision.biz. These websites operated as bulletin boards that allowed criminals around the world to meet virtually and advertise and sell their goods and services electronically. Nineteen members of the Shadowcrew criminal enterprise were indicted in October 2004 for, among other things, conspiracy to provide stolen credit and bank card numbers and identity documents through the Shadowcrew website in violation of 18 U.S.C. §§ 371, 1028, and 1029.

32. The USSS investigation has also revealed that, when criminals use e-gold to buy and sell stolen credit card numbers and other contraband, they will often make a notation

indicating the purpose of the sale (*i.e.*, for “IDs”), which notation is input into the “memo” section of the e-gold transfer web page and is apparent to the recipient of the e-gold transfer. This information is also recorded by e-gold in its transaction logs. On or about November 3, 2005, I reviewed the subpoena returns from GSR provided to the USSS in early 2005 for six e-gold accounts of Shadowcrew members. In the “memo” section of the transaction log, a sampling of the notations made for payments included: “For 3 IDs,” “for dumps,” “10 classics,” “fame’s dumps,” “10 M/C,” “one plat and six classics,” “20 vclassics,” “18 ssns,” “10 AZ IDs,” “4 v classics,” “for cvv2s,” and “for 150 classics.” The terms used in these notations are all vernaculars used by criminals in reference to credit card or identification document fraud.

33. The term “**IDs**” refers to fraudulent identification documents (*i.e.*, fake IDs); “**dump**” refers to stolen credit card numbers; “**classics**” refers to a type of credit card (“**vclassics**” refers to visa classics); “**SSNs**” refers to social security numbers; “**Plat**” refers to platinum credit cards; and “**cvv2**” refers to the 3-digit credit verification value on the back of most credit cards, which helps merchants ensure that the customer actually has the card and that the number is valid.

34. Members of carding websites are known to other members by their chosen screen name or nickname (“**nic**”). Individuals often are known by and conduct their criminal business under more than one **nic**. The carding websites also operate through a hierarchical framework, which includes administrators (overseers of the site), moderators (of the particular forums), reviewers, vendors, and buyers. Vendors, in particular, advertise and sell products and services to members of the criminal organizations via the associated web sites after the product or service has received a favorable written review from a reviewer. Once a reviewer has been designated, a

prospective vendor is required to ship multiple samples of the product or provide access to the service to facilitate completion of the review. This contact between the prospective vendor and the reviewer is usually made through a private e-mail message or through a public post in a forum on the relevant web site.

35. Websites that facilitate the sale of, among other contraband, stolen credit card numbers, compromised identities, and false identifications are typically referred to as “carding websites.” Several carding websites that resemble the (now defunct) Shadowcrew website in nature, form, and purpose include:

a. Mazafaka: The website [www.mazafaka.ru](http://www.mazafaka.ru) was originally founded in 2001 as an online coordination point for thousands of Russian-speaking hackers. In June 2004, a section of the website was spun off in order to create a separate website, which has since operated under the domain names [www.makafaka.cc](http://www.makafaka.cc), [www.carding.ru](http://www.carding.ru), and [www.mazafaka.info](http://www.mazafaka.info), entirely dedicated to online financial crime. As of February 2007, the [Mazafaka.info](http://www.mazafaka.info) site has more than 9,200 registered user accounts. While much of the content at [Makafaka.info](http://www.makafaka.info) is in Russian, there is a part of site that operates in English. Several forums for the English-language section reveal carding activity, including “Real carding, hardware, dumps, plastics,” “ID, passports, documents,” “Programming in carding,” and “Stuff carding.”

b. CarderPlanet: The website [www.carderplanet.com](http://www.carderplanet.com) (also [www.carderplanet.net](http://www.carderplanet.net) and [www.carderplanet.cc](http://www.carderplanet.cc)) was founded in May 2001. By June 2004 the site had attracted more than 6,900 registered users. Although most of the traffic on the website was in Russian, the site had a vigorous English-language section which featured threaded discussions on carding activity, including “Carders Work” (discussion on selling stolen credit card information and purchasing

merchandise online with such information), “IDs” (discussion on creating and selling counterfeit identification documents, including passports), “Anonymity & Security” (discussion on achieving anonymity with use of proxies and security on the Internet), and “Programming. Hacking. Soft.” (providing information on programming and hacking services for carders and available software for these services). Two of the administrators of the Carderplanet criminal organization have been arrested and/or convicted of financial and wire fraud, including Dmitrii Ivanovich Golubov (a/k/a “Script”) (arrested in the Ukraine in July 2005 for financial fraud), and Roman Vega (a/k/a Boa) (pleaded guilty in 2006 to twenty counts of federal wire fraud). In addition, several United States-based senior members of CarderPlanet were indicted federally in 2004 in connection the USSS takedown of the Shadowcrew criminal organization.

36. The following paragraphs identify e-gold accounts used by vendors on carding websites:

a. “Maksik”: “Maksik” is a known vendor of stolen credit card information, stolen financial accounts, and fraudulent Ukrainian passports on the Shadowcrew, Mazafaka, and Carderplanet carding websites and accepts payment for this contraband in e-gold. A search and review of the e-gold database revealed account number **1751848**, with the account name “Maksik’s Job,” and contact email addresses of info@maksikjob.com and maksik@maksik.biz. Several memo fields in the transaction record for e-gold account number 1751848 indicate carding activity, including, for example, “1-27 order amex” (*i.e.*, an order for a stolen American Express credit card number), “Happy H4xOr Dumps” (*i.e.*, stolen credit card information), “For 20 classics” (*i.e.*, a type of credit card). A search and review of the e-gold database also revealed e-gold account number 3399565, with the account name “Maksik’s account,” and containing a

contact email address of Maksik@maksik.cc. A review of this account also shows many transactions with other e-gold accounts controlled by known carders, including e-gold account number 2567183 (controlled by “Lord kaisersose” – a known vendor of stolen credit card information), and e-gold account number 2874688 (controlled by “u26” – a provider of credit card pre-authorization services to vendors). There are several transfers of e-gold out of this account using an exchange service to exchange the e-gold into national currency. As of March 13, 2007, the remaining balance in account 1751848 is 10.505964 grams (\$7,000).

b. “Segvec”: “Segvec” is a vendor of stolen financial information on the carding website Makafaka and accepts payment for his contraband in e-gold. A search and review of the e-gold database revealed number 2464856 – which has as its contact name “segvec.” According to information related to me from agents of New Scotland Yard’s National Terrorist Financial Investigation Unit regarding email communications they had with Douglas Jackson in April 2007, Douglas Jackson was aware that “segvec” was a Ukrainian carder. In addition, according to information related to me from agents of the United States Postal Inspection Service regarding communications they had with Douglas Jackson, in November 2006, Jackson froze approximately 1,491 accounts belonging to individuals engaged in credit card fraud, one of which was “segvec”’s e-gold account 2464856. As the following paragraphs describe, “segvec” hijacked at least two other e-gold accounts, numbers 1115523 and 3584940, which he used to funnel the proceeds of his carding activities.

c. An analysis of “segvec”’s account number 2464856 yielded the following results: The account was created in October 2005. There were 93 transfers into the account with a value of 1524.80951 grams (\$845,545.60). 20 of the 90 transactions, which total 726.623113 grams

(\$410,750.00) and occur between February and May 2006, are transfer of funds from account 1751848, "Maksik's Job" (see paragraph 36(a) in this Affidavit). There were 45 transactions involving the transfer of funds out of the account with a value of 1383.998616 grams (\$817,895.12). On September 13, 2006, a transfer of 509.85724 (\$300,000) was made into account 1115523. The memo field of this transaction reads "repayment of debt."

d. Analysis of e-gold account 1115523 revealed that the account was created in November 2003 under the name of "Sujata Laxmikant More" and that there were 225 transfers into the account totaling 540.37615 grams (\$317,853.37) and 152 transfers out of the account totaling 540.353 grams (\$317,840.91). Analysis also revealed that two minutes after the account received 509.85724 grams (\$300,000) from the "segvec" account (number 2464856), 508.157716 grams (\$299,000.00) was transferred out into account 3584940. The IP address used to make the 508.157716 (\$299,000) transfer to account 3584940 is consistent with other IP addresses used in transactions in account 2464856 and not with IP addresses otherwise used in account 1115523. As a result, it appears that "segvec" hacked into account 1115523 and used it as a means to obfuscate the source and ownership of funds.

e. An analysis of e-gold account 584940 (in the name of Harry Michaels, 208 29th St NW, Bradenton, Florida 34205-3409, michaelpropertyinvestments@yahoo.com, (941) 747-6225) revealed that there was one transfer into the account on September 13, 2006 from e-gold account 1115523 in the amount of 508.157716 grams (\$299,000). The memo field for this transaction states "for down payment of offshore property #8972-2006." There are no other transactions into the account or out of the account. This account was limited by the e-gold operation on September 15, 2006 for "suspected password stealer," showing that the e-gold

operation believed this account had been a victim of account hijacking (*i.e.*, someone had stolen the password for account 3584940 and had taken it over). On April 13, 2007, I spoke with the individual at the address and phone number listed above as contact information for e-gold account 3584940. The individual identified himself as Harry Michael Weindorf and stated that he did not own a computer and had never heard of e-gold. Given that the e-gold operation limited account 3584940 for “password stealer” and that the individual listed as the owner of the account denies ever opening the account, it is likely that “segvec” either stole Harry Weindorf’s information and opened an account in this name or took over an existing account by stealing the password from another user, in order to obfuscate the source and ownership of the funds involved in his criminal activity. As of March 14, 2007 the remaining balance in the account is 505.806965 grams (\$333,377.37).

### **Wire Fraud (Investment Scams)**

#### **Background on Pyramid Schemes**

37. E-GOLD has been a highly-favored method of payment by operators of investment scams, which generally refers to pyramids, ponzis, HYIPs (*i.e.*, high-yield investment programs) and other “get-rich-quick” schemes. During the course of this investigation, I consulted with an Economist at the Federal Trade Commission (FTC) who explained that a pyramid (or ponzi or HYIP) scheme is an organization in which the participants obtain their monetary benefits primarily from the recruitment of newer participants, rather than from the sale of goods and/or services to the general public. Because of this, the overwhelming majority of the participants cannot expect to make any money from their participation. A small minority of participants, namely those who participate at the very beginning, might make money. However,

because of the nature of the pyramid scheme, those who make any money must of necessity be only a small minority of all participants.

38. The FTC Economist further explained that growth of the system does not change the fact that the large majority of participants at any point in time will have lost money. An individual participant might go from having a net loss to a net profit as the system grows, but it must be true that the majority of participants will lose money. The system cannot grow indefinitely, if for no other reason than the fact that growth is limited by the finite human population of the earth. Long before this point is reached though, the number of people willing to pay to sign on as new participants will become fewer and fewer. At this point, no further growth is possible, and the scheme will collapse. When that happens, the majority of the participants will have lost money.

39. The FTC Economist further explained that these scams typically have one of several indicators or “markings,” including (i) the promise of abnormally high short-term returns on investments; (ii) the absence of any legitimate or reasonable business investment; and (iii), as described above, only a small minority of individuals can profit from the operation of the business.

40. According to Omar Dhanani, an individual convicted of access device fraud in the above-described Shadowcrew prosecution, who also used e-gold to participate in pyramid schemes, e-gold has been favored in this area particularly because of a user’s ability to operate accounts anonymously, and e-gold’s policy of making all transfers of e-gold irrevocable and not subject to reversal.

41. A search of the e-gold database revealed over 11, 000 e-gold accounts that have

been opened using the term “hyip” in either the account-owner’s name or e-mail address, or where “hyip” appears in the “memo” field of the transaction record.

#### Patterns of Investment Scams using e-gold

42. This investigation uncovered numerous promoters (or operators) of pyramid, HYIP, and other similar schemes, each of whom operated several different investment scams and laundered their proceeds through chains of interconnected e-gold accounts. Several patterns emerged with regard to the transaction activity within accounts operated by these promoters. First, the promoters would set up an e-gold account to which all investors would send deposits to the program. From this main account, the promoters would pay out three types of “returns”: (1) payouts to a majority of investors in amounts much smaller than the investors’ initial deposits in order that these investors would keep believing this was a worthwhile “investment”; (2) payouts to a select group of investors in amounts far exceeding their initial investment in order that these investors could continue to promote the scheme as actually paying out the “promised return”; and (3) transfers to e-gold accounts controlled by the same promoter in large amounts representing the profits of the scam (*i.e.*, the stealing of investors’ money).

43. The promoters of the large pyramid (or HYIP) schemes appeared to coordinate their activity informally by investing in, and thereby promoting, the other promoters’ programs. This informal coordination allows the promoters to ensure that they will become the select group of investors receiving the “promised return” from any given scam. Such investments in other large HYIP programs also enables promoters to mask their profits from the original scam by layering the scammed funds through many different e-gold accounts. Once filtered through several layers of transactions and accounts, HYIP promoters typically store their funds in a

holding account, waiting for the opportunity to exchange the funds into national currency.

44. Because most of the High Yield Investment Scams are promoted, operated, and maintained on the Internet, most of the communication among the operators and participants is conducted within on-line virtual discussion groups. Discussion groups are places for individuals to place a “post” on a web board for others to read and to reply to. [www.TalkGold.com](http://www.TalkGold.com), [www.HYIPdiscussion.com](http://www.HYIPdiscussion.com), and other discussion boards provide information outlining the programs that are currently operating and other pyramid schemes that have collapsed on themselves. Most of the individual posts to the boards are from those who invest in the pyramid schemes and those who operate and promote the illegal investment scams.

#### Pyramid Terms in “Memo” Fields

45. This investigation also revealed that e-gold accounts involved in the operation of pyramid schemes and HYIPs use certain terms in the memo fields of transaction records that identify a particular scheme in progress. Such terms include “%gains,” “refund,” “payout,” “units,” “loans,” “contracts,” and “compounding.” Use of these terms are indicative of deposits to, and payouts from, a pyramid scheme or HYIP.

#### Identified e-gold accounts operating pyramid schemes

##### **e-gold accounts 2636005, 2825136 and 2828872 (Legisi Holdings LLC)**

46. e-gold accounts 2636005, 2825136 and 2828872 are accounts purportedly owned by Greg McNight of Swartz Creek, Michigan in the name of Legisi Holdings, LLC. These accounts are used to operate the Legisi pyramid investment scheme, which has been operating since December 2005 via the internet website [www.legisi.com](http://www.legisi.com). This program describes itself as

“a private, members-only **High Yield Return-on-Loan** program. . . . Our members loan us funds, choose their repayment terms and enjoy the interest payments.” This scheme offers investors two programs in which to invest their money, including the “Standard Loan” which has a minimum investment of \$250 and no maximum. At the end of the four month term, investors are told they can withdraw their principle investment with 10% a month interest paid, or chose to leave their money in the system and continue to earn 10% a month. The second program offered is the “VIP Loan,” in which the minimum investment is \$10,000. The term of the investment is for one year, and at the end of the year, the investor can withdraw their money or leave it in the program and receive a 12.5% monthly return. Legisi also encourages investors to recruit others to invest in the programs by paying a 5% referral commission on all funds that are put into a new account. The operator of the scheme – Greg McKnight, according to the website – states on his website that investors who may be seeking to refer other investors should never use the terms “investment,” “Tax,” or “Guarantee.”

47. As of March 13, 2007, Legisi e-gold account 2636005 was the highest value e-gold account after the e-gold operation’s own accounts (e-gold, Ltd. and OmniPay accounts), containing approximately 1485.12508 grams (\$978,845.94) worth of e-gold. An analysis of account 2636005 was conducted and yielded the following results: The account was created in December 2005 and transactions can be seen up until March 12, 2007. Approximately 11,254.25814 grams (\$7,022,258.77) in funds in 1,556 transactions occurred into the account with notations in the memo field such as: “Deposit to www.legisireserve.com User ChuckieM” and “Withdraw to Robert Williams from Legisi.com.” The transaction history shows that, while there were some payments out to investors (generally in the tens to hundreds of dollars), the vast

majority of funds were simply taken out of the account for use by McKnight. Approximately 5440.90856 grams (\$3,443,852.80) was exchanged out for national currency through Omnipay or The Bullion Exchange. Another e-gold account, number 2828872 in the name of “LIDO Consulting LLC” and also controlled by McKnight, received 892.133009 grams (\$550,000) from account 2636005.

48. A second Legisi e-gold account, number 2825136 had a balance of 375.641569 grams (\$247,585.36) on March 13, 2007. Analysis of this account, also held in the name of Legisi Holdings LLC, was conducted and yielded the following results: Transactions in the account occur between September 2006 and March 2007. Approximately, 1,315 transactions occur involving the transfer of funds into the account with a value of 7498.626704 grams (\$4,699,786.63), and include notations in the memo field such as: “Deposit to VIP fund.” Most of the funds received into this account, amounting to approximately 5365.237044 grams (\$3,385,048.00), were transferred to Legisi’s account 2636005.

49. A third Legisi e-gold account, number 2828872 received approximately 3724.00066 grams (\$2,499,806.00) worth of e-gold from accounts 2636005 and 2825136, both of which were used to receive investor deposits. Analysis of account 2828872 showed: 116 transactions occur into the account with a total weight of 4866.42213 (\$3,237,669.14), four of which come from account number 2636005 totaling 3348.77982 grams (\$2,240,805.00). Three of the 116 transactions come into the account from e-gold account 2825136 with a weight of 375.22084 grams (\$259,001.00). There were approximately 149 transactions out of the account with a total weight of 2208.24154 (\$1,374,323.44). The smaller transactions out of the account appear to be payouts to keep investors satisfied, while the larger withdraws are to OmniPay for

exchange. Shortly before its value was seized, e-gold account 2828872 was one of the greatest valued e-gold accounts, containing approximately 2657.54163 grams (\$1,804,205.01) worth of e-gold.

**e-gold account 3921533  
(Miguel Jimenez)**

50. e-gold account 3921533 is an account opened under the name of Miguel Jimenez with an address in Santo Domingo, Dominican Republic. As of March 13, 2007, this account contained approximately 1409.27505 grams (\$928,853) in e-gold comprised of wire fraud proceeds generated in other e-gold accounts. Approximately 1491.160565 grams (\$910,500.00) in e-gold was received by account 3921533 during the period of December 26, 2006 through January 7, 2007 from e-gold account number 2291364, an account held in the name of Financial Freedom with addresses listed in Luxembourg and Germany. Account number 2291364 appears to be a feeder account, receiving approximately 1597.315585 grams (\$953,650.00) worth of e-gold from five other e-gold accounts, most of which generated funds through pyramid investment schemes.

51. Approximately 435.523465 grams (\$244,650) worth of e-gold was generated by the "KUM" pyramid scheme that operated via the internet at [www.kum-holdings.com](http://www.kum-holdings.com). According to blog entries on [www.hywd.info](http://www.hywd.info) (High Yield Weekly Digest), this scheme offered an investment program that required a minimum investment (although investment pooling programs were also available to allow smaller investors to participate) of \$5,000 and promised 10% weekly returns on the investment.

52. A search and review of the e-gold database revealed e-gold account number

1999226 with the e-mail address of kum\_ventures\_inc@safe-mail.net listed in the account profile information. Additionally, notations in the memo fields of the transaction history such as “Memo: Michais@safe-mail.net-KUM-10%Spring-Program,” and “KUM payout (new rules - wait for newsletter)” reflect the fact that this e-gold account is the operating account for the KUM pyramid scheme. The account reflects activity starting in July 2005, and the fact that the scheme stopped paying its investors in January 2006.

53. e-gold account 1999226 received approximately 24180.97013 grams (\$11,958,076.74) in fraud proceeds deposited by individuals through approximately 18,404 separate transactions investing in the KUM pyramid scheme. Approximately 488.583179 grams (\$312,000) in fraud proceeds was forwarded from account 1999226 to e-gold account number 2460234 ( an account held in the name of Marcos Diaz, using an address in Stockholm, Sweden that is actually the address of a hotel) during the period of October 2005 through January 2006 in 22 transactions, 260.666956 grams (\$160,000.00) of which was then transferred to e-gold account 2291364 during January 2007 in 4 transactions. Additionally, approximately 174.856905 grams (\$84,650) in fraud proceeds was forwarded to e-gold account number 2291364 during the period of August 2005 through January 2006 in 41 transactions.

54. Approximately 1161.677851 grams (\$709,000) of e-gold contained in e-gold account number 3921533 was received via e-gold account number 2291364, but originated in three additional accounts – 2781422 (account name “DG”), 2792795 (account name “Donlan”), and 354057 (account name “Roni”). Account 2792795 is an account operating under a stolen identity (belonging to an elderly and infirm man in Florida who never created an e-gold account), and accounts 2781422 and 354057 are associated with a company that establishes offshore

corporate identities. Account 2781422 received \$200,000 from e-gold account 1178509, an account that has received over \$400,000 from the KUM scheme. Otherwise, no specific link to pyramid scheme activity has been identified in these accounts. Nonetheless, any non-criminal funds in account 3921533 serve to obfuscate the nature of the criminal funds in the account and thereby facilitate the laundering of those funds.

**e-gold accounts 1359767 and 1424543  
(Nawaaz Meerun)**

55. e-gold account 1359767, with the account name "NM2," and 1424543, with the account name "NM3," are accounts that are held in the name of Nawaaz Meerun with an address in Port-Louis, Mauritius. These accounts are fed by other e-gold accounts that receive funds from illegal pyramid schemes.

56. During the period of May 2004 through October 2006, e-gold account 1359767 received approximately 2833.517727 grams (\$1,285,288.50) in 210 transactions. Analysis of the source of those funds revealed that 169 of those transactions, worth approximately 1045.196 grams (\$462,552) originated from approximately 23 different accounts that were receiving funds from pyramid schemes, as demonstrated by notations in the memo fields and the pattern of incoming and outgoing transactions in those account histories. For example, analysis of the memo fields revealed numerous instances of notations indicating the operation of a pyramid scheme such as "upgrade", "withdraw", "units", "reward", "steps", "tranche," among others. Review of these accounts suggests not that Nawaaz Meerun was operating his own scheme, but that he was receiving a portion of the proceeds of other schemes. An example of the type of accounts from which this person received funds is the illegal pyramid scheme known as

Inestec.com. Participants of the Inestec scam had to leave their money in the scam for 120 days and had a rate of return from 1.6%-2.2% daily depending on the amount of the investment. Transactions out of this account were either for exchange or to other e-gold accounts controlled by the owner of this account. As of March 13, 2007, this account contained approximately 1235.39453 grams (\$814,249) worth of e-gold, of which 691.233599 grams (\$442,320.38) is criminal proceeds.

57. During the period of June 2004 through May 2006, e-gold account 1424543 received approximately 2800.282472 grams (\$1,369,746.58) worth of e-gold in 129 transactions. Analysis of the source of those funds revealed that 103 of the transactions, worth approximately 1823.234 grams (\$902,951) originated in approximately 30 different accounts that were operating pyramid schemes, as indicated by analysis of notations in the memo fields and the pattern of incoming and outgoing transactions. An example of the type of accounts from which this account received funds is the illegal pyramid scheme Freeland Ops, described below. Transactions out of this account were either for exchange or to other e-gold accounts controlled by the owner of this account. As of March 13, 2007, the account contained approximately 1073.2341 grams (\$707,369) worth of e-gold.

**e-gold accounts 3830833 and 2094836  
(IFF "ULWES")**

58. e-gold accounts 3830833 and 2094836 are accounts that contain the proceeds of an illegal pyramid scheme operating via internet website [www.ulwes.com](http://www.ulwes.com), a Russian language site. e-gold account 3830833 named IFF "ULWES," and held in the name of Waldemar Ulrich from Huerth, Germany, contained 495.965787 grams (\$326,891) worth of e-gold as of March 13,

2007.

59. The ULWES scheme was located on the internet through an internet search using the Google search engine for the term IFF ULWES. Using Google's translation function, it appeared that the home page of the site describes a "Dinner Financial Fund," and explains that it "began operations in August 2006 in Germany as a trust fund, putting its task through the financial pilotproekt attract investment for large and small investors, to be used at the international monetary exchange FOREX in New York and a guaranteed increase in the day 1.8% to investors dividends . . ." The registration page for this program indicates that new investors will be assigned a sponsor, which is a hallmark of pyramid schemes.

60. The program is described in more detail on another website created by a purported participant within the program, [intwayplus.com/ulwes.html](http://intwayplus.com/ulwes.html). This promoter (seeking to be the sponsor of new entrants below him/her) describes a program where you can earn 375 euro in 1 year with only an investment of 5 euro. The promoter instructs investors not to invest more than they can lose because investing is risky. The website delineates the sponsor return pyramid: For the first tier below you, you will receive 10% of the investment of the new customer beneath you. Similarly, you will receive 5% for the second tier, 4% for the third, 3% for the fourth, 2% for the fifth, and 1% for the sixth. Calculating the referral commissions that would be paid to one string of sponsors shows that 25% of the 6th tier investors initial investment will go to pay the higher sponsors in the pyramid.

61. Analysis of e-gold account 3830833 yielded the following results: Activity began in the account in November 2006. There have been approximately 8,013 transactions into the account totaling 1144.484009 grams (\$561,504), which is consistent with pyramid scheme

deposits (small consistent amounts and names/non-e-gold account numbers in the memo field). There have been only 38 transactions out of the account totaling 642.549511 grams (\$311,852). Most of this amount (584.39869 grams (\$283,473) in 26 transactions) went to e-gold account number 2094836. No funds have left the account be invested in the FOREX monetary exchange in New York as advertised in the program.

62. As of March 13, 2007, e-gold account 2094836 contained 47.111742 grams (\$31,051) in illegal pyramid scheme proceeds. This account is held in the name of Sven Schalbe with an address listed as being in Hohwald, Sachsen. The account was created on May 7, 2005, and exhibits a very large number of transactions consistent with the operation of a pyramid scheme similar to that described in the paragraph above (numerous transactions of small amounts and memo fields with pyramid program names, e-mail addresses of investors, and non-e-gold account numbers). Specifically, there were 5,784 transactions into the account totaling 1,449.807123 grams (\$730,820.00), and numerous payments out that can be characterized as lulling pay outs to investors.

**e-gold account 1922141  
(Sime Securities)**

63. e-gold account 1922141, with the account name "B-Connected Technology Inc" and purportedly owned by Nor Hisham Hashim from Malaysia, using e-mail address gtv26@safe-mail.net, is an account that contains the proceeds of an illegal pyramid scheme called Sime Securities. Beginning in 2004, Sime Securities operated via the internet at <http://simesecurities.net> and offered various investment programs offering returns of 1.5%-2.5% daily, 15%-25% weekly, or 140%-280% monthly.

64. A search and review of the e-gold database revealed e-gold account 805405, an account named “E-Gold” and held in the name of Maria in Singapore. Individuals who wanted to invest in the Sime Securities programs transferred funds into this e-gold account number. One of the email addresses listed in the account – gtv26@safe-mail.net – is the same as the email address used in account 1922141. Review of the database also identified e-gold account 1922125 as another account in the name of Nor Hisham Hashim that received payments from scheme investors.

65. During the period of June 2003 and August 2005, e-gold account 805405 received 1607.1488 grams of gold (\$694,904) from individual investors in the Sime Securities pyramid scheme. The memo fields in the transaction history for this account include notations such as: “Depositing \$1,001 to 805405 SIME” and “Pay \$2,500.00 to Sime Securities acct# 805405.” As is typical in illegal pyramid schemes, an analysis of this account’s activity indicates that of the investor funds that came in, very little went back to investors. Rather, 954.047016 grams (\$412,280) were transferred to another account, e-gold account 1922141, operating the same Sime Securities scheme, and over 209.289495 grams (\$90,454) were transferred to what appears to be e-gold accounts for the personal use of the operators of the scheme – specifically, e-gold accounts 1922221 and 1922227, both in the name of Nor Hisham Hashim.

66. During the period of March 2005 and October 2005, e-gold account 1922125 received funds in the amount of 599.880305 grams (\$263,046) from individual investors in the Sime Securities pyramid scheme. Except for several large transactions coming from e-gold account 805405, the memo fields in the transaction history for this account include notations such as “Deposit to SIME Securities Ltd. User Maaka.” The majority of funds going out are

transferred to other e-gold accounts belonging to the operators of the Sime Securities scheme, including accounts 1922221, 1922227, 1922191, and 45.423575 grams (\$20,000) to 1922141.

67. From June 11, 2005 through August 28, 2005, approximately 954.047016 grams (\$432,280.00) were transferred from e-gold account 805405 to e-gold account 1922141. As of March 13, 2007, the weight of the gold in account 1922141 was 777.775817 grams (\$512,632).

**e-gold accounts 3931825, 3814228, 3751783, 3781244,  
3711356, 3599523, 3729709, and 3686876  
(World Investment Group)**

68. e-gold accounts 3931825, 3814228, 3751783, 371244, 3711356, 3599523, 3729709, and 3686876 contain proceeds of an illegal pyramid scheme known as World Investment Group (hereinafter “WIG”), which operated via the Internet at worldinvestment.us. WIG was purportedly founded in Boston in 1996 and offered various investment programs with rates of return up to 528% per year. A search and review of the e-gold database revealed one primary e-gold account for the receipt of illegal funds, and numerous additional e-gold accounts among which funds were transferred for the apparent purpose of obfuscating the source and ownership of the funds.

69. e-gold account 3583697 (hereinafter “main WIG e-gold account”) is the primary account into which payments by investors in the World Investment Group scheme made payments. From November 15, 2006 through December 3, 2006, in 1,969 transactions, approximately 6153.971057 grams (\$3,786,368.89) worth of e-gold was received by the account. The memo fields in the transaction history clearly indicate criminal activity, showing investments and some payouts: “Deposit to worldinvestment.us User f31061“; “Withdraw to yuxia686868 from worldinvestment.us.” Significantly, the vast majority of funds received are not returned to

investors, but funneled to other accounts operated by participants in the scheme. These other accounts are characterized by bogus account name and contact information, and many use e-mail addresses with 126.com or 163.com extensions. Such e-mail addresses are available on Chinese language websites that offer e-mail accounts similar to those offered by Hotmail or Yahoo. e-gold account 3583697, which received only fraud proceeds, is the source of all funds sought to be seized in the following accounts associated with the World Investment Group scheme.

70. As of March 13, 2007, e-gold account 3931825, held in the name of “Jrw,” using gibberish contact information, and a 126.com e-mail address, contained approximately 994.796625 grams (\$636,570.36) in proceeds of the scheme. e-gold funds with a weight of 996.491736 grams (\$634,266.99) were received from e-gold account 3794519 in the name of “hao” on December 29, 2006. Account 3794519 had received 1899.273747 grams of gold (\$1,200,000) between November 19, 2006 and December 2, 2006 from the main WIG e-gold account.

71. As of March 13, 2007, WIG-related account 3814228, held in the name of “huang ke,” using gibberish contact information and a 126.com email address, contained approximately 676.870523 grams of gold (\$446,125) in proceeds of the scheme. Approximately 347.606257 grams of gold (\$220,000) of this weight was received on November 23, 2006 from e-gold account 3585875 in the name of “HIK Group,” which had received 895.22602 grams of gold (\$530,000) from the main WIG e-gold account between October 17, 2006 and October 30, 2006. Another 404.102278 grams of gold (\$253,655.00) were received on December 27, 2006 from account 3584519 in the name of “hao,” which funds come out of the 1899.273747 grams of gold (\$1,200,000) that had been received from the main WIG e-gold account during the period of

November 19, 2006 and December 2, 2006. Finally, on January 31, 2007, 94.068807 grams of gold (\$61,521.00) were received directly from the main WIG e-gold account.

72. As of March 13, 2007, WIG-related e-gold account 3751783, held in the name of “bill” and using a 163.com email address, contained approximately 814.610965 grams of gold (\$536,910) in scheme proceeds. The funds in this account come entirely from the WIG scheme. Approximately 321.388398 grams of gold (\$200,000) were received on January 15, 2006 from e-gold account 3781244 in the name of “billy,” which had received 915.956934 grams of gold (\$570,000) on November 15, 2006 from e-gold account 3662361 in the name of “AOP Inc.” and using a 126.com email address. The funds from account 3662361 had originated from the main WIG e-gold account from transfers of approximately 3560.995531 grams of gold (\$2,171,000) during the period of October 11, 2006 through November 15, 2006. Additionally, account 3751783 received approximately 498.242791 grams of gold (\$312,747.00) from e-gold account 3794519 in the name of “hao” on December 27, 2006, which funds had originated in transfers of over 1899.273747 grams of gold (\$1,200,000.00) from the main WIG e-gold account during the period of November 19, 2006 through December 2, 2006.

73. As of March 13, 2007, WIG-related e-gold account 3781244, held in the name of “billy,” contained approximately 592.543491 grams of gold (\$390,545) in scheme proceeds. These funds are the remainder of the funds described in the paragraph above that were received from e-gold account 3662361 in the name of “AOP Inc.” and originated in the main WIG e-gold account.

74. As of March 13, 2007, WIG-related e-gold account 3711356, held in the name of “dou yi feng” and using a 126.com email address, contained approximately 559.834759 grams of

gold (\$368,987) in scheme proceeds. These funds were received on November 15, 2006 from e-gold account 3662361 in the name of “AOP Inc.,” and originated from transfers totaling 3560.995531 grams of gold (\$2,171,000) received in that account from the main WIG e-gold account during the period of October 11, 2006 through November 15, 2006.

75. As of March 13, 2007, WIG-related e-gold account 3599523, held in the name of “tiger” and using a tiger4life@126.com e-mail address, contained 560.27223 grams of gold (\$358,518.20) in scheme proceeds. These funds were received on November 15, 2006 from account 3662361 in the name of “AOP Inc.,” and originated from transfers totaling 3560.995531 (\$2,171,000) received in that account from the main WIG e-gold account during the period of October 11, 2006 through November 15, 2006.

76. As of March 13, 2007, WIG-related e-gold account 3729709, held in the name of “china” and using lc8881998@126.com and dd911dd@126.com email addresses, contained 338.203151 grams of gold (\$222,909.70) in scheme proceeds. These funds were received on October 30, 2006 in two transactions from WIG-related e-gold account 3686876 in the name of “HIK,” which had received 895.22602 grams of gold (\$530,000) from the main WIG e-gold account in October 2006. The account received no other funds.

77. As of March 13, 2007, WIG-related e-gold account 3686876, held in the name of “HIK,” and using a wuxiangwei2006@126.com email address, contained \$0. This amount reflects the remainder of the 895.22602 grams of gold (\$530,000) transferred from the main WIG e-gold account as described above.

**e-gold account 3297330  
(e-gold-invest.us)**

78. As of March 13, 2007, e-gold account 3297330 contained 387.660012 grams of gold (\$255,507) in proceeds of an illegal pyramid scheme operating under the name of e-gold-invest.us Account owner information listed in the profile for account 3297330 lists Goy Tian Seng in Sin, Singapore as the owner. An Internet search for e-gold-invest.us revealed that there was a website that has since been taken down and is no longer available to be viewed. The search did reveal two advertisements posted in different on-line investment forums promoting e-gold-invest-us, which were translated through Google's translation function. These descriptions indicate that the scheme claimed to invest customer funds and produce enormous returns. However, the e-gold account housing the funds shows that they were not actually investing in anything. Another internet forum website translated from Chinese outlines the promised returns as follows: \$200-\$499 investment returns 1.2% per day, \$500-\$999 investment returns 1.5% per day, and \$1,000-\$2,500 investment returns 1.7% per day.

79. Analysis of e-gold account 3297330 revealed the following: The account was "value-limited" by the e-gold operation with the notation of "ROA\_Scammer," showing that the e-gold operation believed the account to be involved in illegal activity. There were 397 transactions into the account totaling 510.410942 grams of gold (\$317,814), while only 124.34259 grams of gold (\$77,689) went out of the account in 1,199 transactions that were lulling pay outs to investors. All but four of the transactions into and out of the account have memo fields that clearly indicate that they are customer deposits or customer withdrawals from the program, for example "deposit to e-gold-invest.us user wuxiaokui." There are no deposits by anyone other than customers of the program. Therefore, there is no return on investment brought into the account. Deposits to the program began on October 1, 2006 and continued through

March 1, 2007. The funds remaining in the account are proceeds of the pyramid scheme.

**e-gold accounts 3900642, 3900899, 3414996,  
2739290, 2739330, 3744230, 3724455, 3777270,  
3910742, 3622583, 3034142, and 4055663  
(VIP Invest Club)**

80. e-gold accounts 3900642, 3900899, 3414996, 2739290, 2739330, 3744230, 3724455, 3777270, 3910742, 3622583, 3034142, and 4055663 contain proceeds of an illegal pyramid scheme known as VIP Invest Club (hereinafter “VIC”), which operates via the Internet at <http://www.vipinclub.net>. VIC advertises on its website that it is “the international investment corporation uniting the offshore companies, registered in Panama, Belize and Cyprus” and that “[w]e work more than 5 years.” The website also states that VIC began the Internet operation in order to “increase the invested capital that will allow increased received profits.” The VIC offers four investment plans: Plan 1 has a minimum investment amount of \$10, a maximum amount of \$99, and pays 1.1% daily; Plan 2 has a minimum investment amount of \$100, a maximum of \$499, and pays 1.3% daily; Plan 3 has a minimum investment amount of \$500, a maximum amount of \$999, and pays out 1.5% daily; Plan 4 has a minimum investment amount of \$1000, no maximum amount, and pays out 1.7% daily. Investors in VIC are allowed to withdraw money after 180 days. VIC also offers a referral program as follows: if an investor has between one and ten active referrals, the investor receives 5% of the total investments made from the referrals; if an investor has eleven or more referrals, the investor receives 10% of the total investments made from the referrals.

81. A search and review of the e-gold database revealed that VIC Invest Club used many e-gold accounts to collect customer deposits (including accounts numbers 3900899,

3910742, 3724455, 3777270, and 4055663), several e-gold accounts through which collection account proceeds would be funneled (including for example 3778107 and 2996818), one large account for making small customer pay outs (including 3900642), and many accounts to which proceeds of the scam would ultimately be funneled for exchange out of the system or to refund other VIC-related accounts, all for the apparent purpose of obfuscating the source and ownership of the funds.

82. Analysis of e-gold account 3900642 in the name of “VIC” yielded the following results: Activity began in the account in December 2006. There have been approximately 1,536 transactions into the account totaling 4648.971903 grams (\$3,018,580.64). All of the transactions into the account were from e-gold account number 3900899 in the name of “VIC”, discussed below, which received its funds from customer payments, or e-gold account numbers 2739290 in the name of “Eugene’s Account” and 2739330 in the name of “VIC” (both discussed below), through which proceeds of the illegal pyramid were funneled. As a result, the funds transferred into e-gold account 3900642 are entirely proceeds of the pyramid scheme. There were 57,065 transactions out of the account totaling 4612.68282 grams (\$2,995,865.54). Because of the number of transactions out of the account, e-gold account number 3900642 appears to be the account from which payouts are made to investors. As of March 13, 2007 the remaining balance in the account was 33.797915 grams (\$22,276.21).

83. Analysis of e-gold account number 3900899 yielded the following results: Activity began in the account in December 2006. There were 13,296 transactions into the account totaling 6445.02614 grams (\$4,181,487.85) and 1,669 transactions funds out of the account, most of which were to VIC account 3900642, totaling 4467.108021 grams

(\$2,900,520.00). All of the transactions into the account were payments from customers of the program as is indicated by the memo field in the transaction record, which references “Deposit to VIP Invest Club User#\_\_\_\_\_”. As of March 13, 2007 the remaining balance in the account was 117.146964 grams (\$77,211.56), all of which are proceeds of the illegal investment scam.

84. Analysis of account number 3778107 in the name of “NmTrsds” yielded the following results: Activity began November 2006. There were approximately 3,093 transactions into the account totaling 1237.966348 grams (\$785,494.42). All of the transactions into the account were payments from customers of the program as is indicated by the memo field in the transaction record, which references, for example, “Deposit to VIP Invest Club User#1028”. There were 489 transactions out of the account totaling of \$781,445.11. 108 of the 489 transactions out of the account were transferred to account 3778286, in the name of “Noname,” totaling 396.632236 grams (\$250,600.00). A review of account number 3778286 indicates that it appears to be a payout account for the VIP Investment Club scam. 35 of the 489 transactions out of the account were transferred to into account number 3414996, “eg account”(discussed below), totaling 143.041543 grams (\$90,520.00). As of March 13, 2007 account 3778107 has no remaining balance.

85. Analysis of e-gold account number 2996818 in the name of “VIP Invest Club” yielded the following results: Activity began March 2006 and ended in November 2006 when the account was limited by the e-gold operation for “False ID/Scammer,” showing that the e-gold operation believed the account to be involved in illegal activity. All of the transactions in the account either reference “Deposit to VIP Invest Club User#1039” in the memo field or are transferred to accounts associated with this scheme. There were 4,955 transactions into the

account totaling 1355.010208 grams (\$819,445.05), and 1,684 transactions out of the account totaling 1299.540846 grams (\$786,618.27). As of March 13, 2007 the account has no remaining balance.

86. Analysis of account number 3414996 in the name of “eg account” yielded the following results: There were 122 transactions into the account totaling 310.585833 grams (\$193,745.00). 83 of the 122 transactions were from account number 2996818 (discussed in the preceding paragraph) totaling 110.084283 grams (\$67,094.00). 35 of the 122 transactions were from account 3778107, “NmTrsds” (also discussed above), totaling 143.041543 grams (\$90,520.00). 4 of the 122 transactions are from account 3900899, VIC account 3900899, totaling 57.460007 grams (\$36,131.00). As a result, the only funds transferred in to this account were from the proceeds of the illegal investment scam. There were 15 transactions out of the account totaling 83.508297 grams (\$52,162.00). 14 of the 15 transactions were transfers to account number 2045761, operated by “G Card,” which allows for the exchange out to national currency on an anonymous prepaid card totaling 75.75113 grams (\$47,562.00). As of March 13, 2007 the remaining balance in the account was 216.22357 grams (\$142,512.95).

87. Analysis of e-gold account number 2739290 in the name of “Eugene’s Account” yielded the following results: Activity began April 2006 and ended in February 2007. There were 42 transactions into the account totaling 356.428379 grams (\$225,494.00). 22 of the 42 transactions were transfers from account number 2996818, “VIP Invest Club”(discussed above), totaling 81.574199 grams of gold (\$50,326.00). 12 of the 42 transactions were transfers from VIC account 3900899 totaling 245.087672 (\$156,200.00). 3 of the 42 transactions were transferred from account number 3778107, “NmTrsds”(discussed above), totaling 29.347468

grams of gold (\$18,700.00). As a result, 356.03342 grams of gold (\$225,226.00) transferred into this account were from the proceeds of the illegal investment scam. There were 32 transactions out of the account totaling 143.051606 grams of gold (\$89,390.66). 10 of the 32 transactions were transferred to VIC account 3900642, "VIC," totaling 124.636942 grams of gold (\$77,822.00). As of March 13, 2007 the remaining balance in the account was 212.942083 grams of gold (\$140,350).

88. Analysis of e-gold account number 2739330 in the name of "VIC" yielded the following results: Activity began in January 2006 and ended in February 2007. There were 41 transactions into the account totaling 288.232932 grams of gold (\$180,394.00). 26 of the 41 transactions involved transfers from account number 2996818, "VIP Invest Club" (discussed above), totaling 80.143927 (\$48,564.00). 8 of the 41 transactions were from VIC account 3900899 totaling 183.687983 grams of gold (\$117,080.00). As a result, 263.83191 grams of gold (\$165,644.00) transferred into this account were from the proceeds of the illegal investment scam. There were 86 transactions out of the account totaling 110.479636 grams of gold (\$68,075.00). As of March 13, 2007 the remaining balance in the account is 183.47636 grams of gold (\$120,929.27).

89. Analysis of e-gold account number 3744230 in the name of "V.Smelov's account" yielded the following results: Activity began in November 2006 and ended in February 2007. There were 19 transactions into the account totaling 209.981567 grams of gold (\$132,924.00). 17 of the 19 transactions were transferred from either account number 3778107, "NmTrsds", or VIC account 3900899, totaling 190.977491 grams of gold (\$121,024.00). As a result, 190.977491 grams of gold (\$121,024.00) transferred into this account were from the proceeds of

the illegal investment scam. As of March 13, 2007, the remaining balance in the account is 172.709009 grams of gold (\$113,832.51).

90. Analysis of e-gold account number 3724455 in the name of "Gromov's account" yielded the following results: Activity began in October 2006. There were 27 transactions into the account totaling 186.600262 grams of gold (\$117,960.00). All of the transactions into the account have "Payment from VIP Invest Club" in the memo field of the transaction record and come from other accounts used by the scheme, including for receipt of investor deposits. As a result, the only funds transferred in to this account were from the proceeds of the illegal investment scam. There were 8 transactions out of the account totaling 22.212081 grams of gold (\$13,975.35), most of which were for exchange. As of March 13, 2007 the remaining balance in the account is 163.992955 grams of gold (\$108,087.76).

91. Analysis of e-gold account number 4055663 in the name of "Svetlov's account" yielded the following results: Activity began and ended in February 2007. There were 8 transactions into the account totaling 147.638825 grams of gold (\$95,800.00). All of the transactions into the account have "Payment from VIP Invest Club" in the memo field of the transaction record and were from VIC account number 3900899. As a result, the only funds transferred in to this account were from the proceeds of the illegal investment scam. There were no transactions out of the account. The remaining balance in the account as of March 13, 2007 is 147.525037 grams of gold (\$97,233.75).

92. Analysis of e-gold account number 3777270 in the name of "Belov's acc" yielded the following results: Activity began in November 2006 and ended in January 2007. There were 14 transactions into the account totaling 144.459737 grams of gold (\$91,006.00). 13 of the 14

transactions have “Payment from VIP Invest Club” in the memo field of the transaction record and come from other accounts used by the scheme, including for receipt of investor deposits. The value of these transactions is 139.742002 grams of gold (\$88,056.00). The only other transaction into the account is from account number 2505155, “Andreeva's e gold,” totaling 4.717735 grams of gold (\$2,950.00). A review of account number 2505155 revealed that on November 13, 2006, 16.181323 grams of gold (\$10,102.00) were transferred into the account from number 2996818, “VIP Invest Club.” Therefore all of the transfers of funds into the account can be directly traced back to the proceeds of VIP Invest Club scam. There are no transactions out of the account. As of March 13, 2007 the value of the account is 144.148963 grams of gold (\$95,008.58).

93. Analysis of e-gold account number 3910742 in the name of VIC yielded the following results: Activity began in December 2006 and ended in March 2007. There were 3,898 transactions into the account totaling 1268.47875 grams of gold (\$825,492.20). All but two of the transactions reference “Deposit to VIP Invest Club User#[number]” in the memo fields, totaling 1265.132365 grams of gold (\$820,694.20), and indicate investor deposits. There were 653 transactions out of the account totaling 1141.430709 grams of gold (\$741,677.50). All but one of the transfers of funds out of the account go to account 3908137 and refer to “Payment from VIP Invest Club” in the memo line. As of March 13, 2007 the account has a weight balance of 123.609384 grams of gold (\$81,470.94), all of which are proceeds of the illegal investment scam.

94. Analysis of e-gold account number 3622583 in the name of “Happy” yielded the following results: Activity began in September 2006 and ended in December 2006. There were

60 transactions into the account occurred totaling 174.418794 grams of gold (\$108,580.00). 40 of the 60 transactions were from account number 2996818, "VIP Invest Club," totaling 77.547182 grams of gold (\$47,280.00). 20 of the 60 transactions were from account number 3778107, "NmTrsds," totaling 96.871612 grams of gold (\$61,300.00) (all but six reference "Payment from VIP Invest Club" in the memo field). Both of these accounts receive investor deposits. Therefore, all the funds transferred into the account can be directly traced back to proceeds of VIP Invest Club. As of March 13, 2007, the remaining balance in the account is 133.507 grams of gold (\$87,994.70).

95. Analysis of e-gold account number 3034142 in the name of "Fast and Profitable" yielded the following results: Activity began in March 2006 and ended in June 2006. There were 8 transactions into the account totaling 47.60672 grams of gold (\$29,537.53). 3 of the 8 transactions were transfers from account number 2996818, "VIP Invest Club," totaling 29.271459 grams of gold (\$18,066.00); 1 transfer of 14.219524 grams of gold (\$8,900) was from VIC account number 3900899; and 4 transfers were from two unknown accounts. As a result, e-gold account number contains at least 43.490983 grams of gold (\$26,966) in criminal proceeds. There are 5 transactions out of the account totaling .244409 grams of gold (\$151.06). As of March 13, 2007 the remaining balance in the account is 47.227413 grams of gold (\$31,127.32).

**e-gold account 3114779  
(Phoenix Surf)**

96. e-gold account number 3114779 contains proceeds of an illegal pyramid scheme known as Phoenix Surf, which operated via the Internet at <http://www.phoenixsurf.com>.

Phoenix Surf advertised itself on its website as a “paid-to-surf opportunity,” in which members could “purchase advertising packages in increments of \$8 until [the member] reached a maximum membership level of \$6,000.00.” The website further advertised that

“[w]e will then pay advertising package members up to a 15% commission of [their] advertising purchase to watch 15 website advertisements a day for only 15 seconds each. That 15% per day will be paid for 8 days totaling 120% total of your initial advertising purchase. (20% profit after only 8 days).”

97. All proceeds in e-gold account 3114779 were derived from e-gold account number 3113881 in the name of PhoenixSurf. An analysis of e-gold account number 3113881 revealed that there were 368 transactions totaling 303.668795 grams of gold (\$192,192.00) from April 21, 2006 through April 22, 2006. The memo field for each of these 368 transactions contained the language “1 Upgrade Unit @ \$8 per Upgrade Unit - Total: \$8” (or language with a different total amount depending on the number of units purchased). There were 12 transactions out of the account (all of which occurred on April 22, 2006), totaling 302.964924 grams of gold (\$191,945.50), to e-gold account number 3114779. There was no other activity in e-gold account 3114779 other than one payment to e-gold account 1700003 (in the name of Best Gold Card) for .088324 grams (\$55.90) on April 22, 2006. As of March 13, 2007 e-gold account number 3114779 contained 300.271888 grams (\$197,909.20) of illegal pyramid scheme proceeds.

98. The website [www.fairpatton.com](http://www.fairpatton.com) provides a forum for discussing different types of auto-surf programs and disclosing those which do not “adopt one simple RULE. ‘Pay your members, and Pay them on time’.” The site posted an announcement on or about May 24, 2006 in which it stated that “Phoenix Surf will close due to the events of the recent DDOS (*i.e.*, a distributed denial of service) attack. During this attack hundreds of thousands of dollars was

illegally stolen and transferred to an anonymous account, which at this stage has not been found.”

The investigation has revealed that pyramid schemes and other HYIPs often falsely claim to be victims of hacking incidents in which investors’ money is stolen in order to explain why the program did not pay out promised returns to investors.

**e-gold accounts - 1141305, 1142733,  
1146912, 1338640, 1426358 and 817253  
Freeland Ops**

99. e-gold account numbers 1141305, 1142733, 1146912, 1338640, 1426358 and 817253 contain proceeds of an illegal pyramid scheme known as Freeland Ops (hereinafter “the FLO operation”), which formerly operated via the Internet at [www.freelandopps.net](http://www.freelandopps.net). This website (and others associated with the FLO operation) are no longer available to be viewed. An Internet blog entry allegedly authored by a former victim of the FLO operation states that the scheme’s operators were David Trimmier and William Trimmier and that they operated the scam from Utah. The blog author also outlined the scheme’s promised returns to be: 1 Week Venture returns 110%, 2 Week Venture returns 125%, 3 Week Venture returns 145%, and 4 Week Venture returns 190%.

100. The FLO operation utilized over 50 e-gold accounts to receive funds from customers for their various programs, transfer the funds through controlled accounts, and disburse funds from dedicated disbursement accounts. Over 36 of the FLO operation’s e-gold accounts have been limited for “scammer,” “False ID,” or “IP, showing that the e-gold operation believed the accounts to be involved in illegal activity.

101. An Internet blog alleges that the FBI and the SEC are investigating the FLO operation, and states that they used e-gold accounts with the names FLO Credit 1, Freeland

Credit 1, FLO Credit 2, Freeland Credit 3, FLO Credit 4, Freeland Credit 4, and Credit 4 to operate the pyramid scheme.

102. Analysis of the FLO operation's e-gold accounts revealed that several accounts used the term "credit" in the account's name. These accounts were used to receive funds (*i.e.*, investments) from customers of the programs as indicated by a very large amount of deposits into the account, and memo fields that are consistent with deposits or investments in pyramids, such as "purchase freeland credits" and "Fund to FLO" with variations of account names, dates, and/or dollar amounts purchased. In these "credit" accounts, there were very few transactions out of the accounts, all of which were large amounts transferred to other e-gold accounts under the control of the scheme's operators.

103. Analysis of e-gold account number 1146863, with an account name of Freeland Credit 1 and contact information of Martin Granger, P.O. Box 2356, Townsville, QLD Australia, yielded the following results: This was one of the accounts used to receive funds for customers as indicated by the transaction history. Memo fields in the transaction record include notations such as "Deposit to FLO" and "Credit #2." Activity began in the account on approximately April 14, 2004 and ended on June 8, 2004, when the account was limited for "scamming," showing that the e-gold operation believed the account to be involved in illegal activity. There were 2,157 transactions into the account totaling 5440.90856 grams (\$997,392). There were only 74 large transactions out of the account, totaling 2558.245488 grams (\$996, 970), to other accounts associated with the FLO operation. As of March 13, 2007 the remaining balance in the account was \$0.

104. Analysis of e-gold account number 1146912, with an account name of Freeland

Credit 2 and contact information of Martin Granger, P.O. Box 2356, Townsville, QLD Australia, yielded the following results: This was one of the accounts used to receive funds for customers as indicated by the transaction history. Memo fields in the transaction record include notations such as “freelandopps” and “Funding FLO.” Activity began in the account on approximately April 15, 2004 and ended on July 30, 2004. There were 2,198 transactions into the account totaling 2224.837503 grams (\$865,214). There were only 70 large transactions out of the account, totaling 2190.284496 (\$851,567), to other accounts associated with the FLO operation. As of March 13, 2007 the remaining balance in the account was 31.101205 grams (\$20,499).

105. Analysis of e-gold account number 1141305, with an account name of Freeland Credit 3 and contact information of Martin Granger, P.O. Box 2356, Townsville, QLD Australia, yielded the following results: This was another account used to receive funds for customers as indicated by the transaction history. Memo fields in the transaction record include notations such as “Freeland Opps” and “FLO Deposit (username).” Activity began in the account on April 14, 2004 and ended on August 6, 2004. There were 638 transactions into the account totaling 637.873973 grams (\$249,354). There were only 22 large transactions out of the account, totaling 631.742299 grams (\$246,872), to other accounts associated with the FLO operation. As of March 13, 2007 the remaining balance in the account was 5.264171 (\$3,455).

106. Analysis of e-gold account number 1142733, with an account name of Freeland Credit 4 and contact information of Martin Granger, P.O. Box 2356, Townsville, QLD Australia, yielded the following results: This was another account used to receive funds for customers as indicated by the transaction history. Memo fields in the transaction record include notations such as “credit to freelandopps” and “FLO-Funding.” Activity began in the account on April 16, 2004

and ended on July 27, 2004. There were 2,473 transactions into the account totaling 3136.126476 grams (\$1,212,977). There were only 76 large transactions out of the account, totaling 3130.711928 grams (\$1,210,516), to other accounts associated with the FLO operation. As of March 13, 2007 the remaining balance in the account was 2.372152 grams (\$1,557).

107. In addition to the credit accounts, analysis of the FLO operation's e-gold accounts revealed that a second group – all falling within the 800000 range of account numbers – were used as pass-through accounts for the apparent purpose of obfuscating the source and ownership of the funds. All transfers into these accounts came from the credit accounts and all transactions out of these accounts went to the debit accounts, discussed below. For example, Freeland Credit 1 (e-gold account number 1146863) transferred large amounts to e-gold accounts 816024, 816144, 817176, and 817253; Freeland Credit 2 (e-gold account number 1146912) transferred large amounts to e-gold accounts 817352, 821135, 822445, 823552, and 826126; Freeland Credit 3 (e-gold account number 1141305) transferred large amounts to e-gold accounts 832152, 832351, 833338, 833578, and 834755; Freeland Credit 4 (e-gold account number 1142733) transferred large amounts to e-gold accounts 817352, 835603, 835688, 837297, and 840008.

108. Analysis of the FLO operation's e-gold accounts revealed that a third group were used for disbursement purposes. These accounts, which used "debit" or "dividend" in the account name, had a small number of large transfers into the accounts and a large number of smaller transfers out of the account. Each of these debit accounts, similar to the credit accounts listed above, have contact information of Martin Granger, P.O. Box 2356, Townsville, QLD, Australia. It is from these accounts that the operators of the FLO operation withdrew the original illegal funds. Examples of the disbursement accounts are e-gold account number 1135210 (in the

name of Freeland Debit 1), 1135334 (in the name of Freeland Debit 2), 1136605 (in the name of Freeland Debit 3), and 1136749 (in the name of Freeland Debit 4). Each of these accounts only received funds from (1) the pass-through accounts listed in the paragraph above or (2) other FLO debit accounts.

109. Analysis of e-gold account number 1338640, with an account name of New Millennium and contact information of David Trimmier, 3 Northridge Cove, Sandy, Utah, yielded the following results: The account was created on April 25, 2004. The following deposits occurred on the following sequential dates from accounts associated with the FLO operation:

- On April 25, 2004, approximately 12.67649 grams (\$4,998) was transferred from e-gold account number 1136749 (Freeland Debit 4)
- On April 26, 2004, approximately 2.508781 grams (\$1,000) was transferred from e-gold account number 1136605 (Freeland Debit 3)
- On April 27, 2004, approximately 14.8226894 grams (\$5,910) was transferred from e-gold account number 1135210 (Freeland Debit 1)
- On April 28, 2004, approximately 15.318818 grams (\$5,910) was transferred from e-gold account number 1135334 (Freeland Debit 2)
- On April 29, 2004, approximately 15.269345 grams (\$5,910) was transferred from e-gold account number 1136749 (Freeland Debit 4)
- On April 30, 2004, approximately 15.269345 grams (\$5,910) was transferred from e-gold account number 1136605 (Freeland Debit 3)
- On May 1, 2004, approximately 20.436636 grams (\$7,910) was transferred from e-gold account number 1135210 (Freeland Debit 1)
- On May 2, 2004, approximately 15.253581 grams (\$5,910) was transferred from e-gold account number 1135334 (Freeland Debit 2)
- On May 3, 2004, approximately 15.212355 grams (\$5,910) was transferred from e-gold account number 1136749 (Freeland Debit 4)
- On May 5, 2004, approximately 26.29156 grams (\$10,280) was transferred from e-gold account number 1135210 (Freeland Debit 1)

These funds, which total 153.0596004 grams (\$59,648) and can be directly traced back to

proceeds the FLO operation, remain in the account to date with only storage fees and gold price fluctuations affecting the total value. As of March 13, 2007 the remaining balance in the account was 148.783118 grams (\$98,063).

110. Analysis of e-gold account number 1426358, with an account name of Goldenbart and contact information of Bart Brennon 506 North Fremont, Fleming, Colorado, yielded the following results: Approximately 233.201716 grams (\$95,000) was deposited into the account from July 8, 2004 through July 9, 2004; 123.790087 grams (\$50,322) was transferred from e-gold account number 881756 (in the name of "credit 4"); 82.62512 grams (\$33,678) was transferred from account 879375 (in the name of "credit 2"); and 26.78651 grams (\$10,878) was transferred from account 1424563 (in the name of "credit 1"). Each of these three accounts received funds from customers of the FLO programs as indicated by a very large amount of deposits into the account, and memo fields including "purchase freeland credits," "fund to FLO," "funding freeland opps," and "funding FLO by \$US (amount)." These funds have remained stagnant from that date until the present with only storage fees and gold appreciation affecting value. An Internet search of the address listed on the account (506 North Fremont, Fleming, Colorado) is the location of a public school, which is a common practice for operators of pyramid schemes, in general, and operators of the FLO operation, in particular. As of March 13, 2007, the remaining balance in the account was 228.716396 grams (\$150,747).

111. Analysis of e-gold account number 817253, with an account name of Ambergold and contact information of Greg K Amber 436 North Cobb, Milledgville, Georgia, yielded the following results: Activity began in the account on February 8, 2004 and ended May 11, 2004: There were 20 deposits into the account totaling 295.462645 grams (\$117,674) from accounts

934576 (in the name of FLO Credit 1), 1136749 (in the name of Freeland Debit 4, discussed above), 1136605 (in the name of Freeland Debit 3, discussed above), 1135334 (in the name of Freeland Debit 2, discussed above) and 1146863 (in the name of Freeland Credit 1). This account only conducts transactions with other accounts associated with FLO. This account was limited on June 9, 2004 for “scammer,” showing that the e-gold operation believed the account to be involved in illegal activity. As of March 13, 2007 the remaining balance in the account was 49.731513 grams (\$32,778).

**e-gold account 2353188  
(ExpInvest International)**

112. e-gold account number 2353138 contains proceeds of an illegal pyramid scheme known as ExpInvest International, which operated via the Internet at <http://www.expinvestcontact.com> and <http://www.expinvest-international.com>. These websites have been taken down and replaced by a forum/blog intended to document ExpInvest International as a scam. ExpInvest International previously advertised that it had been in operation since May 2005 and promised 8% daily or 200% monthly on a minimum investment of \$10.

113. All proceeds in e-gold account 2353138 were derived from two e-gold accounts: 2065103 (in the name of ExpInvest International) and 2352466 (in the name of EXP Deposit Account). An analysis of e-gold account number 2353188 revealed that activity in the account began and ended on August 24, 2005. During this time, there were two deposits totaling 122.26 grams (\$53,400) from e-gold account number 2065103 and two deposits totaling 102.34 grams (\$44,700) from e-gold account number 2352466. As of March 13, 2007 e-gold account number

2353158 contained 137.025231 grams (\$90,313) of illegal pyramid scheme proceeds.

114. Both e-gold accounts 2065103 and 2352466 have been limited for “scammer,” showing that the e-gold operation believed the accounts to be involved in illegal activity. Both these accounts received deposits consistent with illegal pyramid schemes as indicated by the memo fields in the transaction records, most of which include notations such as “Expinvest.com,” “hyip,” “invest,” and other common HYIP terms. Although the perpetrator of the scheme made transfers out of the accounts with memo fields in the transaction record that include “refund,” many of these funds are then immediately transferred to a 1mdc account, discussed below, controlled by the perpetrator or transferred out of the e-gold system through an exchanger.

**e-gold account 2319629  
(E-Gold Daily Pro (EGDP))**

115. EGDP is an illegal pyramid scheme that operated via the Internet at [www.e-golddailypro.biz](http://www.e-golddailypro.biz). EGDP advertised on Internet forums/blogs that its profits were the result of investing customers’ money in foreign exchange markets (*i.e.*, markets that trade in currencies). EGDP offered two investment plans for their customers: “Daily plan one” had a minimum investment amount of \$20.00 and a maximum of \$2,499. This investment purported to pay a 1.1% daily return. “Daily plan two” had a minimum investment amount of \$2,500 and a maximum of \$10,000. This plan purported to have a daily return rate of 1.5%. The deposit had to remain in the account for a minimum of six months. If a customer withdrew the deposit before the six month period, the customer was assessed a 15% penalty. The minimum amount that could be withdrawn at any time was \$20.00.

116. EGDP used two e-gold accounts, 3985608 and 2319629, in its operations, both of which contain proceeds of its illegal pyramid scheme. An analysis of e-gold account 3985608 (in the name of EGDP) yielded the following results: The account was created in January 2007 and ended activity at the end of January 2007. There were 553 transactions into the account totaling 599.907393 grams (\$383,765.95). Each transaction into the account had a Spanish phrase in the memo field which translates to “Once it carried out the payment was created its Upgrade.” There are no transactions out of the account. In January 2007, the account was limited by the e-gold operation for “False ID,” showing that the e-gold operation believed the accounts to be involved in illegal activity. As of March 13, 2007, e-gold account number 3985608 contained 598.531006 grams (\$394,492)

117. An analysis of e-gold account 2319629 (in the name of EGDP) yielded the following results: Activity began in the account in September 2006. There were a total of 884 transactions in the account totaling 412.526319 grams (\$315,111.30). There were 660 transactions into the account totaling 349.815661 grams (\$215,747.70). Most of the transactions make a reference to the Spanish phrase quoted above that translated means “Once it carried out the payment was created its Upgrade.” There were 224 transactions out of the account totaling 162.710658 grams (\$99,363.60), which appear to be small customer payouts. On January 12, 2007, the account was limited by the e-gold operation for “False ID,” showing that the e-gold operation believed the accounts to be involved in illegal activity. As of March 13, 2007, e-gold account number 2319629 contained 192.363881 grams (\$126,787).

**e-gold accounts 808080, 808081, and 808082  
(1mdc)**

118. “1mdc” operates via the Internet at [www.1mdc.com](http://www.1mdc.com) and advertises itself as a “digital gold currency” that is backed by e-gold rather than gold bullion. The website states:

“Whereas the reserve of most [digital gold currencies] is gold bars, the reserve of 1mdc is actually e-gold grams. A 1mdc gram is just an e-gold gram, stored for you, in 1mdc’s e-gold accounts. You can swap between the two any time.”

In other words, 1mdc is “simply e-gold moved to a collective e-gold account.”

119. The 1mdc website provides no contact information, although the investigation has revealed that 1mdc operates via a software developed by Interesting Software, Ltd., which is located in 102 Gillwell Offices, The Valley, Anguilla, BWI. The founder of the software is J.P. May.

120. In order to open an account, 1mdc requires an individual only to provide an e-gold account number, initials (maximum of five), a password, a PIN, and an email address. 1mdc also advertises on its website that: (1) it is “[c]ompletely and totally offshore,” (2) it offers an “[i]ngenious PIN PAD” to “boost security” and “eliminate accidental spend disasters,” and (3) “there are NO storage fees at 1mdc ... [a]nd most users pay NO spend fees!”. As such, it appears that 1mdc offers a more anonymous, private, secure, cost-effective payment system in comparison to other digital currency systems, in particular, to the e-gold operation.

121. After customers have created a 1mdc account, in order to obtain 1mdcGrams, customers can either: (1) exchange e-gold into 1mdcGrams by transferring e-gold from their e-gold account to their 1mdc account, or (2) similar to the process for exchanging national currency into e-gold, use one of several digital currency exchangers listed on the 1mdc website to

exchange national currency into 1mdcGrams, for example by wire transfer, cash deposit to a bank, credit card or other payment methods.

122. Conversely, in order to sell 1mdcGrams, customers can either exchange their 1mdcGrams into e-gold or use an exchanger to exchange the grams into national currency.

123. As stated on the 1mdc website in response to the question, “[w]hat happens to 1mdc if e-gold® collapses or is shut down?,” 1mdc states:

“1mdc simply ‘is’ e-gold®. Much as e-gold stores gold bars, 1mdc stores e-gold. Let’s say that aliens steal all the gold bars in the e-gold system so that an e-gold gram is valueless. A 1mdcGram simply IS an e-gold gram, so in that situation 1mdc would be valueless. Let’s say e-gold shuts down for some time (but, of course, e-gold still has all their gold). In that case ‘you’re all set’ because 1mdc will still function perfectly normally.”

124. 1mdc utilizes three e-gold accounts for its operations: 808080 (in the name of 1mdc “BAIL IN” Sweep Account), 808081 (in the name of “1mdc operations”), and 808082 (in the name of “1mdc assets”). Analysis of activity occurring in e-gold account number 808081 from June 2001 through March 2007 yielded the following results: There were a total of 15,556 transactions totaling \$51,256,764.15, comprised of 14,020 transactions into the account valued at \$25,582,256.54 and 978 transactions out of the account valued at \$25,674,507.58. As of March 2007, approximately 718.862047 grams (\$459,999.82) remained in e-gold account number 808081.

125. 1mdc’s e-gold account 808080 is similar to its operational account 808081 in that it provides a way for customers to transfer e-gold into 1mdcGrams. According to the 1mdc website:

“There’s a secret way to move your gold from e-gold to 1mdc ... [m]ake a

small spend from your own e-gold account to the 'special' e-gold account 808080 ... [w]ait about a minute, and log into your 1mdc account. The gold has been magically 'bailed in' to your 1mdc account."

Analysis of activity occurring in e-gold account number 808080 from June 2001 through March 2007 yielded the following results: There were a total of 3,063 transactions with a total value of 21258.41431 grams (\$15,865,725.74), comprised of 2,941 transactions into the account valued at 10639.30288 grams (\$7,767,942.81) and 122 transactions out of the account valued at 10619.11143 grams (\$8,097,782.93). As of March 2007, approximately 7.200981 grams (\$4,718.88) remained in e-gold account number 808080.

126. Whereas 1mdc uses e-gold accounts 808080 and 808081 primarily for purposes of accepting transfers into the accounts, it utilizes account 808082 primarily for transfers out of the account. Analysis of activity occurring in e-gold account number 808082 from June 2001 through March 2007 yielded the following results: There were a total of 11,528 transactions with a total value of 86041.3313 grams (\$59,061,110.53), comprised of 325 transactions into the account valued at 43166.2264 grams (\$29,509,907.04) and 11,203 transactions out of the account valued at 42875.1049 grams (\$29,551,203.49). Most of the large value transfers into the account were from 1mdc's operational accounts, numbers 808080 and 808081. As of March 2007, approximately .083572 grams (\$70.00) remained in e-gold account number 808082.

127. According to Omar Dhanani, an individual convicted of access device fraud in the above-described Shadowcrew prosecution, in addition to e-gold, members of carding websites use the digital currency 1mdc to buy and sell stolen credit card numbers and other contraband particularly because 1mdc is completely anonymous, and advertises itself as being completely offshore. Also according to Mr. Dhanani, 1mdc is preferred over other digital currencies because

1mdc is out of reach of U.S. law enforcement.

128. Mr. Dhanani used e-gold account number 1110111 to operate his digital exchange service for members of carding websites, discussed above. Analysis of e-gold account number 1110111 revealed 17 transfers totaling 710.306765 grams (\$286,972.54) to and from 1mdc's e-gold account number 808081.

129. ExpInvest International, discussed above, also used 1mdc to further obfuscate the source and ownership of its illegal pyramid scheme proceeds. Both e-gold accounts 2065103 (in the name of ExpInvest International) and 2352466 (in the name of EXP Deposit Account) transferred large amounts of e-gold through another e-gold account to 1mdc's operating account number 808081. For example, on February 26, 2006, after a value limit for "scammer" was placed on the account, approximately 1417.172758 grams (\$792,057) was transferred from e-gold account 2065103 through e-gold account number 2549363 to 1mdc's account 808081. Similarly, on February 26, 2006, after a value limit for "scammer" was placed on the account, approximately 174.642855 (\$97,608) was transferred from e-gold account 2352466 through e-gold account 2549363 to 1mdc's account 808081. Analysis of e-gold account 2549363 revealed that the only transactions into the account were these two above-referenced transfers and the only transactions out of the account were these two transfers to 1mdc's account 808081.

130. As of October 2006, 1mdc's operational accounts had a balance exceeding \$2,300,000 in e-gold, making 1mdc the largest account holder at that time within the e-gold

system.

I, Roy Dotson, a Special Agent with the United States Secret Service, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Affidavit is based upon reports and information known to me and/or furnished to me by law enforcement agents, and that everything represented herein is true and correct to the best of my knowledge and belief.

Executed on this \_\_\_\_ day of June, 2007.

/s/

---

Roy Dotson  
Special Agent, USSS