MONEY LAUNDERING VIA INTERNET IN GEORGIA

Aleksandre Glonti, PhD Student
Grigol Robakidze University, Tbilisi, Georgia

Abstract

The given article mainly focuses on the money laundering crime conducted using the online gambling websites in Georgia. It offers an insight on the scheme of how advanced computer users transfer finances using digital wallets, avoid attention from the law enforcement bodies, and ultimately withdraw the laundered money. In the end of the article, a reader will find recommendations for the legislative implementations on the national/supernational level to make online fund transaction more transparent process for the law enforcement agencies.

Keywords: Money Laundering, Cybercrime, Cyber Security, Legislation, Georgia

Introduction

Technological advancements of the information era brought many profound changes to our everyday lives. Internet, indeed one of the most revolutionary inventions of the contemporary times, introduced new possibilities of interaction and socialization. Eventually, these novelties led to transformation of nearly every institution, including the financial institutions. Online banking, e-commerce, and digital monetary transactions made financial interactions much more convenient, however, led to the outburst of the new type of crime - Financial Cybercrime. While there are numerous ways to commit financial cybercrime, this article will deliberately focus on money laundering via Internet.

In fact, recent researches in the field of financial cybercrime depict that in the last decade there has been a colossal raise in property crimes using the cyber technologies. For example, the Center for Strategic and International Studies reports that in 2013 worldwide annual loss from financial cybercrime was ranged from 300 billions to 1 trillion of US Dollars (http://csis.org/publications/browse/all/all/Reports). Other researches show that from 2000 until 2010 statistical amounts of cybercrime raised more than ten times (Norton Cybercrime Report, 2012).

As finances got digitalized, money-laundering crime has become relatively easier to commit. The reason behind the stated hypothesis is that digital wallets and other types of online financial institutions are relatively less monitored by the law enforcement agencies worldwide. According to "A Global Overview of Digital Wallet Technologies" published by University of Toronto, a digital wallet refers to an electronic device that allows an individual to make electronic commerce transactions (University of Toronto, 2011). This can include purchasing items on-line with a computer or using a smartphone to purchase something at a store. Increasingly, digital wallets are being made not just for basic financial transactions but also to authenticate the holder's credentials. For example, a digital-wallet could potentially verify the age of the buyer to the store while purchasing alcohol. It is useful to approach the term 'digital wallet' not as a singular technology but as three major parts: the system (the electronic infrastructure) and the application (the software that operates on top) and the device (the individual portion).

Introduction of the digital wallets entailed many legislative and enforcement problems. The most notable of these problems are almost uncontrolled cross border

transactions of finances. At the moment, it is hard, if not impossible, to monitor the actual sender and the beneficiary of the funds transacted via Internet.

In Georgia, utilization of the digital wallets became popular only recently. Nevertheless, today it would be extremely challenging to find any financial institution that does not provide its users with possibility to manage their financial accounts and make monetary transactions via Internet.

The source, which preferred to remain incognito, reported that monitoring of the online financial transactions is practically an insurmountable task; afore stated fact has several solid reasons. First and foremost, to start the investigation process of the given case law enforcement bodies require an official declaration of the committed crime. In case of money laundering, in particular, there is usually no one to report the crime incident. Consequently, such acts usually remain outside of the focus of the law enforcement agencies. Secondly, identification of the particular criminal on the Internet is frequently a futile attempt. Advanced computer users have a wide variety of software and hardware tools to disguise their IP addresses, as well as the accounts they used to register on the digital wallets. Even if the cyber criminal gets apprehended, prosecutor usually lacks credible evidence to provide it to the court in terms of proving that there was one particular person behind the used IP address to commit the crime.

From the empirical perspective, there are many methods to launder money via internet. One of the most widely used method, I would like to discuss in this article, is online gaming. In 2013, Jean-Loup Richet published an article titled "Laundering Money Online: a review of cybercriminals' methods." In the given article Mr. Richet advocates "Online role playing games provide an easy way for criminals to launder money. (Jean-Loup Richet, 2013: 17). This frequently involves the opening of numerous different accounts on various online games to move money. 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" (McAfee Center for Strategic and International Studies, 2014).

Instead of the role-playing games, in Georgia cyber criminals usually use Internet gambling websites. As a matter of fact, online casinos have become increasingly popular in the last couple of years. Since digital gambling is relatively new phenomenon to Georgia, cyber criminals managed to successfully exploit many loopholes to achieve their illegitimate goals, including laundering of money. Regardless of several in depth investigations of the online gambling providers, some of the weak spots still remained unattained.

To extend the research I have chosen one of the most popular Internet gambling providers in Georgia. To register on the given website applicant needs to indicate:

- Country
- Name
- Family Name
- Cellphone Number
- Email Address
- ID, Driver's License, Passport, or Residence Permit
- Physical Address
- Sex

To the date, from all the above-mentioned credentials, the given gabling service provider requires only cellphone number authentication/verification. The issue is that in Georgia, it is exceedingly easy to obtain a cellphone number without actually providing your personal information. Those who want a number for malicious activities can purchase one outside of the official branch of the telecommunication providers. Owner of such unregistered SIM card can also have a covert Internet access to perform the illegal manipulations.

To physically withdraw the money from the Casino a cashier user is asked to present his/her ID, driver's license, passport, or the residence permit. However, in case of transferring money from the personal account to any of the possible digital wallets, the user does not have to be authenticated. This is the very loophole cyber criminals use to transfer the illegitimately acquired money to a foreign country. Once digital money leaves borders of Georgia, it becomes impossible to monitor its further flaw. Experience shows, that majority of digital wallet service providers are not eager to cooperate with law enforcement agencies. However, even if they agree to cooperate, the investigation process usually takes very long time. Meanwhile, the cyber criminal transfers money back and forth from one unauthenticated digital wallet service provide to another. This is done to wind up the trace of the money flow. Ultimately, the laundered money returns back to Georgia. Eventually, it is impossible to indicate the source of the transaction.

Most sophisticated criminals use other people's banking cards to withdraw the laundered money from received abroad. Consequently, law enforcement agencies are left without any chance to investigate the case.

For the sake of making a contrast, I have observed another popular Internet gambling service in Great Britain. Perhaps not surprisingly, online transactions were relatively more complicated. One notable discovery was that it was absolutely impossible to transfer money to the unauthenticated users. To validate user was required to provide scanned digital copies of:

- Passport
- Document that indicates current place of residence
- Banking card that was used to deposit money to the given account

If the banking card did not belong to the user, he/she was required to send the scanned copy of signed declaration of liability that cardholder permits using of his banking card. Once the account was validated, Casino permitted online transactions to digital wallets.

Indeed, such credible security system may also be compromised, but it would be a complicated process for the cyber criminals.

It has to be admitted, that investigation of any type of cybercrime is a very difficult procedure. Even if law enforcement agencies apply maximum of their capabilities and efforts to investigate any given cyber criminal act, there are very high chances that it will remain without a court verdict, due to lack of convincing evidence. In future, financial cybercrime is only expected to grow in its intensity. Hence, it is still possible to implement certain legislative measures to complicate the process for the criminals.

Conclusion

World must accept the severity of the consequences of cyber criminality. Digital wallet service providers should be more flexible and willing to cooperate with law enforcement agencies. At the same time, partner nations should implement harmonized legislative acts regarding financial transactions. If any country rejects the given process, it will remain an offshore zone for the illegitimate financial activity. In the given case, these countries should be limited to use digital wallet services from abroad.

Another effective way to reduce financial cyber crime is to reconsider norms that regulate financial transactions to the unidentified digital wallet accounts. In the partner countries they should be harmonized. The best idea would be to reject/banish not validated digital wallet accounts. Doing so would seriously alter cyber criminal activity, as well as unmonitored flow of the funds.

References:

1. McAfee Center for Strategic and International Studies: “Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II” – 2014.
2. http://csis.org/publications/browse/all/all/Reports
3. Norton Cybercrime Report – 2012.
4. Kaspersky Lab: “Global IT Security Risks” – 2012.
5. University of Toronto: "A Global Overview of Digital Wallet Technologies” – 2011.
6. Jean-Loup Richet: “Laundering Money Online: a review of cybercriminals’ methods” – 2013.