

**Emerging money laundering methods:  
Digital precious metals**

*By Saskia Rietbroek, CAMS*

*November 2009*

*This article was published in the Nov/Dec 2009 edition of Fiserv's client magazine NetPractice Exchange (www.netpractice.fiserv.com).*

Well-financed and technologically savvy criminals can move large amounts of funds easily and quickly from one country to another. They use new payment methods that have emerged in the last couple of years. They take advantage of our weaknesses, and are constantly looking for new opportunities to launder money. In this article, we take a look at a money laundering method involving digital currencies.

*Organized Crime: the world as stage*

Organized crime groups commit crimes using the whole world as a stage; the most international of them all being the ultimate organized crime: money laundering. And they do that because they know that for law enforcement it is difficult to work international cases, where the crime crosses borders. The reason is that it's difficult to collect evidence in other countries to build a case against the criminal. It takes a lot of time, and sometimes cooperation between different jurisdictions is not as it should be.

*"As in other criminal fields, also in money laundering, organized crime groups display peerless skill in managing the international dimension, while national and international authorities are constantly struggling with it."*

*Europol 2008 Organized Crime Threat Assessment*

*The path of least resistance*

Money laundering methods and routes evolve because of several factors. Technology is one of them, but other things as well influence the flow of dirty money.

For example, a weakening U.S. dollar has an impact on where criminals invest their money. Capital preservation is not only important to legitimate investors; it is for launderers as well. They will try to get a better return on their investments. So if the euro is high against the dollar, there is an influx of dirty money into financial institutions in the Eurozone.

2009 © All rights reserved. AML Services International, LLC

Tel. +1-305-608-7888

[www.nomoneylaundering.com](http://www.nomoneylaundering.com)

[saskia@nomoneylaundering.com](mailto:saskia@nomoneylaundering.com)

# AML Services International, LLC

New rules and regulations also influence the flow of the ill gotten funds. It will always try and take the path of least resistance. While governments have been issuing anti-money laundering regulations for decades for the banking sectors, others sectors, until recently, were often overlooked. For example, in many countries, AML regulations for digital currency issuers are either nonexistent, or were only recently enacted.

## *Digital smurfs*

In the first phase of the laundering cycle, the launderer wants to introduce the cash into the financial system. To avoid detection, they may want to physically transport it to another country where financial institutions are less likely to report large cash deposits to the authorities. This is why launderers engage in so called "Bulk cash smuggling." The vehicles that were used to transport the drugs sometimes do double duty. They also use it to smuggle the cash back. But there is a practical challenge. Cash is heavier than drugs. Take the example of cocaine. If you sell 20 pounds of heroin for let's say US\$ 1 million, and it was paid in US\$20 bills, this will result in 100 pounds of cash. So that is 5 times as much load that you have to carry back after you sell the heroine. This is why the cash needs to be deposited in the financial system, converted into larger bills (refining) or digital value.

Today, digital smurfs exchange dirty money for digital value in the form of digital precious metals, or digital currency.

## *Digital currency accounts*

With digital currencies you can move money internationally in a manner that approximates money remittance or wire transfers. Digital currencies are denominated into internationally recognized weights of precious metals, such as gold or silver. You can open an anonymous digital precious metal account online. A digital precious metal account is very much like an online bank account except your funds are held in precious metal and not paper currency. The balance on your statement is denominated by weight in grams of gold and not dollars or euro.

Anonymity is heavily marketed characteristic of the digital currency industry. Because digital currency accounts are obtained online and are not subject to the customer identification procedures associated with obtaining a traditional bank account, they often can be opened and funded anonymously. Some issuers require identification, but because users open digital currency accounts online, documents are generally faxed or scanned to the issuer and can be easily falsified. Interesting for the launderer is also that a digital

# AML Services International, LLC

currency account can function as a merchant account. This means that a digital currency account holder can be a front or shell company.

To fund the account, you can use wire transfers, money orders, or by making cash deposits directly to an exchanger's bank account. Many exchangers will convert digital currency balances into anonymous prepaid (stored value) cards that can be used to withdraw funds by various methods, including at ATMs all across the world.

The anonymity and international features are very attractive to a money launderer. Digital currency accounts also allow individuals to execute multiple currency-to-currency exchanges in a short period of time and therefore they can become an ideal layering mechanism.

## *Real life case: E-Gold*

E-Gold, was a digital currency operator that was once used by millions of people in more than a hundred countries. Today the currency is barely alive. Its owner pled guilty last year to money laundering-related crimes, and to operating an unlicensed money transmitting service.

In 2003, the Secret Service launched an undercover operation against a website called Shadowcrew — a legendary forum for “carders” who trafficked in stolen credit card numbers. Cyber crooks in Eastern Europe were stealing millions of card numbers in phishing and skimming scams, then passing the data to accomplices around the world. The low-end cashers coded the numbers onto blank cards, then siphoned money from ATMs and transmitted the bulk of proceeds back to the former Soviet bloc. Authorities discovered that E-Gold was among the fraudsters’ preferred money-transfer methods, because the system allowed users to open accounts and transfer funds anonymously anywhere in the world.

According to the indictment, persons seeking to use the alternative payment system E-Gold were only required to provide a valid e-mail address to open an E-Gold account--no other contact information was verified.

When the authorities seized the E-gold computer database, they found that in the account records sometimes indicated the type of (criminal) activity that the account-holder was engaged in, including, among other things, "child porn," "Scammer," and "CC fraud."

In E-Gold, accounts holder names were often obviously fake names such as “Donald Duck,” “Bud Weiser,” “Anonymous Man.”
--

2009 © All rights reserved. AML Services International, LLC

Tel. +1-305-608-7888

[www.nomoneylaundering.com](http://www.nomoneylaundering.com)

[saskia@nomoneylaundering.com](mailto:saskia@nomoneylaundering.com)

# AML Services International, LLC

According to Jeffrey A. Taylor, U.S. Attorney for the District of Columbia, "The defendants operated sophisticated and widespread international money remitting business, unsupervised and unregulated by any entity in the world, which allowed for anonymous transfers of value at a click of a mouse. Not surprisingly, criminals of every stripe gravitated to E-Gold as a place to move their money with impunity."

*What can financial institutions do to mitigate the risk posed by digital currencies operators?*

It's obvious that new laundering techniques surface regularly, and for each method, there will be a number of variations, permutations, and combinations constructed to avoid creating a pattern.

Government agencies are often strapped for funds to tackle new trends, and often react too slowly. In the current economic environment, financial institutions also often lack the budget to adjust their monitoring efforts to emerging typologies. AML Compliance is a moving target. Financial institutions must find a way –even with few resources – to continually reassess what they are doing in order to detect emerging money laundering methods.

One example is to regularly review the client data base to see if the financial institution has accounts for digital currencies operators. If so, are the accounts marked as higher risk in your automated solution for enhanced monitoring and with appropriate (lower) thresholds?

There is a variety of automated solutions to help financial firms protect against abuse by high risk customers. Examples are software that can assist the institution in properly classifying the risk for accounts, including those of digital currency operators, and automatically adjust the monitoring thresholds accordingly, if necessary.

*From 2001-2005, Saskia Rietbroek served as the founding Executive Director of the Association of Certified Anti-Money Laundering Specialists (ACAMS). She currently serves on the ACAMS Advisory Board and is a frequent speaker at money laundering conferences. She is Partner at [www.nomoneylaundering.com](http://www.nomoneylaundering.com), a company providing anti-money laundering services, training and audits to firms worldwide. She is also Financial Crime Advisor for Fiserv, a Fortune 500 company.*

2009 © All rights reserved. AML Services International, LLC

Tel. +1-305-608-7888

[www.nomoneylaundering.com](http://www.nomoneylaundering.com)

[saskia@nomoneylaundering.com](mailto:saskia@nomoneylaundering.com)