Laundering Money Online: a review of cybercriminals' methods

Jean-Loup Richet

Tools and Resources for Anti-Corruption Knowledge – June, 01, 2013 - United Nations Office on Drugs and Crime (UNODC).

Executive Summary

Money laundering is a critical step in the cyber crime process which is experiencing some changes as hackers and their criminal colleagues continually alter and optimize payment mechanisms. Conducting quantitative research on underground laundering activity poses an inherent challenge: Bad guys and their banks don’t share information on criminal pursuits. However, by analyzing forums, we have identified two growth areas in money laundering:

- **Online gaming**—Online role playing games provide an easy way for criminals to launder money. This frequently involves the opening of numerous different accounts on various online games to move money.

- **Micro laundering**—Cyber criminals are increasingly looking at micro laundering via sites like PayPal or, interestingly, using job advertising sites, to avoid detection. Moreover, as online and mobile micro-payment are interconnected with traditional payment services, funds can now be moved to or from a variety of payment methods, increasing the difficulty to apprehend money launderers. Micro laundering makes it possible to launder a large amount of money in small amounts through thousands of electronic transactions. One growing scenario: using virtual credit cards as an alternative to prepaid mobile cards; they could be funded with a scammed bank account – with instant transaction – and used as a foundation of a PayPal account that would be laundered through a micro-laundering scheme.
Laundering Money Online: a review of cybercriminals’ methods

Millions of transactions take place over the internet each day, and criminal organizations are taking advantage of this fact to launder illegally acquired funds through covert, anonymous online transactions. The more robust and complex the various online marketplaces become the more untraceable methods criminals are finding to pass ‘dirty’ money into online accounts and pull ‘clean’ money out of others. The anonymous nature of the internet and the ever evolving technologies available allow numerous opportunities for online money laundering operations to take place. Many of these methods involve using a ruse to pull unsuspecting participants into their money laundering schemes, often with serious financial and legal consequences for victims. The best way for law abiding citizens to avoid becoming complicit in such illegal activities is to stay informed as to the methods criminals are using to pull them in.

We all know the oldest ‘physical’ placement methods of money launderers: cash smuggling, casinos and other gambling venues, insurance policies (launderers purchase them and then redeem them at a discount, paying fees and penalties but receiving a clean check from the insurance company), hawalas / fe chi’en or the black market peso exchange (informal value transfer system), shell corporations, and so on and so forth. But there is also a number of online money laundering schemes currently being used by criminal enterprises to pass illegally received funds through legitimate accounts, and new ones are popping up all the time. Some of the most widespread schemes are detailed in this article.

Methodology

Ostensibly, conducting quantitative research on underground laundering activity poses an inherent challenge: Bad guys and their banks don’t share information on criminal pursuits. Our approach utilizes an online ethnography, observing large online hacker forums and communities and researching topics related to money laundering on their databases. We used a large variety of keywords, from those linked with payment solutions to those associated with black markets. After a first review, we filtered our data, and discarded irrelevant forum threads. We then analyzed the content of these threads and synthesize our findings into the following categories.
The classics: from money mule scams to black markets

Liberty Reserve

Frequently associated with carding communities\(^1\), Liberty Reserve (LR) had a bad reputation amongst some Black Hats boards\(^2\).

But there were very few ways to receive money anonymously, and LR was one of them. Thus LR was widely advised when one wanted to launder money:

\(^1\) Cybercriminals involved in credit card fraud.
\(^2\) Internet forum boards which aim to share advice on cybercrime and fraudulent methods.
Exchanging money could be done through the use of verified exchangers such as ebuygold.com - they have been verified by Liberty Reserve. There is a lot of fly-by-night firms and scammers in this shady market. Because of that, peers markets are growing. The following screenshot is an
example of a peers market (e-currency auction service, member to member), a marketplace for anyone who wants to exchange currencies.

However, the closure and seizure of Liberty Reserve will not end these fraudulent practices – there are numerous competitors and alternatives (WebMoney, Bitcoins, Paymer, PerfectMoney and so on)…
Money mule scams

**Guide posted on a board about how to use a money mule to launder hacked bank account**

This is a method you’re probably familiar with if you check regularly your spam e-mail box. It involves a very friendly e-mail from someone from a foreign country claiming that they need your help to transfer a large sum of money to your country. For your help with the transfer you will receive a percentage of the transfer, which, according to the e-mail, will amount to several thousand dollars or more. All you have to do is supply your bank account information.
Some of the senders claim to be Princes, government agents, or other high ranking officials from the country they claim they are from. They are written in a very gracious and humble tone, and very politely ask for your help, as if you’d be doing them a huge favor.

While most people know that any inquiry requiring your personal financial information should immediately throw up a red flag, some folks do fall victim to this kind of scam. While some of these scammers will simply try to steal money from your account, others will attempt to transfer large sums of money stolen from other accounts to you. They’ll have you send the majority of the funds to an alias account of theirs in exchange for your cut. Once the bank realizes the transaction was illegal, you will be held accountable, as the stolen funds were withdrawn from your account.

Other scams involve supposed job offers. With so many individuals interested in work from home jobs, there are a countless number of potential victims here. The ‘job’ that you’ll be doing involves accepting money transfers to your account and passing the money on to alias accounts set up by your so called employer. Of course, the transfers you’ll receive will contain illegally
obtained funds, and when law enforcement traces the funds, it will lead them to you, not the criminals who illegally obtained the money.

Prudential L.T.D

Job Summary

Company
Prudential L.T.D
Location
New York, NY 10001
Industries
Financial Services
Job Type
- Full Time
- Part Time
Years of experience
1-2 years
Career Level
Manager (Manager/Supervisor of Staff)
Salary
$40,000.00 - $60,000.00 USD/year commission

Finance Manager

About the Job
Dear Sir/Madam,

Our firm has an opening for a FINANCE MANAGER position.

This will be a part-time/home based position and the applicant must have the following qualifications:
- Be able to check your email several times a day
- Confident PC user (SW package office), mail programs, Internet
- Cell phone
- Adult age

What we offer:
- Generous salary- $5,000 per month
- Social benefits and medical insurance
- Free training and seminars

More benefits:
- You don't have to pay for anything to work for us
- No selling
- This is not network marketing
- This is not a distributorship

We are proud to be an equal opportunity employer.
Over $7 billion each year is laundered through Colombian corporations from Mexican and Colombian drug cartels. This is done through the Black Market Peso Exchange or BMPE. The BMPE is actually a covert system of banking that helps drug dealers to exchange American dollars for pesos. These dollars are then purchased by Colombian businessmen and used to buy American goods which are then sold back home in Colombia. This traditional form of crime is enhanced with ICT: Drugs could be sold through illegal online marketplaces such as the Silk Road, in e-currencies like bitcoins in order to increase the difficulty to trace the operation, while brokers use blackberry messengers and negotiations are conducted through the internet.
The BMPE is similar to *hawalas* – meaning transfer in Arabic – or *fe chi’en* in China: they are international underground banking systems. Online money laundering techniques are interconnected with these traditional methods, which are no longer ‘localized’. Online operations contribute to complexity the audit process and thus hide the illegal source.
Increasing trends in online money laundering

Online Games as obfuscators

Online role playing games provide an easy way for criminals to launder money. This frequently involves the opening of numerous different accounts on various online games to move money.

Other clever scammers have found a way to launder money using online games. Massively multi-player online role playing games (MMORPGs) provide an easy way for criminals to launder money. This frequently involves the opening of numerous different accounts on various online games.

Since MMORPGs use credits that players can exchange for real money, it is easy to do. Popular games for this type of scam include Second Life and World of Warcraft for instance.
While the market increase, new services emerge for gold sellers; those websites also provide prepaid cards useful for money laundering purposes.

MMORPG players very rarely know the people that they meet online. Citizens from dozens of different countries play these online games. Using the virtual currency systems in these games, criminals in one country can send virtual money to associates in another country. Then, the virtual money can be transferred into real money, with the criminals leaving no trace of evidence authorities could follow back to them.
Underground forums share money laundering best practices and tips

It is important to note that the game developers are not associated with the scam at all, and in many cases are involved with the efforts to stop such crimes from occurring.

Recent years have seen the emergence of virtual communities and online gaming; scams related to MMORPGs will rise with these virtual worlds.
Micro laundering: micro-payment, micro-jobs and m-commerce

Cyber criminals are increasingly looking at micro laundering via sites like PayPal or, interestingly, using job advertising sites, to avoid detection. Moreover, as online and mobile micro-payment are interconnected with traditional payment services, funds can now be moved to or from a variety of payment methods, increasing the difficulty to apprehend money launderers. Micro laundering makes it possible to launder a large amount of money in small amounts through thousands of electronic transactions. One growing scenario: using virtual credit cards as an alternative to prepaid mobile cards; they could be funded with a scammed bank account – with instant transaction – and used as a foundation of a PayPal account that would be laundered through a micro-laundering scheme.

Cleaning money might be an issue for some beginner money launderers… They frequently ask for partnership on forum boards.
For larger amounts of money, hackers' forum boards provide advice on how to launder PayPal money while minimizing the commission.

Laundering online money is a growing topic of interest on hackers' forum boards; in term of trends, the use of CCNOW is a favored PayPal alternative.
Using online job marketplaces are an increasing recommendation

Online jobs marketplaces such as Freelancer or Fiverr provide an interesting legitimate covert for money launderers. Job marketplaces could be used as anonymizers, escrow services providing a useful way for covering up the launderer’s traces.
Fiverr micro-services ranging from $5 to $30 could also be used to reduce the footprint of a scammed account: amounts are small enough not to trigger a review under banking regulations. New money mule scams related to these platforms emerge. Indeed, many marketplaces users have been receiving emails asking them to join into a partnership involving the use of their accounts to sell services. They will usually provide some reason that they can’t open their own account, and offer to pay you a percentage of every transaction made through yours. These supposed contractors will put up many fake auctions, and ask you to transfer the funds from them to alias accounts. This is an evolution from the precedent model (classic money mule scam) as it no longer involves bank transfers but e-currency transfer (from Paypal to Bitcoin), and no longer concerns a large sum of money send once but small amounts send multiple times.

The spread of mobile banking has been especially rapid and broad in Africa and Russia (see M-Pesa - Kenya’s mobile wallet - and SMS Coin for instance) while global M-commerce market has grown steadily. It is now possible to send money from prepaid mobile card to criminal partners that will convert the credit into cash. This method provides criminals anonymity with a quick and easy access to money from nearly anywhere in the world.
Virtual credit cards are a growing alternative to prepaid mobile cards; they could be funded with a scammed bank account – with instant transaction – and used as a foundation of a paypal account that would be laundered through a micro-laundering scheme.

Because online and mobile micro-payment are interconnected with traditional payment services, Funds can now be moved to or from a variety of payment methods, increasing the difficulty to apprehend money launderers. It is possible to launder a large amount of money in small amounts through thousands of electronic transactions.
Conclusion

As we spend more time and money online, opportunities for criminals to involve us in their money laundering scams will only continue to grow. This will create an increasingly difficult situation for the various law enforcement agencies that are already being put to the test by the cunning of such criminals and the myriad untraceable means they have discovered to launder illegally obtained money.

As individuals, it is our responsibility to stay informed, and always be aware of the methods these criminals may use to involve us in their laundering schemes.

Jean-Loup Richet

About the Author

Jean-Loup Richet is Information Systems Service Manager at Orange and Research Associate at ESSEC Business School - Institute for Strategic Innovation & Services. He graduated from the French National Institute of Telecommunications, Telecom Business School, and holds a research master's from IAE/HEC Paris.

Expert in IS Security, Jean-Loup Richet has been a speaker at several national and international conferences in Information Systems and has published articles in academic and trade journals. He is also a lecturer in IS Risk Management at Sorbonne Graduate Business School (International MBA).