Virtual Currencies in Online Gaming:

The Perfect Money-Laundering Tool

Research Project for Emerging Issues/Advanced Topics Course

Diploma in Investigative and Forensic Accounting Program

University of Toronto

Prepared by Billy Chung

June 20, 2013

For Prof. Leonard Brooks

Table of Contents

Abstract

Often linked to organized crimes and terrorism, money laundering is a serious problem in today's world that deserves much of our attention. Despite the government's best efforts in protecting its citizens from illegal actions, criminals have been able to stay ahead by exploiting new technologies, and by attacking areas with weak regulatory measures. Virtual money laundering has become something of great interest to criminals in recent years. This is partly due to the fact that each micro-payment or transfer is too negligible to raise the eyebrows of crime-monitoring authorities, but when such payments or transfers are made in aggregate, the negative impact on our economy should not be overlooked. This paper will analyze the existing anti-money laundering ("AML") measures in online games. In particular, the questions—are the AML measures sufficient, and what can be done to deter money laundering—will be examined in detail. Previous research has focused on money-laundering risks in virtual currency exchanges within a more global context. Instead, I will examine money-laundering risks that are specifically relevant to online gaming, with reference to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("PCMLTFA") in Canada. Since online games are mostly popular to young adults, I find it necessary to begin this thesis by offering a comprehensive overview of the current status of online gaming, the diversity of gaming commerce, and the various payment methods that are involved, in order to reach out to the readers who may not be familiar with the subject. Moreover, the ways in which online games use virtual currencies and credits to facilitate e-commerce and money transfers, as well as the current key money-laundering risks, will be discussed in my analyses. I will conclude this thesis by offering suggestions on how the Canadian government can possibly attack money-laundering activities in virtual currencies in the future.

What is money laundering? What are the consequences of money laundering?

Essentially, money laundering is the process whereby "dirty money" from any criminal activity is transformed into "clean money," as noted in the diagram below. There are many ways to launder illicit funds and regardless of the method used, the ultimate goal is to conceal the source of money obtained by illicit means and to do that, a money laundering process would go through the following three recognized stages:

- Placement involves placing the proceeds of crime in the financial system.
- Layering involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds.
- Integration involves placing the laundered proceeds back in the economy to create the perception of legitimacy.

This money laundering process is a continuous flow, with new dirty money being introduced into the financial system after the old dirty money gets cleaned.

source: money.howstuffworks.com

"The International Monetary Fund ("IMF") stated in 1998 that the aggregate size of money laundering in the world could be somewhere between two and five percent of the world's gross domestic product. Using 1998 statistics, this roughly translates to between USD 590 billion and USD 1.5 trillion."[1] Illegal acts of such magnitude could have serious potential social and political costs if left unchecked. As a result, governments around the world and AML bodies have undertaken efforts to

[1] Money Laundering F.A.Q., The Financial Action Task Force, accessed on May 2, 2013 from http://www.fatf-gafi.org/pages/faq/moneylaundering/.

deter, prevent and apprehend money launderers. Collectively, authorities implemented AML controls that require financial institutions and other regulated entities to detect and report money-laundering activities. Although these anti-money laundering guidelines have existed for some time, it only came into prominence globally as a result of the formation of the Financial Action Task Force ("FATF"), an intergovernmental body whose purpose is to develop and promote an international response to fight money laundering.

source: Financial Action Task Force

In additional to international bodies, G7 countries have all enacted their own laws to combat money laundering. In Canada, a money laundering offence usually involves various acts committed with the intention to conceal and convert proceeds of crimes derived from designated offences. Here, a designated offence means the most serious offences under the Criminal Code and the Canadian federal Act that addresses the anti money laundering issues is the Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("PCMLTFA")[2]. Essentially, all financial transactions from suspected proceeds of crime with illicit origin are to be reported to the Financial Transactions and Report Analysis Centre of Canada ("FINTRAC"), a financial

[2] *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, Financial Transactions and Reports Analysis Centre of Canada, accessed on May 2, 2013 from http://www.fintrac.gc.ca/act-loi/1-eng.asp.

intelligence unit under the Minister of Finance that deals with financial information on suspected money laundering and terrorist activities financing.

source: FINTRAC

Money laundering is simply the transfer of illicit funds but the real dangers come from the ultimate use of the proceeds. In many cases, the laundered money has wound up in the hands of terrorists or people behind organized crime. In the case of terrorism, the threat is ever so real and close to home. The 2013 Boston bombing, the subsequent arrests in Canada, along with the Bulgaria bombing in 2012, are all evidence of a persistent threat. All these events combined highlight one simple fact – terrorist financing has not slowed down despite our very best efforts to safeguard against money laundering. Perhaps equally troubling is the fact that no matter where we are, the world is all connected and thus, we cannot ignore the threats that are happening elsewhere in the globe. With no ends in sight, we can only assume that the threat of terrorism will continue to go up as groups like the Al Qaeda continue to branch out into other countries. With no slowdown in terrorism, the ability of the Canadian governments to detect and deter criminal groups from using the financial system as a means to further their acts of violence, becomes ever more critical. The evidence of the Boston bombing is a fresh reminder to us that no one is isolated from any acts of terrorist violence and our government must now remain more vigilant at all times. Strengthening the Canadian anti-money laundering and counter-terrorist financing ("AML/CTF") is a necessary step in the right direction because criminal

activities elsewhere in other parts of the world can have repercussions on our economy.

Another alarming observation is the rapid increase of organized crime in today's world. The connection between organized crime and money laundering is obvious. In almost all of these cases, there are victims, losses, and in the end, a real social disruption. Organized crime can alter the way a business is conducted, the method in which a contract is entered, and in some extreme cases, the determination of the winner and loser. Organized crime can happen anywhere at any time, and when it is combined with money laundering, together they could weaken the integrity of our financial system, which could create negative effects on our society. A very recent case with the HSBC bank helps to highlight prevalence of money laundering in organized crime. "For a period of four years between 2006 to 2009, the bank helped two drug cartels handle at least 881 million dollars in laundered funds and wire transferred over 200 trillion dollars through its banking system."[3] Putting this into perspective, Canada's annual GDP for 2012 was slightly less than 2 trillion, so this scheme was a hundred times the size of our GDP. With the underground economy potentially many sizes bigger than our real world, how can we afford to turn a blind eye on money laundering? Looking beyond the numbers, this case also helps to highlight the real danger that a single financial institution alone could have if no one inquires into questionable transactions and irregular transfers. It is unfortunate that the bank's money laundering preventive measures were deficient, and the latter has led to massive penalties to HSBC and its stakeholders at the end.

---

[3] Financial Transactions and Reports Analysis Centre of Canada, Media Release, "Keynote address by Director Gérald Cossette - Financial Transactions and Reports Analysis Centre of Canada to the Canadian Institute's Annual Anti-Money Laundering Forum," accessed on May 6, 2013 from http://www.fintrac-canafe.gc.ca/new-neuf/ps-pa/2013-04-24-eng.asp.

Aside from banking institutions, organized crimes could also infiltrate many other industries if existing statues or regulations are not robust enough to handle the challenges. At the end of the day, the truth is that the existing AML regimes are outdated and if this situation is not rectified immediately, we are bound to see an increase in organized crime, which can hinder economic growth, and ultimately disrupt our lives.

With is online gaming? What are the different types?

Online gaming refers to playing games over a network of computers or through the Internet. It is the new phenomenon and has the potential to grow in popularity for a number of reasons. Casual gamers can easily find opponents of a similar skill level when playing a head-to-head online game. Heavy gamers can compete in massively multiplayer online role-playing games ("MMORPGs"), where dozens of players either play for or against each other in a virtual world environment. Some games include a series of quests to excite gamers, while others simply let you roam around in a virtual world, allowing users to meet strangers or reacquaint with old friends. In almost all cases, players communicate to each other via text chat or audio headset.

As a subset of online games, social games grow out from online social networking where players log on to meet up with old friends and make new ones. Virtual world gaming is another subset of online games where players are typically charged a monthly fee for access to a network that helps them to connect to other gamers remotely. When joining a virtual game, participants are usually given an End User License Agreement ("EULA"), a set of rules that define the required behavior. Anyone caught violating the rules will be banned from playing the game.

Although the game play and audience may be different, social games and virtual world gaming have one thing in common: players in either space can have the option of exchanging virtual money for real currency, thus virtual world gaming and online social gaming are both easily vulnerable to money laundering. The European Network and Information Security Agency ("ENISA") defines virtual worlds as having the following characteristics[4]

• Advanced graphic capabilities;
• Global reach;
• Use of immersive or inter-real characters;
• Persistence (the virtual environment as seen by all users is the same);
• Central storage on a database controlled by the service provider;
• Interaction by users in real time;
• Physical laws determine how interactions take place "in-world"; and
• Users participate using avatars (a digital representation of the user), which enables a degree of virtual interaction not possible through text-based Internet technologies such as chat.

source: The European Network and Information Security Agency

With many game-playing possibilities, players in virtual world gaming can purchase goods and services to enhance their game experience with credit cards,

[4] Geary, Joy, "Only in the Virtual World," Anti-Money Laundering Magazine, December 2011, pg.17, http://www.amlmagazine.com.au/amlwr/_assets/main/lib90004/only%20in%20the%20virtual%20world_issue%2031_dec11.pdf.

PayPal or prepaid cards. They can then transfer, buy or sell goods and services using virtual currency that can be converted into real currency. Theoretically, these individuals can use this process to funnel proceeds of crime from one jurisdiction to another, and avoid the regulatory safeguards that were already set up to detect these money laundering activities. Such criminals can also exploit online games by opening hundreds of separate accounts. They can buy and sell things in the virtual world to and from themselves. These transactions are hard to detect because they would appear to be routine on the surface. What typically happens in the end is that the virtual money will be funneled to a master account held by the criminal, who will then cash it out into real money.

MMORPGs

Of the all subsets of online gaming, perhaps the sales of MMORPGs with game titles like "World of Warcraft" or "League of Legends" have outpaced all others.

source: League of Legends

source: "Riot releases League of Legends beta client for Mac," Venturebeat.com

MMORPGs are massively multiplayer online role-playing games and a well-made one can generate millions of diehard followers. Unfortunately, the same MMORPG can also be a great money-laundering tool. Due to its virtual location, the names of its operators are unknown, and they are often beyond the reach of law enforcement in most jurisdictions. According to Myke Sanders, a board member of the International Game Developers Association ("IGDA"), money laundering in MMORPGs can be easily achieved. Nothing more than a computer, an internet connection and a stolen credit card number is needed to create a new account in a MMORPG. A user account can be created from a stolen credit card, while virtual currency can be purchased from the prepaid card purchased from proceeds of crime. The main reason to use this is that at no time can the activities be attached to an individual when stolen identities were used in the first place.

According to Amir Orad, the CEO of Actimize Inc., a provider of anti-crime software, "proceeds of crime can be easily placed, layered, and eventually laundered through MMORPGs."[5] In the game of "World of Warcraft" for example, criminals

[5] Financial Transactions and Reports Analysis Centre of Canada, "Money Laundering and Terrorist Activity Financing Watch: October-December 2010," accessed on May 4, 2013 from http://www.fintrac-canafe.gc.ca/publications/watch-regard/2011-04-eng.asp.

can launder money by simply buying virtual gold coins with their criminal proceeds, and such gold coins can be purchased either from friends or employed cheap labor from places like India or China to help with the gold coin gathering.

Cyber-security tracker Winn Schwartau claims that it would not be unusual for drug cartels to hire gamers to launder their proceeds through these online games. "At the layering stage of the money laundering cycle, one would simply open hundreds of separate accounts in a game and then buy and sell items in the virtual world to and from themselves. On the surface, these trading activities can appear very legitimate, and the small amounts used in each transaction are hard to detect. Once the trading accumulates to a sizable amount, all the virtual money will be funneled into one master account held by the criminal and sold to someone else in the game for real money." [6]

According to Orad's figures, the percentage of money being laundered through MMORPGs is relatively low because the games are not as big as the real economy. However, as the online gaming industry continues to grow, this less-controlled environment will become an ideal place for criminals to carry out their money laundering business. Mr. Orad further believes that as of 2010, "trillions in various real local currencies already get circulated into virtual money, which when converted into dollars, would be tens to hundred of millions of dollars."[7]

Second Life

When it comes to virtual world gaming, Second Life is the game that has

[6] Ibid.
[7] Tsuruoka, Doug, "Cash in the millions circulating via games." *Investor's Business Daily*. December 23, 2010.

the longest running communities. The game centers on players known as residents

source: www.secondlife.com

interacting in their virtual world with other humanlike Avatar characters. The avatars would move around in an imaginary world that can nearly replicate real life. While they are interacting, they can trade or buy virtual items like houses and jewels with the game's own currency called the Linden dollars. Due to supply and demand, the exchange rate fluctuates and at one time, a few hundred Linden dollars can be traded for one real life U.S. dollar in our world. With real life game environment, Second Life has spread like a wildfire since it launched, and there seems to be no limit to the virtual goods, services and assets that one can buy inside the game. Over the years, not only has the game producer made money, hardcore players have also financially benefited by selling others virtual products and services in the virtual game world.

An often-quoted example is the famous Anshe Chung, the virtual land baroness, who became the first real US dollar millionaire in Second Life. Her real-

world persona, AilinGraef, explained that "her fortune was achieved by beginning with small- scale purchases of virtual real estate, which she then subdivided and developed with landscaping and themed architectural builds for rental and resale. Her operations have since grown to include the development and sale of properties for large-scale real world corporations and led to a real life spin-off corporation called Anshe Chung Studios, which develops immersive 3D environments for applications ranging from education to business conferencing and product prototyping." [8]

With the potential to convert virtual currency into real money, Second Life has not only made millionaires in real life, but it has also created a very good potential for laundering criminal proceeds. To use the game as a money-laundering tool, a player can simply use any stolen credit or prepaid card to purchase online money, which could then be used to redeem for virtual items or actual money with another player in a different country and with its local currency. Such a scenario has offered new opportunities for transferring funds anonymously, and has made room for evading detection of law enforcement and taxing authorities as well. In most cases, all that is required to open an account is an unverified name and verified email address. Should stolen credit cards be used, Second Life claims they would absorb the value and end the paper trail. As in many other MMORPGs, a launderer can open up numerous separate virtual accounts, all with fictitious identification. These accounts can all be funded by the proceeds of crime using prepaid cards. The launderer can then make purchases in the virtual world to and from himself by using those accounts as if he or she were purchasing assets from other residents. Subsequently, the same individual may direct all the proceeds to a designated account. Withdrawal of funds can then be from made at a local bank or ATM, and by that time, it would be nearly

[8] Hof, Rob, "Second Life's First Millionaire," Bloomberg Businessweek, accessed on May 7, 2013 from http://www.businessweek.com/the_thread/techbeat/archives/2006/11/second_lifes_fi.html.

impossible to trace the source of those funds. Therefore, without proper policing, games like Second Life can turn out to be a convenient channel for money laundering.

Online Social Games

Unlike MMORPGs, the world of online social games is typically reserved for casual gamers. In the past five years, this segment of market has exploded in size, volume, and visibility. Nowadays, it has impacted many people's lives, and even has the potential to reach billions of people. "Facebook alone has one billion active monthly users, more than 600 million of whom use Facebook mobile products. Twitter has more than 140 million active users who are tweeting at a rate of nearly 350 million tweets a day. And LinkedIn, reportedly the largest professional networking site, has more than 185 million members in over 200 countries and territories."[9]The demographics of these millions of active social network users cover a wide range of ages. "A 2011 study by the Pew Institute found that 83 percent of those who are 18 to 29 years of age, 70 percent of those 30 to 49, 51 percent of those 50 to 64, and 33 percent of those 65 and older are social network users."[10] With such widespread adoption, it is not surprising that the use of social sites has become the dominant way people spend their online time. With this sheer number of users, commercial activities have started to pick up, but what come along with these are opportunities as well as a range of potential risks. Online commerce activities can take place in various forms. In the case of sale of goods or services, conventional methods such as card payments and PayPal are commonly used. However, as the business pie grows bigger, alternative payment methods such as Linden dollars,

[9] Bradford, Terri, "Where Social Networks, Payments and Banking Intersect," Federal Reserve Bank of Kansas City, accessed on May 8, 2013 from http://kansascityfed.org/publicat/PSR/Briefings/psr-briefingdec2012.pdf.
[10] Ibid.

Facebook credits and, etc. have started to emerge. Unfortunately, these new mediums of exchange are not always subject to the same level of regulation as our current traditional methods.

How does commerce take place in online social games?

The nature of commerce on social sites varies. In the simplest case, commerce may involve the purchase of "virtual goods" in games. Transactions can range from the purchase of real goods from "storefronts" on social network sites, to those from the use of social media to make payments between members. As social networks grow in number and popularity, innovative features such as the ability for players to sell items to each other for virtual currencies has become available. Similarly, the purchase of in-game items for real-world currency and exchanges of real-world currencies for virtual currencies has also started to become a key feature offered by many leading social networks and online game operators.

Virtual goods and micropayments

A popular activity among users of social networking sites is to play games. While games are usually free to play, players are often given the option of purchasing goods to enhance their gaming experience and to increase their chances of success in the game. A key feature of these virtual goods is that each purchase is of small value and can be afforded by almost all individuals who socialize online. Because payments for virtual goods are usually in the form of micropayments, payment methods differ than those used for online purchases of real goods and services. Unlike traditional payment methods of card payments and bank transfers, which require sellers to pay a fixed processing cost for each transaction, many social games allow players to pre-

fund their accounts ahead of time. Under this arrangement, there is usually one initial top-up cost when a player adds funds to the account, rather than for every time a virtual good is purchased. These micropayments are growing in popularity and according to a research done by Javelin Strategy and Research 2011; "revenue in the United States from virtual goods in the 2012 was projected to be $2.4 billion, more than double the revenue from 2010."[11]

Aside from the exchanges of real currency for virtual money, consumers can also pay for virtual goods with rewards earned by participating in online promotions. Over the years, I have come across my share of online advertising companies trying to link up consumers like myself to game providers seeking to monetize their games. Typically, the player would be asked to participate in a promotion, and the game provider would then add an agreed- upon amount of virtual currency to the consumer's account.

Purchase of real goods from social storefronts

With the growing popularity of social networking sites like Facebook, it is not surprising to find retailers rushing to set up their respective online storefronts. Retailers are beginning to realize that social networking websites can be a good place to collect information of value. Information such as the gender, age, place of residence, and language spoken can often be useful to vendors trying to improve their services, refine their marketing promotion, and most importantly create a more pleasant shopping experience. Take Facebook for example, a retailer can set up a page to promote its products and encourage users to become "fans." Once the user

[11] Ibid.

becomes a fan, the retailer can start posting special promotions on the user's Facebook page. For some, they may have a link to the retailer's website, taking users off the Facebook platform. Others may choose to operate storefronts allowing users to make purchases without leaving the Facebook platform. Purchases in these situations are usually made through payment intermediaries like PayPal. As in traditional e-commerce, the payment intermediary processes payments on the consumer's credit card and the transaction is settled between the customer and the credit card company at month end just like any other offline purchases.

Banking Services on Social Network

Aside from socializing online, banking on social networks will soon become possible. Although it is still in the developmental stage, there is a growing interest among financial institutions looking to pioneer payment services, allowing customers to send payments to their Facebook friends. "Commonwealth Bank of Australia is building an application that will allow its customers to make payments to third parties and friends through Facebook."[12] "New Zealand's ASB Bank has a mobile application that allows its customers to make P2P payments directly to Facebook friends."[13]

Implications for Payments Risk

The growth of commerce and payments on social online networks has implications for money laundering risk. With respect to money laundering in the physical world, financial institutions are mandated under their respective local laws

[12] Commonwealth Bank of Australia, Media Release, "CommBankKaching for Facebook," accessed on May 13, 2013 from http://www.commbank.com.au/mobile/commbank-kaching/kaching-for-facebook.html.
[13] Bradford, Terri, "Where Social Networks, Payments and Banking Intersect," Federal Reserve Bank of Kansas City, http://kansascityfed.org/publicat/PSR/Briefings/psr-briefingdec2012.pdf.

such as the PCMLTFA in Canada, the Bank Secrecy Act of the United States, as well as the USA Patriot Act to "know your customer" ("KYC"). Essentially, KYC requires operators to collect and analyze basic identity information, as well as monitor financial transactions against expected behavior. In the virtual world, money laundering is an emerging vulnerability that could occur as social gamers interact internationally, trading virtual goods and services. In contrast to the physical world, the KYC responsibilities of operators of virtual world are less certain. Until recently, virtual currency and/or credit are legal. In fact there are not many rules and laws on it with the exception of the United States - Unlawful Internet Gambling Enforcement Act on Internet gambling. However, "in July 2011, under a requirement of the Credit Card Accountability, Responsibility and Disclosure Act of 2009, the Financial Crimes Enforcement Network ("FinCEN"), who is tasked with the mission to safeguard the United States' financial system from money laundering, issued a rule amending the Bank Secrecy Act ("BSA") implementing regulations regarding Money Services Businesses ("MSBs")."[14] Although online social networking operators are not specifically labeled as MSBs in the context of money laundering, the new rule hinted which entities would qualify as MSBs and therefore be subject to the anti-money laundering regulations of the BSA. Given this clarification, it could be interpreted that providers of virtual currencies are MSBs and be regulated as such. Unlike the United States, FINTRAC, which is Canada's equivalence to FinCEN, stated that its AML regulations would not apply to virtual currency exchanges of any kind. What this means is that the traditional definition of MSBs in Canada would not be expanded to cover online social networks with virtual credit or currency exchanges. This is a

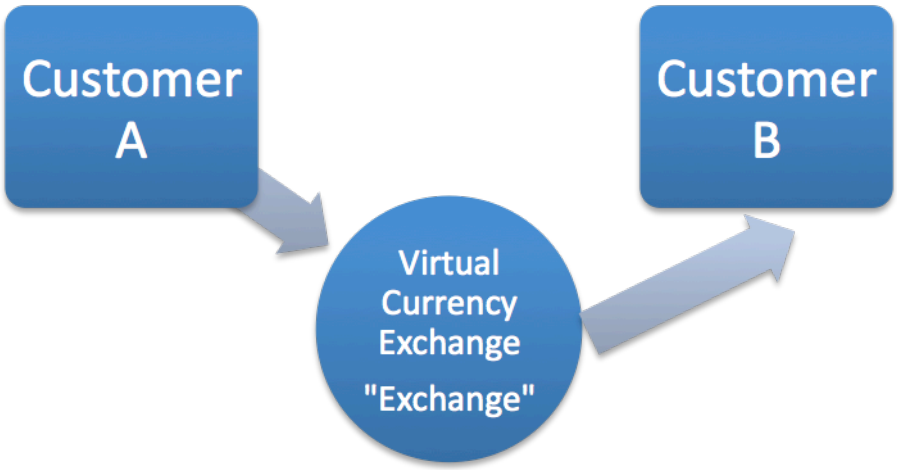
[14] *Brief summary of the Bank Secrecy Act*, FinCen, July 21, 2011, accessed on May 1, 2013 from http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf.

significant departure from that of the United States and may one day prompt virtual currency exchanges to move up north in order to take advantage of our relaxed regulatory regime. However as of today, Canada has not followed the United States' lead on virtual currency, but I believe it is only a matter of time, as the number of online micropayments and transfers grows, Canada may have to adapt to some, if not all, of the measures that our neighbor has already implemented.

What is virtual currency?

A "real" currency is a currency that is accepted as legal tender. In contrast to real currency, "virtual" currency is a medium of exchange that operates like a currency in some environments but does not have all the attributes of real currency. A simple way of defining virtual currency is that it has no inherent value other than a belief that it can be redeemed for value at a recognized rate of exchange. In particular, virtual currency does not have legal tender status in any jurisdiction in the world.

The following diagram illustrates the workings of a typical digital currency exchange operator, in which the actual payment is broken down into three separate steps, each carried out by a different party:



Step 1: Funding of the customer account: Customer A pays real money to the Exchange, who holds a certain amount of digital currency. In exchange for the money received, the Exchange transfers an equivalent amount of digital currency into Customer A's digital currency account.
Step 2: Transfer of Digital currency: Customer A instructs the Exchange to transfer a certain amount of digital currency to the digital account of Customer B.
Step 3: Withdrawal of funds: Customer B exchanges the newly acquired digital currency from her digital currency account to an equivalent amount of real money and withdraws it out.

In recent years we have seen the emergence of electronic currencies linked to virtual worlds, where online users convert real currencies into virtual currencies in order to complete purchases within the virtual world environment. As with real currencies, one can use it to layer in an AML scheme and can potentially get away. Take for example of someone wanting to pay a bribe. He or she could have paid it using airline loyalty points or through gifts. However, most corporations have disclosure rules on accepting gifts. To avoid that, the bribe could be paid by Facebook Credits, BitCoins, Linden Dollars, or Liberty Reserves. Since existing regulations behind virtual currencies are not the same as financial institutions, the payment may not be easily traced back to its source, creating a loophole that can be exploited by criminals. The real danger is that unlike real money, virtual currency has currency-like properties but not with the same intermediaries to regulate it, making it a very good tool for dubious activities like money laundering and terrorist financing activities. It is very conceivable that if regulations are not strengthened, virtual

currencies could one day become the new Swiss bank accounts, allowing criminals to park their wealth offshore where authorities have difficulties getting to.

Virtual currencies, like Bitcoin and Liberty Reserve, have taken the spotlight recently due to its recent wide fluctuation in value. Bitcoin is a virtual decentralized currency that has gained much interest since its inception in 2009. "Bitcoin is also a global payment system, allowing value to be stored and transferred anywhere, at any time, potentially anonymously with little counterparty risk."[15] According to Expensify CEO David Barrett, it solves a practical problem with international transactions, and doing business with it is "secure, instantaneous, and totally free."[16] However, due to its growing acceptance, FinCEN announced in early March 2013 hinting that every person who has ever had any virtual currency and has exchanged that virtual currency for real currency may be considered a money transmitter under the BSA. Consequentially, FinCEN has implemented a new standard for MSBs:

- Foreign-located MSBs are subject to the same civil and criminal penalties for violations of the BSA and its implementing regulations as MSBs that are stationed in the United States.
- FinCEN is aware of Bitcoin and they are actively monitoring its progress in order to determine what regulations to apply to Bitcoin exchanges or merchants using bitcoins as currency for trade.

Here is a summary of the FinCEN guidance on virtual currency:

- A person may spend money to purchase Bitcoin and then exchange the currency for goods and/or services without having to register with FinCEN as

[15] Gaming Counsel, "Canada becomes Bitcoin-friendly," Pokerati, accessed on May 13, 201 from http://pokerati.com/2013/05/canada-becomes-bitcoin-friendly/.
[16] Ludwig, Sean, "Expensify adds Bitcoin support, lets companies reimburse international workers without the PayPal fees," Venturebeat.com, April 27, 2013, accessed on May 13, 2013 from http://venturebeat.com/2013/03/27/bitcoin-expensify/#aAahOLtmtPLcsDLC.99.

an MSB.
• If a person receives real money in exchange for their Bitcoin, they may have to register with FinCEN.
• If a miner exchanges their Bitcoin for real money they must register with FinCEN.
• Anyone transacting Bitcoin on someone else's behalf must register with FinCEN.

source: FinCEN Statue, FIN-2013-G001

From the guidance, it follows that regulation can be interrupted differently depending on whether you are a user or an exchanger. It appears that people who use Bitcoin to purchase goods and services are exempted because using Bitcoin, in and of itself, does not fit within the definition of "money transmission services" and therefore is not subject to FinCEN's registration, reporting, and recordkeeping regulations. Similarly, a person who creates Bitcoin and uses it to purchase real or virtual goods and services is nothing more than a user of the virtual currency and therefore should not be subjected to regulation as a "money transmitter," which is a type of MSB. However, any user or business that exchanges Bitcoin for another currency qualifies as a "money transmitter" and must be registered with FinCEN. It goes further to say that any person who creates Bitcoin and sells the unit to another person for real currency is engaged in the business of money transmission and is therefore a "money transmitter." It follows that the counterparty to this transmission is also an exchanger and a money transmitter if he or she accepts Bitcoin and

transmits it to another person as part of the acceptance. Services to convert to "real" currency are covered as an Exchanger and are as such a MSB. With all these new classification, it appears FinCEN wants money transmitters to submit tax information, contact information, bank information, and details of the types of transactions they conduct. Accordingly, registration must be renewed every two years, and registrants are required to retain extra information as supporting documentation in the case FinCEN asks for it. Although this is United States' first step towards regulating virtual currency, I believe what this ultimately could lead to can have serious repercussion. If this is allowed to progress further, I would not be surprised in the foreseeable future we will all be required to file our virtual holdings on tax returns.

Bitcoin is an international phenomenon and Canada trades its own Bitcoin through the Virtual Exchange ("VirtEx"), a platform that allows customer to buy and sell Bitcoins with Canadian dollars. Furthermore, the platform also acts as an intermediary between the buyer and seller, providing assurance to the funds being exchanged. It was launched on June 8th, 2011 and currently operates under a registered Alberta corporation. Since Bitcoin is not yet a Canadian government recognized currency, it is up to VirtEx to ensure that all money handling laws and regulations are complied with. As such, VirtEx chooses to operate as a money service business under the law of Canada by following the FINTRAC and AMF requirement to perform KYC compliance for all its customers. This entails requesting a government issued photo ID, third party address confirmation (e.g. utility bill) within the last three months, and a signed contract for those who want to open up an account. Once the information is provided, VirtEx will call the customer directly to confirm the information given.

Liberty Reserve, an alternative-payment network and digital currency, is

another Bitcoin-like currency that has hit the news headline recently. In early June 2013, the United States federal prosecutors closed it down after being operational for five years. According to the United States' Justice Department, Liberty Reserve was "one of the Internet's largest payment processors for criminal transactions and this network has handled more than fifty-five million transactions totaling more than six billion dollars since its inception in 2006."[17] The indictment charges a group of men with money laundering conspiracy for allegedly operating a money transfer service that moved funds by means of virtual currencies. It was alleged that the system functioned like a bank, giving criminals a way to move money earned from fraudulent activities without being detected and caught by law officials around the world. To launder money in this scheme, one would simply open an account with a name and an e-mail contact. Instead of making the deposit directly into the account, one would exchange real money for Liberty Reserve currency through a number of unlicensed middlemen in countries like Malaysia, Nigeria, and Vietnam, where regulations were less stringent than those required by the United States. Accordingly, Liberty Reserve would charge a one-per-cent fee on the transactions and the exchangers would charge anywhere in the range of five to ten per cent. This arrangement was restructured so that the Liberty Reserve bank would not have record of how or where the money was sent. With all the deposits and withdrawals being done through the exchangers, Liberty Reserve was able to function like a shadow bank for criminals without being subject to the AML regimes and FATF regulations.

In addition to functioning like a bank, Liberty Reserve also served as a digital currency for criminals. Over the years, there were a number of merchants who

[17] Surowiecki, James, "Why Did Criminals Trust Liberty Reserve," THE NEW YORKER, MAY 31 2013, http://www.newyorker.com/online/blogs/newsdesk/2013/05/why-did-criminals-trust-liberty-reserve.html, accessed on May 13, 2013.

accepted Liberty Reserve currency as a form of payment for goods and services. These merchants included questionable individuals ranging from drug dealers to hackers, who knowingly engaged in transactions in which both the buyer and the seller wanted to be anonymous. For that reason, criminals traded real goods and services in exchange for the Liberty Reserve currency in large volume, making Liberty Reserve the currency of choice in a virtual world that operated under the radar of governments. This willingness and frequency of trades suggested that they were confident that the currency would not become worthless and could be converted into real currency with ease and at a reasonable price. This is fascinating on many fronts. Before the system was shut down, one Liberty Reserves currency was pegged to one U.S. dollar even though there were no legally binding rules that guaranteed that exchange rate. In contrast to its sister currency, Bitcoin, which permanently limits the number of Bitcoins in existence, there were no restrictions that could have prevented Arthur Budovsky, who founded Liberty Reserve, from further printing more currency and using it to buy illicit goods. Logically speaking, the infinite supply and lack of financial backing together are already sufficient to make this a ticking time bomb for criminals using it as a means to launder money. Now with the indictment, it appears the bombs have exploded and the whole situation has resulted in serious implications. Not only are the outstanding Liberty Reserves likely worthless now, the future of virtual currencies like Bitcoins will be forever in the spotlight, under the watchful eyes of the FATF members and government officials from around the world.

What are the legal risks with virtual currencies in online social gaming?

Essentially there are two fronts when it comes to legal risks on virtual currencies. The first is the financial regulatory law. As the use of virtual currency

increases, online social gaming operators have started to come out with their own virtual currency, allow peer-to-peer transfer, and even offer full cash redemption. As virtual currency shifts from being a prepayment for goods or services within a game environment to a widely accepted proxy for real currency or even as a means of transmitting money between various participants, online social gaming operators may need to deal with money transmitter laws and money service business laws. These laws have strict compliance obligations and costly civil and criminal penalties for non-compliance. In Canada, the laws are governed under the PCMLTFA**.**

Another area of risks is from the illegal lottery perspective. Instead of allowing users to purchase virtual currency, online social game operators may allow users to earn virtual currency through game play. Allowing users to earn virtual currency through game play that can then be redeemed for valuable virtual or real-world property presents a risk that the operator may be engaging in an illegal lottery or gambling. Simply put, most of the gambling laws today make it illegal for game operators to require a person to pay money for the purpose of entering into a promotion in which a prize may be won at the end. Any game play that involves these three elements (consideration, valuable prize and chance) is generally an illegal lottery and if taken to the extreme, may even constitute gambling. Therefore, as game operators that are involved in virtual currency, it is always best to do away with consideration and eliminate the element of chance.

How is virtual currency regulated now?

An important objective of money laundering activities is to remove the proceeds of crime from the place in which they originated. As noted earlier, this frequently involves an international movement of proceeds, which is often masked by

a series of legitimate activities. Although money laundering has become a global problem that affects many countries in varying ways and degrees, jurisdictional boundaries have become one of the biggest obstacles for AML regime. Global co-operation and coordinated efforts have therefore become essential to the deterrence, detection and prosecution of money laundering. Over the past decades, many international initiatives have surfaced to address this issue.

Perhaps the most well known of these initiatives is the FATF, which was established by the G-7 countries in 1989. The FATF is an intergovernmental body that comprises of 34 member jurisdictions and two regional organizations, for which Canada has been its member since it was established. Its purpose is to develop and promote policies to combat money laundering and terrorist financing, which are set out in the FATF 40 Recommendations and the 9 Special Recommendations on Terrorist Financing. These recommendations, in turn, determine international standards that cover its members' criminal justice system, law enforcement, as well as its financial system.[18]

In 1995, a group of Financial Intelligence Units met at the Arenberg Palace in Brussels and decided to establish an informal group known as the Egmont Group of Financial Intelligence Units, whose goal was to facilitate international cooperation. Canada has been an active member of this group since 2002. In early 2008, the Egmont Group established its Secretariat in Canada.[19]

Other international anti-money laundering initiatives include but are not limited to the following:

- European Convention on Laundering, Search, Seizure and Confiscation of the

[18] Financial Transactions and Reports Analysis Centre of Canada, "Guideline 1: Backgrounder," December 2010, accessed on May 4, 2013 from http://www.fintrac-canafe.gc.ca/publications/guide/Guide1/1-eng.asp.
[19] Ibid.

Proceeds from Crime

- Asia Pacific Group on Money Laundering ("APG")
- Caribbean Financial Action Task Force on Money Laundering ("CFATF")
- United Nations Single Convention on Narcotic Drugs
- United Nations Convention on Psychotropic Substances
- United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances
- United Nations Convention Against Transnational Organized Crime

The FATF classifies virtual currencies under New Payment Methods ("NPM") and the organization has so far issued two reports (yr. 2006 and yr. 2010) that discussed it extensively. According to the FATF's findings, despite its recommendations requiring all entities transferring money or issuing means of payment to be subject to the AML oversight, NPMs are still not applied uniformly in different jurisdictions around the world. Mainly, exceptions occur when there are several entities acting together to carry out a financial activity, making it difficult to judge which entity should be ultimately responsible to the FATF regulation. The FATF noted in some jurisdictions that certain NPMs are not subject to regulation. In others, the degree of regulation depends on the type of NPM. Regardless of the case, it appears that there is no one set of rules that can be applied universally throughout the world. Furthermore, it was also noted that third parties associated with Internet payment services ("IPS") can be regulated or unregulated entities (refer to Appendix 1). Regulated entities are subject to AML obligations and may include traditional money remittance businesses like the Western Union, prepaid card issuers or banks. Unregulated third parties are not normally within scope of AML legislation and may

include digital currency exchangers. Some jurisdictions apply the same regulatory regime to NPM service providers as they apply to traditional financial institutions, restricting NPM services only to banks or other traditional financial institutions. All in all, the FATF notices that there is no uniform application among its members when it comes to the AML regime on virtual currencies, with some jurisdictions subjecting IPS providers to the same legal and regulatory requirements as traditional financial institutions, while others restricting IPS provision only to banks.[20]

Aside from no regulations in certain jurisdictions, in countries where NPM service providers are regulated, law enforcement agencies and regulators often come across a number of legal and practical challenges in executing their duties. For example, several jurisdictions allow financial institutions to apply simplified Customer Due Diligence ("CDD") measures in low risk areas. However, there is no consensus on when a product can be considered low risk as well as to what degree CDD measures can be reduced. Furthermore, the FATF standards do not provide guidance on low-risk scenarios or related monetary thresholds specifically for NPM. Several members in their own jurisdictions have identified certain low risk scenarios in which simplified due diligence can be applied. With regard to NPMs, most jurisdictions rely mainly on transaction thresholds to define low risk scenarios, while others look at more risk factors like the cross-border functionality of a product, the funding mechanisms and the usage limits of a product. Where jurisdictions use value limits to designate low risk situations, they also differ significantly among jurisdictions.[21]

Perhaps the most sensitive area of the FATF standards is the rules dealing

[20] The Financial Action Task Force, "Money Laundering Using New Payments Methods October 2010," http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf.
[21] Ibid.

with reporting exemptions on low risk financial activities and institutions, as well as on low risk products. The current FATF standards provide some flexibility that would allow jurisdictions to apply their own exemptions. In dealing with activities of low risks, the standards give the options of a partial/ full exemption from AML regulation or a compliance with a simplified CDD. Based on this, jurisdictions are permitted to exempt from or limit the application of the standards for certain financial activities on the basis of a proven low risk and in certain justified circumstances. Such an exemption would only apply to the respective financial activity but also automatically affect all the institutions carrying out such an activity.[22]

Where a certain financial activity is not exempted from AML regulation and supervision, the FATF requires that financial institutions should undertake CDD measures. The extent of such measures should be determined on a risk-sensitive basis, allowing for the application of simplified CDD measures in cases of low risk. Although the term "simplified CDD measures" has not been defined, an exemption from CDD measures can only be granted in limited cases. Consequently, where firms carry out a designated financial activity and therefore are subject to AML obligations, exemptions from the CDD requirement will be considered a breach of the FATF regulation.[23] Overall, with so many exemptions and counter-arguments, needless to say, the current FATF standards are by far perfect, leaving many holes to fill before being able to effectively tackle the AML problem globally.

[22] Ibid.
[23] Ibid.

How does Canada deal with money laundering issues relating to virtual currency?

As a member of the FATF, Canada is active in the international fight against money laundering. The Federal PCMLTFA is Canada's commitment to the fight against money laundering and FINTRAC of Canada is at the forefront of the fight against money laundering and terrorism. Essentially, FINTRAC is an independent federal government agency reporting directly to the Minister of Finance with a mandate to detect, deter and prevent money laundering and the financing of terrorist activities. It is empowered under the Canadian federal PCMLTFA and the attendant regulations, including the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations ("Regulations"). It analyzes financial transaction reports and discloses financial intelligence to law enforcement and the Canadian Security Intelligence Service, where it has reasonable grounds to suspect that the information would lead to further investigation of money laundering and terrorist activity financing offences or threats to the security of Canada.[24]

FINTRAC is part of Canada's Anti-Money Laundering and Anti-Terrorist Activity Financing Initiative. The initiative is led by the Department of Finance and includes the RCMP, CSIS, Public Safety Canada, Canada Revenue Agency, Canada Border Services Agency, Communications Security Establishment Canada and the Department of Justice.[25]

More specifically, all businesses with nature of business that fits within the requirements set out under PCMLTFA are required to keep certain records, identify clients, maintain compliance regimes, and submit reports to FINTRAC.

---

[24] Financial Transactions and Reports Analysis Centre of Canada, " Proceeds of Crime (Money Laundering) and Terrorist Financing Act," accessed on May 14, 2013 from http://www.fintrac-canafe.gc.ca/act-loi/1-eng.asp.

[25] Ibid.

FINTRAC has the authority to issue administrative monetary penalties in response to non-compliance with the PCMLTFA and related regulations since December 30, 2008. The purpose of penalties is to ensure compliance with the law. Particularly, administrative monetary penalties serve as an adjunct to existing criminal penalties in order to avoid double penalty, as both criminal and civil penalties cannot be issued against the same instances of non-compliance. Violations are classified as "Minor," "Serious," or "Very Serious," and may carry maximum penalties of $1,000, $100,000 and $500,000 respectively. In order to avoid penalties and ensure compliance with PCMLTFA, FINTRAC regularly provides guidance to all reporting entities on how to report suspected financial transactions.[26]

FINTRAC is a very central piece of the Canadian regime on AML and it recognizes that an effective AML regime is a shared responsibility among all the FATF members. In order to effectively combat the problem of money laundering, it is important for the members of Canada's AML regime to come together, with international partners, to strengthen everyone's capacity to deter, detect and prevent money laundering and terrorist activity financing. The problem of AML is becoming more of a shared responsibility now than ever before. FINTRAC recognizes this early on by being the medium to exchange information with like bodies in other countries. It has in place information exchange agreements with certain FIUs worldwide, enabling it to provide financial intelligence to its counterparts that can be crucial to investigations of cases involving the international movement of funds. Equally, it can receive information from these FIUs, which is useful to its own analysis. Essentially, FINTRAC has the same responsibilities and functions as FINCEN, which is the United States' FIU.

[26] Ibid.

In carrying its obligations under PCMLTFA, whenever FINTRAC is satisfied that it has reasonable grounds to suspect that the information would be relevant to investigations, it has the power to disclose this financial intelligence to law enforcement and/or intelligence agencies. These agencies will conduct investigations, and if warranted, bring charges against the criminals involved. In Canada, FINTRAC would report to Royal Canadian Mounted Police (RCMP), provincial and municipal police agencies, CSIS, CRA, CIC and foreign FIUs with which the Centre has a Memorandum of Understanding ("MOU") for the exchange of information.[27]

Besides analyzing information, FINTRAC also shares the best practices designed to strengthen the support for AML regimes in other places of the world. There are five regulations under the PCMLTFA:

1. The Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations
2. The Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations
3. The Cross-Border Currency and Monetary Instruments Reporting Regulations
4. The Proceeds of Crime (Money Laundering) and Terrorist Financing Registration Regulations
5. The Proceeds of Crime (Money Laundering) and Terrorist Financing Administrative Monetary Penalties Regulations.[28]

The key objectives of PCMLTFA are to implement measures to detect and deter money laundering and terrorist-financing activities, which are very similar in

[27] Financial Transactions and Reports Analysis Centre of Canada, "Canada's Anti-Money Laundering and Anti-Terrorist Financing Initiative," accessed on May 14, 2013 from http://www.fintrac-canafe.gc.ca/fintrac-canafe/antimltf-eng.asp.

[28] Financial Transactions and Reports Analysis Centre of Canada, " Five Regulations Under the PCMLTFA," accessed on May 14, 2013 from http://www.fintrac-canafe.gc.ca/reg/1-eng.asp.

capacity to those held by the FinCEN and other FIUs around the world. Under the five regulations of PCMLTFA, the discussion of virtual currency is under the section on MSBs, which are defined in subsection 5(h) of the PCMLTFA. Accordingly, a MSB is a person or entity "engaged in the business of foreign exchange dealing, of remitting funds or transmitting funds by any means or through any person, entity, or electronic funds transfer network, or of issuing or redeeming money orders, traveller's cheques or other negotiable instruments except for cheques payable to a named person or entity." [29] Accordingly, funds are defined as "cash, currency or securities, or negotiable instruments or other financial instruments, in any form, that indicate a person's or an entity's title or interest in them," but this definition does not go further to define what "negotiable instrument" is. With no definition from neither the Regulations nor the PCMLTFA, I would think that virtual currencies would be deemed as "negotiable instrument" such that Bitcoin-like currency would be caught in the definition of funds and money services business, making it under the Canadian AML regime. However, I was pleasantly surprised to find out that FINTRAC does not view virtual currency as funds within the meaning of the PCMLTFA and the Regulations. This is significant in many ways because not equating them to transaction of funds, by means of electronic funds transfer or in negotiable instruments means that FINTRAC is taking the view that exchanges of virtual currency, either alone or in online games, should not be covered under the existing AML statutes or regulations. This interpretation can have a lasting impact with the global AML regime, as Canadian virtual currency operators are no longer required to register, identify clients, and report under the money services business rules. Because

[29] Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17), Government of Canada, Justice Law Website, http://laws-lois.justice.gc.ca/eng/acts/P-24.501/index.html.

FINTRAC has many of the same responsibilities and functions as FinCEN, this also puts Canada and the United States at two opposite ends. Being different from the United States is an interesting position taken by the Canadian regulators. Not regulating virtual currency exchanges as money services businesses could possibly make Canada as a breeding ground for virtual money-launderers.

With countries at two opposite ends, AML regulators in the United States will experience compliance difficulties when trying to exercise their authorities and this will ultimately slow down the effectiveness of the global AML initiatives. This is the case today but I suspect as the transaction volume continues to ramp up, it will only be a matter of time before the Canadian regulations are amended to include online gaming companies with virtual currency exchanges as reporting entities.

With an understanding of the law, why is virtual currency the perfect ground for money laundering?

There are many more reasons why virtual currency is the perfect ground for money laundering. the FATF sums it up relatively well in its 2010 report on New Payment Method ("NPM"). This 2010 report was a follow-up to its 2006 publication where the FATF published its first report on NPMs. The report was an initial look at the potential money laundering and terrorist financing implications of payment from personal computers and other technical devices. NPMs initiated as a relatively new phenomenon in 2006, with only a few case studies being reported. Since then, NPMs have become a more widely accepted alternative to initiate payment transactions. The 2010 report highlighted a total of 33 cases, many of which involved prepaid cards and internet payment systems. Although the amounts of money laundered varied considerably from case to case, the FATF noticed a marked increase in the number of

money laundering cases. Along with more reported cases, most of the NPM services conducted jointly with digital currency providers were outside the scope of AML legislation and therefore not subject to AML regulation and supervision.[30]

For the entities required to report, the FATF identified a number of challenges on virtual currencies, including "the absence of credit risk, speed of transactions, and the non-face-to-face nature, as key threats to AML."[31] An absence of credit risk means that online operators do not have the incentives to obtain full and accurate information on the customer and the nature of his or her business. Without a statutory reason to collect information, authorities have no way to trace the funds to its original source, making this the perfect mask for criminals wanting to hide his or her identifies. Furthermore, transactions with virtual currencies can be carried out much quicker when compared to more traditional channels. This has the potential to complicate monitoring and may slow down efforts to freeze the questionable funds. Lastly, transactions done online are typically non-face to face and this increases the chance that customers may not be who they say they are.

According to the author of the book, *McMafia: A Journey Through the Global Criminal Underworld*, Mr. Misha Glenny, online games offer a foolproof way to mask and move money from drug and other criminal activities. According to his findings, enforcement is still an uphill battle as players only meet online and can be from different countries. The fact that most players do not know their fellow game players in real life makes paying virtual money to cohorts in far-flung places and converting it into local currency a preferred choice for criminals, when compared to other means of money laundering. At the moment, most of these transactions are

[30] The Financial Action Task Force, "Money Laundering Using New Payments Methods October 2010," http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf.
[31] Ibid.

taking place below the radar of regulators and with little government oversight there is much danger of criminals exploiting these games to move cash for illegal purposes. Although there are no reliable figures on the size of such money laundering, it is believed to be substantial. According to Mr. Glenny, "the amount of real cash changing hands in virtual-world games could total in the hundreds of millions."[32]

Aside from the reasons identified by the FATF and Mr. Glenny, I find low transaction cost is a key reason for the rising use of virtual currency among criminals. In the pre-internet era, people passed physical bills through different fronts but had to pay a cut to the intermediaries who helped launder the cash. The arrival of Internet has vastly eliminated these middlemen. Nowadays when an illicit online transaction dressed up as a legitimate source gets transferred across borders, there is not much the authorities can do but perhaps to tax it at a statutory rate that is often less than the cost of transporting physical cash.

Equally troubling is the fact that virtual world has no physical boundaries and legal prosecutors face jurisdictional difficulties when trying to enforce laws to detect and prevent money laundering. The questions about who to prosecute, who to investigate and what laws to apply are often unclear, making it hard for law enforcement officials in different nations to pinpoint where an online crime has occurred. Furthermore, online social game operators are normally not within the scope of AML legislation, making them the target of choice for illicit fund transfer and money laundering. To illustrate this jurisdictional dilemma, we have a Canadian citizen in another country, who is logged onto a computer in the United States and is dealing with another player in China. Should this involve money laundering, the

[32] Tsuruoka, Doug, "Online games are new choice for money laundering," Investor's Business Daily, accessed on May 20, 2013 from http://www.policeone.com/police-technology/articles/3115040-Online-games-are-new-choice-for-money-laundering/.

question of which authorities to take action and what laws to apply can become confusing. In the end, I believe the only effective way to combat this is to have countries and law enforcement officials collectively enforced anti-crime technologies into their online games. Fortunately, companies behind MMORPGs are already increasing their efforts to help detect illicit practices. Owners of Second Life for example, have installed software controls to detect suspicious behavior in money movements. However, these measures are voluntary and done without strict guidelines. In spite of their best intentions and efforts, many questionable transactions could still take place and not be flagged out for further investigation.

Lastly, virtual world is unaffected by the laws of demand and supply, as it is a place where every physical object can be rendered in unlimited quantities. Theoretically, without finite limit, virtual items can be created and sold, allowing criminals to transfer value in unlimited quantities.

Clearly online social networks with virtual currencies have many holes that need to be filled in order to stop criminals from exploiting it. It appears many experts in the field have spoken and written about it. With terrorist bombings happening in our backyard as in the case of the Boston bombing, perhaps it is time for our government to step forward and take action to broaden its existing statues.

What are the arguments for more regulation? Should social networking operators be regulated like other money service businesses (MSB)?

The problem of money laundering has long existed and our global financial system has various protections in place to govern institutions, such as MSBs, from being exploited by criminals. The central piece of protection is the "know your customer" (KYC) requirements for wire transfers, with a de minimis exemption

threshold of a $1,000 USD. But for unlicensed entities in the virtual world, such as those exchanging bitcoins and social networking operators, there are currently no such reporting mandates.

Online money laundering can be extremely complex and may involve players implicated in transnational and covert illicit activity. What can be done to deter this problem from growing any bigger? One of the ways is to deem online social networking operators as MSBs and be regulated under the various Acts such as the PCMLTFA in Canada, the Bank Secrecy Act of the United States as well as the USA Patriot Act. Classifying online game operators as such will put them in line with regular banks and doing so may be one of the more effective ways to keep on top of increasing fraud and money laundering risks involved in the virtual worlds. According to FINTRAC, all MSBs in Canada must be registered and as part of the registration process, they have to supply information on themselves and their activities. They also have to keep the information provided up-to-date and advise FINTRAC of changes. Registration is valid for a two-year period and has to be renewed before it expires. Failure to comply with the compliance regime, reporting, record keeping or client identification requirements can lead to criminal charges against a reporting entity. Conviction of failure to retain records could lead to up to five years imprisonment, to a fine of $500,000, or both. Alternatively, failure to keep records or identify clients can lead to an administrative monetary penalty.[33] With virtual currencies in social online games growing at an astronomical rate, it appears mandated polices may be the way to go and allowing authorities such as the FATF, FinCEN and FINTRAC to monitor suspicious transactions may be a step in the right direction.

[33] Financial Transactions and Reports Analysis Centre of Canada, "Who is a Money Services Business," accessed on May 14, 2013 from http://www.fintrac-canafe.gc.ca/msb-esm/intro-eng.asp.

The argument follows whether or not it is fair to treat social networking operators as MSBs. Without a doubt, social networks and online games are intended for pleasure and if these new regulations were to be implemented, it may have a dampening effect on this whole industry from reaching its fullest potential. However, leaving it unregulated may create a loophole for money-launders to exploit. As authorities around the world continue their efforts to guard against money laundering criminals, there should be higher expectations on compliance and more penalties in failure to implement effective KYC compliance programs. Ultimately, regardless of whether social game operators should be deemed as principal registered MSBs, agents of a registered MSB, or no affiliation with any MSBs at all, we should all agree that an increased degree of KYC is needed in order to correct the current situation. If the online social channel is to reach its full potential, every interested party will need to remain vigilant and guard against money laundering risks.

What are the arguments for less regulation? Are we ahead of ourselves by treating social gaming operators as MSBs?

Although there are many arguments for implementing new regulations on virtual currencies and online social games for the sake of money laundering, I would argue that criminals need not resort to virtual worlds especially when the real world may be more suitable for their needs. One of the natural limits of online games is the low value of virtual goods and services, thus requiring a huge volume in order to sustain a worthwhile money laundering operation. Using online games for money laundering may not be efficient and cost effective.

Many experts echo this point and believe we are ahead of ourselves by treating online social games as MSBs. Professor of Economics at Johannes-Kepler-

University in Linz, Dr. Friedrich Schneider, did an extensive research on online gambling and concluded that not even online gambling can be used for money laundering purposes. Playing online gambling games like Poker through the gambling channels is not an effective way of conducting money laundering. He explained that "even if all the money that is wagered at online poker sites would be used for money laundering purposes, the total volume would still be much smaller than the opportunities offered by some other means of laundering money. As such, he concluded that it's extremely unlikely that online gaming is being used for illegal purposes."[34]

Similarly, PokerStars director of northern European operations, Sven Stiel, explained "that using online poker for money laundering purposes is technically not even possible. He pointed out that the overwhelming majority of deposits, which are made at online gaming sites, are of very small sums. Only professional online poker players make large deposits and their transactions are publicly known in the business and in the media. As such, their activities are in most cases well monitored. These large deposits and withdrawals would be detected and traced because the money transfer would have to be done using licensed banks already equipped with various anti-money laundering measures in place to detect any type of fraudulent activity. Likewise, it is only possible to withdraw real money from a poker room after players verify their identity. This is another reason why anonymously transferring money using online casino site is not technically possible. There will always be records detailing the nature of a transaction in case of an investigation."[35]

---

[34] Mills, Michael, "EU Experts – Online Casinos cannot be used for Money Laundering," Online Casino Advice.com, accessed on May 15, 2013 from http://www.onlinecasinoadvice.com/news/eu-experts-say-that-online-casinos-cannot-be-used-for-money-laundering/.
[35] Ibid.

Experts like Mr. Schneider and Mr. Stiel believe online gaming such as poker and gambling is as safe as any other mainstream offline gaming activity. Placing restrictions on online gaming is not a solution to the growing money-laundering problem since fraudulent offshore operators would still have access to the market. Instead, more vigilance in the conventional channels of combating money laundering may be the right way to go forward.

What are the key takeaways? What is the impact of virtual currencies on FINTRAC? How will the work of AML specialists involved be affected?

I hope that by writing this paper, one can begin to appreciate the volume and variety of the money-laundering challenges that are currently faced by our investigators and prosecutors. As the FATF and other international bodies continue to battle real-world money laundering, criminals will also endlessly seek new ways to attack areas of weak AML jurisdictions, for example. The makers behind virtual world gaming and online social gaming have successfully built a virtual city that has everything in it, ranging from shopping, commerce, to entertainment; but a virtual police force has unfortunately been neglected. This lack of policing is reason for the need of more rules, regulations, and laws to protect our financial integrity. In the end, regardless of how small each transaction is, whenever money is exchanged, there is the possibility of it being exploited by criminals. Hence, rules and regulations should be enforced and adhered to at all times, even in a virtual world. Since the FATF is the main inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing, I believe any kind of change should start from them. With coordinated efforts and strict enforcement, it is my sincere wish that the recommendations made here could one day

become the global AML standards.

Here are my recommendations to the FATF:

- The FATF should follow FinCEN's earlier enforcement by treating all virtual currency exchangers and providers, as well as all online game operators with virtual money exchanging services as MSBs.
- All online trades between players should be logged by game operators and submitted to their respective FIUs.
- All transactions should be made a matter of public record in the game. Game operators that exchange virtual goods for real world money, regardless of size, should be required to keep records of buyers and sellers. Limits should be placed on players' balances of virtual currencies, volume, as well as value of transactions over time. Drawing reference from the real-world KYC requirements of wire transfers with a de minimis exemption threshold of a $1,000 USD, the threshold for online casual games could be set at $500 USD and at $1,000 for MMORPGs and other virtual world games.
- Valid identification should be obtained from online game operators. After all preventive measures are the most effective tools in the fight against money laundering. Criminals will likely become more cautious to using virtual worlds to exchange value when their transactions become traceable and linked to authorities with the powers to punish the acts of crime. Currently, much is at stake as "online" continues to dominate our lives, but much more is yet to be discovered. Only by narrowing the focus to money laundering and making the connection between the transaction and the person controlling the account can money laundering be effectively deterred.

- All online gaming operators should be licensed by regulators as they are currently not. Those licenses should link the operator's bank account with the users of virtual worlds, making it extremely difficult for virtual currency to be passed within the virtual world without monitoring. This operational supervision can be managed at many points in the delivery chain. For example, in order to open up an account, the game operator must request from the gamer a government issued photo ID, third-party address confirmation (e.g. utility bill) within the last three months, and a signed agreement that details a list of penalties in response to criminal offenses such as money laundering. Once the information is provided, the game operator must call the customer directly to confirm the information given before the account can be activated. Furthermore, monitoring should also go beyond the account opening stage. All game operators with virtual currency exchanges should function like a MSB, with an obligation to monitor and report all suspicious transfers and trades beyond the earlier suggested de minimis exemption threshold (i.e. $500 USD for online casual games and $1,000 USD for MMORPGs and other virtual world games). The FIUs from the respective jurisdictions will be tasked with the job of analyzing suspicious transactions and be asked to take action on the individuals suspected of money-laundering crimes. Administrative penalties and criminal prosecution will be issued to the game operators for non-compliance, just like any other MSBs in the real world.

While it is crucial to address the money laundering risk that online game operators pose, we should also take into account and balance the risk that games will vanish if they are saddled with MSB-like measures under the current AML regime.

Pushing this envelope too far may lead to a new form of underground games that are less co-operative with authorities and harder to regulate. With that in mind, I believe authorities like the FATF should start having a dialogue with all the major online game operators, and help them phase in these new initiatives in an orderly way. In the end, co-operation among game operators, nations, and law enforcement officials within each jurisdiction, becomes critical to stem the rising threat of money laundering.

Here are my recommendations to FINTRAC:

There is no question that the global AML regime is producing tangible results. In the virtual world, however, the same regime has yet to take shape. From the facts highlighted so far, we know that money is still being laundered in the online world. Our neighbor, United States, has already started to tackle this problem by hinting to include operators of virtual currency exchange as MSBs, but Canada is still sitting on the fence of this emerging issue. The fact that FINTRAC does not currently view Bitcoin-like currency as "funds" within the meaning of the PCMLTFA can slow down or even halt the progress of an otherwise aggressive interruption taken recently by FinCEN on MSBs and its impact on the global AML regime. To understand the potential danger of excluding virtual currency exchange as a MSB under FINTRAC, let us consider the three scenarios below in the context of an online gaming environment:

- Scenario 1) Exchanges between players—If player A sells to player B a game item for a certain amount of digital currency, there is no remittance or transfer of funds by the game operator. FINTRAC would generally view this exchange

as a simple purchase or in-game transfer that is facilitated by the game operator.

- Scenario 2) Exchanges from reserves—If player A buys or sells virtual currency from the reserves of the game itself, then there is still no remittance or transfer of funds by the exchange. This is simply an exchange of virtual goods for money with no currency conversion. In this case, the foreign exchange rules would not apply and the game would not be an MSB within the meaning of the PCMLTFA.
- Scenario 3) Should the situation change so that the online game becomes an intermediary step between two fiat currencies, the transaction would not fall under a foreign exchange, nor would it be subject to the MSB rules since virtual currency is not defined as "funds" under the PCMLTFA. Here is an example: Player A transmits Canadian dollars to player B, who then converts them into a game currency. As part of the transaction, the game operator allows player B full cash redemption in a different currency (i.e. UK pounds sterling). Unlike a real-world foreign money transfer, this series of transfers would not show up as a foreign exchange transaction and the game operator would not have to comply with the MSB rules.

This last scenario helps to highlight the problem of not viewing virtual currencies as "funds" within the meaning of the PCMLTFA and the Regulations. Since this type of exchange of virtual currency for real world dollars is already an integral part of most online gaming environment, by treating digital currency like foreign currency would in fact make more conceptual sense. The Canadian view today is that virtual currency-for-Canadian dollar and vice versa exchanges are

generally outside of the ambit of the PCMLTFA mainly because this statutory and regulatory structure was drafted before digital currencies were invented. This current posture by FINTRAC could lead to a number of money laundering risks that, if unaddressed, may draw the FATF's attention. The FATF monitors and periodically reports on every country's anti-money laundering and counter-terrorist financing regimes. The FATF may bring immense pressure on Canada through its membership, requesting it to change its laws or at least curtail its current practices.

With or without pressure from the FATF, I believe the 2013 Boston bombing is a vivid reminder to our government that they must take action now to stop the flow of criminal proceeds from being used for terrorist financing. Deterrence has always been one of the more effective tools of the Canadian AML regime. In fact deterrence is the most long lasting as it has the potential to change the behavior of those who choose to abuse the system. At the end of the day, regardless of whether online game operators with virtual currency exchanges are MSBs or not, something more must be done now. It is evident that there is an urgent need for FINTRAC to catch up to this increasingly complex virtual world. As simple as client identification that can be verified, at the point of account opening, can create a measure of deterrence as it removes anonymity and creates a paper trail that can be referred to later. Since FINTRAC is already a specialist in the collection and analysis of large volume of financial intelligence, it is in a unique position to offer assistance and take charge of this initiative. The existing compliance program at FINTRAC is designed for deterrence by helping to ensure that reporting entities meet their legal obligations. FINTRAC can simply extend this requirement to all online game operators without officially classifying them as MSBs. Given FINTRAC is already at the forefront of intelligence collection on organized crime, terrorism and other threats, I believe they

should start enforcing the KYC regime on all online game operators in Canada, and report all questionable series of transnational transactions, regardless of size, to FIUs around the world. The reported transactions will be analyzed, and once suspicious information is identified, prosecution can take place in the different jurisdictions around the world. Such a mandatory compliance program will be targeted towards all online game operators with servers and principle place of business in Canada. FINTRAC can work closely with them to ensure that they understand their obligations under this new KYC regime. The KYC compliance, along with the AML measures that are already in place from the FATF, will be critical to protecting the integrity of our financial system and in making Canada a hostile place for virtual criminals to operate.

More specifically, here are my recommended action plans to FINTRAC:

Undoubtedly, FINTRAC's legislation is the most important tool that can be used to strengthen and improve Canada's AML regime. With increased complexity brought on by the virtual world, we should start looking to change the law that would allow FINTRAC to better exchange financial intelligence among its peers. This will change the whole landscape and will have the potential to uplift FINTRAC's role in the fight against online currency threats. My suggested recommendations below have to do with what information can be collected, how is it analyzed, and under what conditions should intelligence be shared.

- In order to effectively tackle the problem of online money laundering, FINTRAC will need to work with its fellow members of the FATF. The quality of the intelligence it discloses to its various local and international partners must be in line with the best practices from around world. Therefore,

it should look at strengthening its relationships with them and even expand these relationships from being an information provider to a professional group that initiates compliance on new fronts. It may consider partnering up with its neighbor, the United States, in collectively defining new terms of coverage in the fight against new sources of money laundering.

- Given virtual money laundering is a new phenomenon, FINTRAC must better define, based on its analysis of the information, the risk factors that should be monitored more closely. This establishment of risk profiles by different online game operators would help to facilitate the handling of information at FINTRAC, as well as for the businesses that need to send in the suspected transaction reports. The world of online will be increasingly more of micro-payments and transfers, making the current KYC regime at FINTRAC ineffective in dealing with it. Therefore, I would like to see FINTRAC change its existing compliance program, with the goal of enhancing the transparency and objectivity of the process, including but not limited to licensing game operators as a subset of MSB. This will hopefully stimulate behavioral changes from game operators to bring forward suspected problems that pose a higher risk than others. Along with this new designation, I would also suggest the use of penalties for non-compliance on all hosting networks with presence in Canada. These penalties may range from monetary penalties to public naming, all of which can be similar to those suggested by FinCEN and other members of the FATF. This new regime is about the protection of the Canadian financial system, so for those game operators who are negligent, they should expect significant penalties. After all, the goal of any penalty system should be aligned with the highest objectives of the global AML

regime, reinforcing compliance where there is the greatest potential of risk and real danger.

- In order to effectively conduct the KYC regime, the Canadian Parliamentary review will need to address some of the limitations of its current legislation, particularly in relation to the information that FINTRAC is entitled to receive, along with the production and disclosure of intelligence. If FINTRAC were to be effective in collecting and analyzing financial intelligence, it would require a renewed focus on the quality of information being reported. In the virtual world, game operators are the first line of defense in the fight against money laundering. To start, FINTRAC would have to approach all the major game operators in Canada and provide the tools and information necessary to address the fields of data to be reported. Since this is an emerging area, FINTRAC will need new hires with expertise and familiarity in virtual gaming environment. This new team will be responsible for managing FINTRAC's relationship with all the reporting entities in the online gaming sector. Given the potentially high volume of transactions, these new members of FINTRAC will need to be vigilant in the detection, deterrence and prevention of money laundering going throughout the virtual space. A tailored engagement and regular supervision on the online gaming operators will be the key to an effective and efficient operation.
- In a world of virtual space, FINTRAC needs to brush up on the universe in which they are to enforce compliance. They need to identify and work with all online gaming operators to tailor an approach according to the risks that are inherent in each of their transactions and activities. FINTRAC will need to work with its international allies to gain a better appreciation of the numbers,

types, and level of risk associated with the online transfers and micropayments that take place throughout the world on any given day. Unless there is a collective effort, the fight against online money laundering and terrorist financing is only going to get worse. Once FINTRAC has established the risk profiles and agreed on the blueprint for an end-to-end process, they should be allowed access to the best electronic overlay to ensure a seamless flow of large volume of data expected to come in from the online game operators. This capability should allow for the electronic manipulation of data, which focuses more on value-added works such as analysis than clerical works such as data entry.

- Lastly, there should be continuous training provided to FINTRAC employees and flexible budget to help transition to this changing virtual environment.

Understandably, all or any of these suggested changes must come from the PCMLTFA. The goal here is to change the law to make FINTRAC a stronger and more effective intelligence agency in the fight against virtual money laundering.

As FinCEN and other FIUs continue to close down loopholes, money-laundering criminals may have no choice but to turn to smaller and more cost-effective transactions as ways to challenge the current AML regime. Smaller and dispersed sums are typically less visible and less tangible target, making micro-transactions the ideal method for laundering illicit funds online. With that in mind, authorities like FINTRAC will need to be ready for the challenges ahead—its analysis of financial transactions must be able to cope up with the changes in emerging technologies and methods for conducting transactions in this ever-changing virtual world. It appears that new payment systems will be an area that deserves further

examination, as criminals will constantly seek ways to avoid detection and convert criminal assets into useable currencies. New experts will need to be hired with expertise in online micropayments and micro-transactions. New analytical tools will need to be in place; these should be capable of analyzing and identifying patterns of suspicions created by social networking operators.

We as Canadians depend on the financial system in our everyday lives, and therefore it cannot in any way fail us. In order to cope with the recent advent of the online dimension, we will need to have a set of preventive measures and monitory methods that are efficient enough to ensure smooth sailing in the virtual world. It is also critical for online game operators in both Canada and abroad to follow strict compliance to the KYC regime. Otherwise, it would be very difficult to paint a complete picture of potential money laundering and terrorist activity financing in the virtual world. Canada's effort will not be alone. With financial intelligence from other members of the FATF, Canada can piece the puzzle together, and create an environment that would be increasingly hostile to those who seek to abuse our financial system. The ultimate goal is to make it harder and riskier for criminals to move their proceeds to different places, thus trapping them to inescapable situations where their wrongdoings will be caught, or where their illegal activities are forced to end to avoid themselves being prosecuted.

In conclusion, it is evident that money laundering is a high profile issue that needs to be dealt with in depth. Extending the current KYC regime to online game operators may be a step in the right direction, but like any effective compliance programs, it should be guided by a sense of responsibility. With the recent Boston bombing and the subsequent Canadian arrest, it is clear that terrorist activities are very real and close to heart. In our vulnerable world, criminals will continue to look

for ways to move money to fund their operations without being caught. Unless we shut down all possible channels, we will always have to constantly fear the threats posed by money laundering or terrorist financing. Thus, everyone has a stake in strengthening the AML regime, and we should all contribute our own efforts to make it work collectively.

Appendix 1:

The Treatment of Internet Payment Services Providers among the FATF Members

Countries	Regulation/ Licensing (Y/N)	Supervision (Y/N)	Customer Due Diligence (Y/N)	Record-keeping (Y/N)	Legally possible to use service anonymously (Y/N)
Argentina	Y	Y	Y	Y	N/A
Australia	N	Y	Y	Y	Y if under AUD 1000
Belarus	Y	Y	Y	Y	N/A
Belgium	Y	Y	Y	Y	N/A
Brazil	N	N	N	N	N
Bulgaria	N	N	N	Y	N
Canada	Y	Y	Y	Y	N
Cayman Islands	Y	Y	Y	Y	N
Colombia	N	N	N	N	N/A
Denmark	N/A	N/A	N/A	N/A	N/A
Estonia	Y	Y	Y	Y	N
European Union	Y	Y	Y	Y	Y
France	Y	Y	Y	Y	N
Germany	Y	Y	Y	Y	N
Gibraltar	N/A	N/A	N/A	N/A	N/A
Italy	Y	Y	Y	Y	Y
Japan	N/A	N/A	N/A	N/A	
Lebanon	N/A	N/A	N/A	N/A	N/A

Luxembourg	Y	Y	Y	Y	N
Macao	Y	Y	Y	Y	N/A
Mexico	N/A	N/A	N/A	N/A	N/A
Netherlands	Y	Y	Y	Y	N/A
Norway	Y	Y	Y	Y	N
Peru	N/A	N/A	N/A	N/A	N/A
Philippines	Y	Y	Y	Y	N
Portugal	N/A	N/A	N/A	N/A	N/A
Republic of America	N/A	N/A	N/A	N/A	N/A
Republic of Poland	N/A	N/A	N/A	N/A	N/A
Russia	N	N	N	Y	Y
Singapore	N/A	N/A	N/A	N/A	
Slovak Republic	Y	Y	Y	Y	N
South Africa	Y	Y	Y	Y	N
St. Vincent & the Grenadines	N/A	N/A	N/A	N/A	N/A
Sultanate of Oman	Y	Y	Y	Y	N
Sweden	Y	Y	Y	Y	N/A
Ukraine	N/A	N/A	N/A	N/A	N/A
United Kingdom	Y	Y	Y	Y	N
United States	Y	Y	Y	Y	Y

Source: The Financial Action Task Force, "FATF Report - Money Laundering Using New Payments Methods October 2010"

Bibliography

Bradford, Terri, "Where Social Networks, Payments and Banking Intersect," Federal Reserve Bank of Kansas City, accessed on May 8, 2013 from http://kansascityfed.org/publicat/PSR/Briefings/psr-briefingdec2012.pdf.

Brief summary of the Bank Secrecy Act, FinCEN, July 21, 2011, accessed on May 1, 2013 from http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf.

Commonwealth Bank of Australia, Media Release, "CommBankKaching for Facebook," accessed on May 13, 2013 from http://www.commbank.com.au/mobile/commbank-kaching/kaching-for-facebook.html.

Department of the Treasury Financial Crimes Enforcement Network, Media Release, "FIN-2013-G001 - Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013, http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.

Financial Transactions and Reports Analysis Centre of Canada, "Guideline 1: Backgrounder," December 2010, accessed on May 4, 2013 from http://www.fintrac-canafe.gc.ca/publications/guide/Guide1/1-eng.asp.

Financial Transactions and Reports Analysis Centre of Canada, Media Release, "Keynote address by Director Gérald Cossette - Financial Transactions and Reports Analysis Centre of Canada to the Canadian Institute's Annual Anti-Money Laundering Forum," accessed on May 6, 2013 from http://www.fintrac-canafe.gc.ca/new-neuf/ps-pa/2013-04-24-eng.asp.

Financial Transactions and Reports Analysis Centre of Canada, "Money Laundering and Terrorist Activity Financing Watch: October-December 2010," accessed on May 4, 2013 from http://www.fintrac-canafe.gc.ca/publications/watch-regard/2011-04-eng.asp.

Financial Transactions and Reports Analysis Centre of Canada, " Proceeds of Crime (Money Laundering) and Terrorist Financing Act," accessed on May 14, 2013 from http://www.fintrac-canafe.gc.ca/act-loi/1-eng.asp.

Financial Transactions and Reports Analysis Centre of Canada, "Canada's Anti-Money Laundering and Anti-Terrorist Financing Initiative," accessed on May 14, 2013 from http://www.fintrac-canafe.gc.ca/fintrac-canafe/antimltf-eng.asp.

Financial Transactions and Reports Analysis Centre of Canada, " Five Regulations Under the PCMLTFA," accessed on May 14, 2013 from http://www.fintrac-canafe.gc.ca/reg/1-eng.asp.

Financial Transactions and Reports Analysis Centre of Canada, "Who is a Money Services Business," accessed on May 14, 2013 from http://www.fintrac-canafe.gc.ca/msb-esm/intro-eng.asp.

Gaming Counsel, “Canada becomes Bitcoin-friendly,” Pokerati, accessed on May 13, 201 from http://pokerati.com/2013/05/canada-becomes-bitcoin-friendly/.

Geary, Joy, “Only in the Virtual World,” Anti-Money Laundering Magazine, December 2011, p. 17, http://www.amlmagazine.com.au/amlwr/_assets/main/lib90004/only%20in%20the%20virtual%20world_issue%2031_dec11.pdf.

Glenny, Misha, *McMafia: A Journey Through the Global Criminal Underworld.* Vintage; Reprint edition (April 7, 2009).

“Government Compliance,” Charles Currency Exchange, http://charliescurrency.ca/cce_gover.html.

Grubb, Jeffrey, “Riot Releases League of Legends Beta Client for Mac,” Venturebeat.com, March 1, 2013, 1:13pm, http://venturebeat.com/2013/03/01/riot-releases-league-of-legends-beta-client-for-mac/, accessed on May 15, 2013.

Hof, Rob, “Second Life's First Millionaire,” Bloomberg Businessweek, accessed on May 7, 2013 from http://www.businessweek.com/the_thread/techbeat/archives/2006/11/second_lifes_fi.html.

Layton, Julia, “How Money Laundering Works,” HowStuffWorks, accessed on May 15, 2013 from http://money.howstuffworks.com/money-laundering1.htm.

“London City New Area,” SecondLife, http://secondlife.com/destination/london-city-new-user-area.

Ludwig, Sean, “Expensify adds Bitcoin support, lets companies reimburse international workers without the PayPal fees,” Venturebeat.com, April 27, 2013, accessed on May 13, 2013 from http://venturebeat.com/2013/03/27/bitcoin-expensify/#aAahOLtmtPLcsDLC.99.

Mills, Michael, “EU Experts – Online Casinos cannot be used for Money Laundering,” Online Casino Advice.com, accessed on May 15, 2013 from http://www.onlinecasinoadvice.com/news/eu-experts-say-that-online-casinos-cannot-be-used-for-money-laundering/.

Money Laundering F.A,Q., The Financial Action Task Force, accessed on May 2, 2013 from http://www.fatf-gafi.org/pages/faq/moneylaundering/.

Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17), Government of Canada, Justice Law Website, http://laws-lois.justice.gc.ca/eng/acts/P-24.501/index.html.

Proceeds of Crime (Money Laundering) and Terrorist Financing Act, Financial Transactions and Reports Analysis Centre of Canada, accessed on May 2, 2013 from http://www.fintrac.gc.ca/act-loi/1-eng.asp.

Surowiecki, James, “Why Did Criminals Trust Liberty Reserve,” The New Yorker, May 31 2013, http://www.newyorker.com/online/blogs/newsdesk/2013/05/why-did-criminals-trust-liberty-reserve.html, accessed on May 13, 2013.

The Financial Action Task Force, “Money Laundering Using New Payments Methods October 2010,” http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf.

Tsuruoka, Doug. "Cash in the millions circulating via games." *Investor's Business Daily*. December 23, 2010.

Tsuruoka, Doug, “Online games are new choice for money laundering,” Investor's Business Daily, accessed on May 20, 2013 from http://www.policeone.com/police-technology/articles/3115040-Online-games-are-new-choice-for-money-laundering/.