2010

How to Tame the New Wild-Wild West: Potential Lassos for Virtual Crime

Ian Leyden
Seton Hall Law

HOW TO TAME THE NEW WILD-WILD WEST: POTENTIAL LASSOS FOR VIRTUAL CRIME

Ian Leyden

TABLE OF CONTENTS

How to Tame The New Wild-Wild West: Potential Lassos for Virtual Crime

Introduction

Online virtual worlds have become, without equivocation, as advanced, complex, and dynamic as the "real world" we grew up in. The advancements in these communities has been rapid by and standards leaving a somewhat unusual situation in their wake. As these communities continue to evolve they have, to varying degrees, come to replicate certain parts of the real world, in particular, capitalist economies. The intricacies of operating such a marketplace aside, their development has for some, served to provide a striking example of the once theoretical, and presently realized, threat due to lack of regulation.

As quick as these worlds have come into existence one might logically assume that just as they replicate the real worlds economies so too would they with at least baseline regulations however, that is not the case. Little if any efforts have been made to regulate these booming economies as consequently, the illegal activities that are actively policed in the modern day real world economy, have sprung up unchecked and to some extent unhindered in the virtual setting. In particular, virtual worlds present a ripe opportunity for money launderers and individuals or groups that seek to commit fraud – most often the type of which would be dealt with by securities regulations.

This paper seeks to examine the money laundering schemes and securities violations that have been, and if no changes are make, are likely to continue within virtual communities. The first part of the paper provides an introduction into virtual worlds, their economies, and isolated examples of the fraudulent activity already taking place in virtual worlds. Part two provides baseline information into the practice of money

laundering and then advances that understanding to explore how such activity can be executed in the virtual setting. The third part of the paper will examine how existing governmental bodies, branches, and legislation might serve to prevent and secure online communities from these types of harmful illegal activity. The fourth and final section provides some brief insight, and words of caution, for those charged with regulating virtual worlds.

Part I: Welcome to the Virtual World

Virtual worlds began to take their most rudimentary form as early as the 1970s.[1] The earliest virtual worlds were text-based, and allowed users to communicate, chat, and interact with one another by typing set commands.[2] As one might imagine the text based worlds soon gave way to graphics based worlds which serve as the foundation of modern virtual worlds.[3]

Eager to capitalize on the potential profit in this newly emerging market, the video game industry soon began relying upon the multiplayer virtual world format.[4] Until the 1990s however, the video games developed were unlike the early text based worlds in that they were not persistent. This is to say that once the game ended and the player logged, off all trace of that player disappeared and the game reverted back to its initial stage.[5] Starting towards the tail end of the 90s, and in particular with the introduction of

[1] Beth Simone Noveck, The State of Play, 49 N.Y.L. Sch. L.Rev. 1, 6 (2004) (nothing that early virtual worlds evolved out of the text-based social environments of multi-user dungeons (also known as multi-user domains or dimensions) such as MUD1(1979) or LamdaMOO(1990)).
[2] Id. (the text commands would allow a user to communicate actions to other users and thereby to act out scenes and scenarios across a distance like an online Dungeons and Dragons).
[3] Id. ("In a MUD, the fantasy is described exclusively through words, Subsequently, other designers, such as Randall Farmer and Chip Morningstar, created graphical role-playing worlds like Habitat, the first multi-user domain with a graphical interface.").
[4] Id., at 7.
[5] Id.

Ultima Online, the persistent and social aspects of early text based worlds were unified with the gaming elements of the industries, later in time, developed worlds.[6] Upon its introduction in 1998 Ultima[7] received nearly a quarter million subscriptions and its progeny, Lineage, came to attract more than 4 million; unquestionably then at this point the MMORPG (Massively Multiplayer Online Role Playing Game) boom had begun.[8]

Most recently there has been in influx of non-game play associated worlds such as Second Life, the Sims, City of Heroes, and Eve Online. These reality based games do not provide storyline or goals for their participants and instead merely serve as stage setters for participants to engage in any activity they see fit. Most often these worlds provide their users the ability to create and design a great deal of the content within the world; this would certainly include clothing, possessions, and structures.[9] In so doing, virtual world administrators ensured not only exclusivity, but also independence from game based worlds.[10] Critically though, this means that so long as bandwidth is continually provided these worlds will continue to exist, to expand, and to *evolve*.[11] (*emphasis added*)

---

[6] See generally, Viktor Mayer-Schonberger, Napster's Second Life?: The Regulatory Challenges of Virtual Worlds, 100 Nw. U. L. Rev. 1775, 1782-88 (2006).

[7] See Noveck, supra note 1, at 7 ("Ultima Online linked the graphics or video games to the social and role playing culture of MUDs to the internet in what is considered to be the first persistent, massively-multiplayer commercial success.").

[8] See MMOGchar.com, An Analysis of MMOG Subscriptions Growth Version 23.0, available at http://www.mmogchart.com/charts/ (the charts are most helpful in that they demonstrate clearly not only the meteoric rise in popularity of MMORPGs but also, and more critical to the point at hand, that it was indeed at the 1998 time period that began the MMORPG boom).

[9] See Noveck, supra note 1, at 9 (noting the dual purpose of allowing users the ability to create their own content as it fosters in world creativity and productivity while simultaneously cutting down of development costs associate with building content).

[10] Id., at 9-10.

[11] It should be noted that the reality based worlds ability to continuously evolve provides the ability for true growth and development however, it brings along with it an opportunity ripe for exploitation by means of illegal activity.

A Real Economy in a Virtual World

The developers and administrators have/had as their goal for these games, often by way of significant contributions from its users, to create and establish a very realistic world. Unsurprisingly then, as these reality based worlds come to mimic and adapt real world customs and institutions, large and productive economies have sprung up. Moreover, and undoubtedly more important to the issues to be examined in this paper, many of the virtual economies have currency which has real world monetary value. While this issue will be fleshed out later in the paper, for now Second Life can provide an illustrative example.

Second Life, relative to the other reality based games, has a robust and diverse economy all its own.[12] Second life has its own currency called the Linden Dollar ("LD") which users rely upon to purchase virtual land, and pay for goods and services. The LD is readily exchangeable for U.S. dollars at a rate that fluctuates with demand and can be monitored on the Linden website.[13] The exchangeability of LD into the U.S. dollars and back again has been one of the most important aspects to the development of private

[12] It should be noted that many commentators attriute the growth and popularity of Second Life and its economy to the rather unique stance Linden Labs takes of intellectual property. Specifically, Second Life allows its users to retain the intellectual property rights to any content which the user creates. As explained by Linden labs:

> Under Linden Lab's Terms of Service, residents retain intellectual property rights in the original content they create in the Second Life world, including avatar characters, clothing, scripts, textures, objects and designs. The result is a vibrant marketplace of Second Life content. If you create it, you can sell it, trade it, and even give it away for free, subject of course to our Terms of Service.

See, Second Life, IP Rights, http://secondlife.com/whatis/iprights.php

[13] See, LindeX Market Data, available at, http://secondlife.com/statistics/economy-market.php (as of March 2010 the exchange rate operated between 260-269 Linden Dollars to the U.S. Dollar); see also, UsableMarkets, Linden Dollars vs. Other Currencies, Mar. 16, 2008, available at, http://www.usablemarkets.com/2008/03/16/linden-dollars-vs-other-currencies/ (demonstrating that the Linden Dollar along with the Yen, Euro, and Pound appreciated in value relative to the U.S. Dollar over a period approaching four years).

enterprise in Second Life.[14] Paradoxically, the ready exchange of LD to other real world currency also provides for a ripe opportunity for wrongdoers.

The economies of Second Life and its reality based virtual world counterparts now represent a markets of significant size, and most likely power to boot.[15] More importantly, these economies are expected to grow further as more participants, hailing from the world over seek to capitalize on the fertile ground of virtual commerce.[16]

A Threat Realized: Virtual Banks and Fraudulent Investment Schemes

Virtual economies represent sizeable financial opportunity and as such have attracted quite a bit of interest and activity from both the legitimate as well as the less savory online user. It really ought be of not great surprise that the virtual worlds that strive to offer its users a realistic alternative to the real world see the rise, in some respects, in illegal activity. While the threat of criminal activity remained largely theoretical in MMORPGs developmental and initial stages, the communities in present day are sophisticated and substantial[17] enough to facilitate, if not permit, a worrying amount of

[14] See, Chris Gourlay & Abul Taher, Virtual Jihad Hits Second Life Website, Sunday Times (U.K.), Aug. 5, 2007, at 4 (while the subject of the article is tangential to the point being made the authors noted that according to Linden Labs several hundred thousand pounds a day were exchanged in Second Life).
[15] Albert C. Lin, Virtual Consumption: Second Life for Earth?, 2008 BYU L. Rev. 47, 84-85 (2008); see also, Schonberger, supra note 6, at 1788 (citing a 2001 estimate of Everquest economy as having an GNP of $135 million which at the time was equal to that of Russia); see also, Bobby Glushko, Tales of the (Virtual) City: Governing Property Disputes in Virtual Worlds, 22 Berkley Tech L.J. 507, 524 (2007) (noting that economists have estimated that the total gross domestic product of the virtual worlds exceeded seven billion dollars in the year 2008 which is comparable to the gross domestic product of Estonia or the Ivory Coast).
[16] See, Ben Quarmby, Pirates Among the Second Life Islands – Why you Should Monitor the Misuse of Your Intellectual Property in Online Virtual Worlds, 26 Cardozo Arts & Ent LJ 667, note 30 (2009) (the author notes that while Second Life is an interesting example it is by no means the most popular or heavily frequented virtual world on the market); see also, David Lazarus, Real Fear in Virtual Worlds, S.F. Chron., Sept. 15, 2006, available at http://articles.sfgate.com/2006-09-15/business/17310324_1_san-francisco-s-linden-lab-second-life-linden-dollars (noting that half of all Second Life users live outside the United States).
[17] See, Daniela Rosette, The Application of Real World Rules to Banks in Online Games and Virtual Worlds, 16 U. Miami Bus L. Rev. 279, at 285 (2008) (Referring to Professor Edward Castronova of California State University, Fullerton, who conducted an economic study in 2002 in which he estimated the average hourly wage for Norrath (the fantasy world of Sony's Online 430,000 player game, Everquest) to

illegal activity. The following examples illustrate this very point, and while they do no involved money laundering it should not require the leaping of any major intellectual hurdles to see how they could have.

In the online MMORPG EVE Online[18] a user recently set up an in-world bank. The EVE Intergalactic Bank ("EIB") as it was known, allowed players/users to deposit in-game currency and in return receive a few percentage points of interest over a given period of time.[19] The bank operated for several months during which hundreds of players deposited their money.[20] Although its unlikely to have actually occurred, the bank at least advertised loan and insurance products in addition to interest earning deposits[21] and for all intents and purposes EIB seemed every bit as real and legitimate a bank as those we walk into every week.[22] The EIB seemed a sound, natural progression in the thriving capitalist economy EVE Online fostered as it played a key role in the facilitation of entrepreneurial opportunity in the community.[23]

---

be about $3.42 and its Gross Domestic Product to be about $135 million. Moreover, if one assume the same rates for other online games, such as Ultima Online, Dark Age of Comelot, Asheron's Call, and Anarchy Online, the workforce operating in these virtual worlds would generate more than $300 million in *real* wealth every year).

[18] Eve Online, Frequently Asked Questions: Eve Basics, available at http://www.eveonline.com/faq/faq_01.asp (EVE Online is a popular science fiction based, persistent world where players take the role of spaceship pilots seeking fame, fortune, and adventure in a massive "galaxy." The game enable participants to partake in player to player conflicts where the winner cans accumulate substantial monetary rewards. The game also operates much like a system of real world corporations by enabling participants to establish commercial and capitalist ventures where they can trade virtual items for real currency.).

[19] James Grimmelman, When Virtual Banks Fail, The Laboratorium, Aug. 2006, available at http://laboratorium.net/archive/2006/08/26/when_virtual_banks_fail (noting that the interest rates "may be high by offline standards, but it's low for in-world ventures, abductively suggesting low risk. Indeed, the falling value of the ISK versus the dollar (50% or more a year) made the EIB the practical equivalent of treading water. It just beat holding useless ISK yourself and watching them depreciate.")

[20] Id.

[21] Id.

[22] Id.

[23] Id. (Grimmelman notes that "the EIB was doing what offline banks do—using its deposits to make investments, and profiting from the spread in rates of return between them. Thus, it was acting as a true financial intermediary, greasing the wheels of capitalism and, in effect, helping depositors and

EIB however, in spite of the perceived economic gains it might otherwise derive from legitimate business turned out to be an elaborate scam.[24] Whether this was the case from its inception or whether its proprietor(s) fell victim to the temptation that sat in front of them on their computer screens is unclear.[25] What is known is EIB's proprietor(s) decided to take the deposited money and run, taking away approximately 790 billion ISK (EVE Online currency) which at the time equated to about $170,000.[26] Despite the size of the fraud, EIB was an unregulated online bank, and as such its hoodwinked investors and depositors were without viable means of holding anyone liable.[27]

The economies of the virtual worlds have rapidly evolved almost entirely without a countervailing and corresponding legal system for oversight and regulation. Indeed, users can now purchase "stock" in virtual corporations and trade on in-game stock markets.[28] While the existence of these new investment schemes raises a host of issues relating to securities regulation (a topic to be examined later in the paper) the potential hazards are demonstrated via the "Nightfreeze scam."[29] The scam, set again in EVE Online, involved a user named Nightfreeze who was able to entice several other users to invests in a plan that would allow them collectively to purchase an in-game item that

---

entrepreneurs find each other. ISK were going to productive use, and presumably the economy was humming along just a little faster.").

[24] Id.

[25] Id.

[26] Id.

[27] See Id. (Grimmelman believes that the EIB bank scam cam dangerously close to actionable real world fraud and that had EIB existed in the United States and dealt in U.S. dollars the scam would indeed have been actionable. In so noting Grimmelman gets at a key hurdle to any type of regulatory structure in online worlds, that being jurisdiction.)

[28] Post of Ed Felton to Freedom to Tinker, Virtual World, Meet Terrestrial Government, available at, http://freedom-to-tinker.com/blog/felten/virtual-world-meet-terrestrial-government .

[29] See generally, Nightfreeze, The Great Scam, available at www.wirm.net/nightfreeze/ (detailed description of a small but successful fraudulent investment scheme perpetrated on the virtual community EVE Online).

individually they could not.[30] Nightfreeze's investment plan turned out to be a scam that allowed him to walk away with a real world value of $1,000.[31] Without question, Nightfreeze's scheme, had it taken place in the real world would have fit neatly into the Securities Exchange Commission's widely accepted and enforce definition of a security and thereby permit an avenue for recovery and regulation.[32]

As these two examples demonstrate, much of virtual worlds are presently unregulated in any meaningful way, allowing wrongdoers the chance to prey upon the unsuspecting or unprepared. The following section will examine how virtual worlds, and their lack of regulation, may be facilitating money laundering and what consequences it might have in the real world.

Part II: Money Laundering 101

What is it and Why do we Care?

The practice of filtering illegally obtained currency through a transaction or series of transactions in order to transform the "dirty" money into "clean" currency which can thereafter be used legitimately is by definition money laundering.[33] This process allows the reaches of a given criminal enterprise to enter the lawfully operating economy or commerce. Given the fact that good deal of money laundering goes undetected, compiling numbers on how much is actually occurring is not an exact science however,

---

[30] Id.

[31] Id.

[32] See, 15 USC §77b(a)(1) (2000); see also, Securities Act 1933 §2(a)(1) (providing that a security shall be defined as any note, stock, treasury stock, security future, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement…any interest or instrument commonly known as a "security", or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing).

[33] See, U.S. Gen. Accounting Off. (GAO), Money Laundering: Efforts in the Securities Industry, GAO-02-111 (Oct. 10, 2001), at pg 1, available at, www.**gao**.gov/cgi-bin/getrpt?**GAO-02-111** (the link provides direct route to a pdf version of the document)

Congress has estimated that money laundering may amount to 2-5 percent of global gross domestic product.[34] Officially speaking, Congress states that money launderers subvert legitimate financial mechanisms and banking relationships by using them as protective covering for the movement of criminal proceeds and the financing of crime and terrorism.[35] Congress continues to maintain that in so doing, money laundering threatens the safety of United States citizens and undermines the integrity of United States financial institutions and of the global financial and trading systems upon which prosperity and growth depend.[36]

To be sure, money laundering is most often a diverse and complex process but at its core is comprised of three independent steps that may or may not occur simultaneously.[37] The initial process, through deposits or other means, of placing unlawful cash proceeds into traditional financial institutions is known as "placement."[38] The next step, "layering", is the process of separating the proceeds of criminal activity from their origin through the use of complex layers of financial transactions.[39] "Integration," the final of the three stages is the reintroduction of the money into the economy through the use of apparently legitimate transactions that serve to disguise the

[34] See, Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No 107-56 115 Stat. 272 (2001) [hereinafter "USA PATRIOT Act] (to provide a more concrete understanding of just how much money laundering Congress is estimating with their global GDP figure, it would likely land in the $600,000,000,000.00 category); see also, Computer, Telecommunications Skills Will Drive Future World Crime Waves, Money Laundering Alert, Apr. 2001, at LEXIS/Banking/General News & Information (estimating this same number to be closer to $2trillion annually and between $100-300billion in the United States).

[35] Id.

[36] Id.

[37] See, Comptroller of the Currency, Comptroller's Handbook: Bank Secrecy Act/Anti-Money Laundering (September 2000), at 2 [hereinafter Comptroller's Handbook].

[38] Id.

[39] Id. (Examples of transactions that are most often used in the layering stage of money laundering include converting cash into traverlers checks, money orders, wire transfers, letters of credit, stocks, bonds, or purchasing valuable assets such as jewelry or art.).

illegal funds.[40] To the extent a criminal is successful in these processes their money is essentially "washed" and presumably will be used to continue some facet of the criminal enterprises and will do so without arousing any suspicions by law enforcement.

Money laundering is a critical component of any type of continuous organized criminal activity.[41] Organized crime, in a general sense, would be unable to bankroll its ongoing criminal activities without the access to the legitimate financial systems that money laundering forges for illegal/dirty funds.[42] Furthermore, money laundering permits the criminal enterprise to move, hide, and secure against confiscation by authorities of potentially enormous amounts of wealth.[43] Logically then, money laundering might permit any criminal enterprise to escape the reaches of law enforcement but most recently, and no doubt most worryingly, it has become closely associated with international crime and terrorism.[44] Indeed, the investigations into the September 11, 2001 terrorist attacks of sparked a turning point for anti-money laundering legislations in the United States.[45]

The increased regulation, scrutiny, and transparency in the financial system has forced criminals to develop new and more creative ways to clean their money to avoid detection.[46] By structuring transactions below certain reporting thresholds, mixing illegal

---

[40] Id. (The Handbook provides a non-exhaustive list of financial transactions that are often used in the integration stage which includes sham loans or false import/export invoices.).
[41] See, Andres Rueda, The Implications of Strong Encryption Technology on Money Laundering, 12 Alb. L.J. Sci&Tech. 1, 8 (2001).
[42] Id.
[43] Id.
[44] Id.
[45] Id.
[46] See, Selena Nelson, Note, Regulating Money Laundering in the United State and Hong Kong: A Post 9-11 Comparison, 6 Wash. U. Global Stud. L. Rev. 723, 726 (2007) (Because money is most vulnerable at the placement stage, U.S. legislation has focused here by regulating financial institutions. Regulations including "Know Your Customer" identification requirements, Currency Transaction Reports for amounts

funds with the legitimate funds of a cash intensive business (e.g. restaurant, hotel, casino), or using trade based money laundering techniques criminals have quickly adapted to the change in law.[47] Criminals that have the financial necessity to launder money have demonstrated an intelligence beyond that of the common criminal. One would imagine however, that if presented with an equally effective and less restrictive method to clean their money they would justifiably jump at the opportunity. The lack of regulation combined with the interconnectedness on a truly global scale, of virtual communities might provide such an avenue.

Money Laundering via Virtual Worlds and Their Banks

In what has been coined "Real Money Trade" ("RMT") within the industry, individuals can exchange virtual items or currency for offline, real world currency.[48] Most often this exchange takes place by way of internet banks, internet auctions, and increasingly via the mechanics of the virtual worlds themselves.[49] This exchange is made possible through the notion, which the EIB and Nightfreeze scam ought to have at least impliedly made clear, that virtual property (e.g. land, buildings, items, or currency) has developed a real world value. And, quite naturally that real world value is something individuals are now seeking to capitalize upon.

Second Life alone reports that it handles over $400,000 in virtual currency each day, supports several thousand businesses, and in certain cases has allowed entrepreneurs

---

over $10,000, and Suspicious Activity Reports aim at destroying criminal anonymity and detecting illegal funds).

[47] Id.

[48] See Gregory Boyd & Matthew E. Moersfelder, Global Business in the Metaverse: Money Laundering and Securities Fraud, The SciTech lawyer, Winter 2007, at 4.

[49] Id.

to earn over $200,000 per year in real world income.[50] Taking a wider vantage point, certain reports estimate the value of RMT transactions on an annual basis to be in excess of $200million.[51] The numbers, aside from being staggering for such a recent phenomena, demonstrate the RMT is potentially a viable and avenue for money laundering.[52]

People that are in possession of illegally obtained money will always be seeking means by which to legitimize the funds so that they can be spent safely. While doing this has traditionally meant the funneling of dirty money through brick and mortar institutions, RMT makes available a new, more efficient, and more direct means to launder money.[53] The traditional means of money laundering have required the need to physically relocate money over borders, requisite taxation, and compliance with reporting standards for businesses and financial intuitions.[54] Consider the following example illustrating how an overseas criminal might transfer large sums of money across borders into the United States:

> First, a foreign criminal buys $500,000 worth of virtual currency for a certain virtual world. Depending on the virtual world, it is possible to purchase through third parties with minimal recording of the transaction and the absence of personally identifiable information required for an international wire transfer. After the criminal obtains the virtual currency, he can gain access to the virtual world and distribute that currency to two other player accounts. One account is for an associate in New York; the other for an associate in Los Angeles. Those associates can now use a third-party transaction to "cash out" that virtual currency.[55]

---

[50] See, Rosette, supra note 17, at 290 citing Peter Yellowlees, Virtual Online Worlds: Living a Second Life, The Economist, Sept. 30, 2006 at 77-8.
[51] See, Boyd, supra note 5.
[52] Id.
[53] Id.
[54] Id.
[55] Id. (The authors note that there is no reason the recipients have to be in the United States and that the sending party and the receiving parties can be almost anywhere in the world. It is also possible, although it only adds what might be unnecessarily precautionary steps, to convert currency into virtual worlds or to go

The transaction described above has allowed a sizeable amount of money over international borders with no governmental regulation or reporting, little if any risk, and can usually completed in less than 24 hours.[56] It is frequently the case that the virtual game hosts themselves maintain no record of transactions and so the practice of such record keeping by the banks themselves would unlikely,[57] unnecessary, and potential unwise.

The individual structural make up of each virtual world is often critical in determining whether or not it is suited for money laundering. Not all virtual worlds allow virtual currency and those that do can be separated into games which have sanctioned and those that unsanctioned currency trades.[58] Worlds with unsanctioned currency trade often contain third party intermediaries operating on a black market within the world and consequently transactional costs increase to process currency into and out of the virtual world.[59] On the other hand, some worlds sanction the currency trade and will even process the transaction itself.[60] Regardless of whether the currency exchange is

---

though multiple virtual worlds or accounts but in so doing some of the efficiencies of moving money in this manner will obviously be lost.).

[56] Id. (It should be noted that despite taking funds from outside the United States in this example and funneling them in that the process at no point involved a bank, speaking to anyone, travel, and it is unlikely that any tax or game records of the transaction exist.).

[57] Id.

[58] Id., at 5.

[59] Id.

[60] Id. (In the instances in which the virtual world operators sanction a currency trade in addition to processing transactions which take place there is normally a fee associated. Most often that fee is minimal and almost certainly less than the cost to conduct a similar transaction via a third party intermediary operating on a currency black market in a world with an unsanctioned currency trade. The only potential downside to this type of transaction is the increased level of traceability. The lack of a third party intermediary for the exchange means that currency will mean a more direct transaction with fewer steps from start to finish.).

sanctioned or not early research indicates that currency can be moved with an efficiency ranging between 90 and 98 percent.[61]

Part III: Fixing the Problem

Clean-As-You-Go: Regulation from the Inside

Historically speaking the notion of regulation through the efforts of the game developers themselves has been unwelcome. Game developers have put forth several arguments in support of their "hands-off" stance. Some have argued that online games are merely games, and thus people who invest in them lose nothing of real value.[62] Others have proffered a "swim at your own risk" response stating that people who invest in online games understand that nature of the games and do so at their own risk.[63] Certain commentators posit that the relative lawlessness experienced in certain virtual communities is a direct result of this shortsighted approach taken by game developers.[64]

Despite being late to respond, some game developers have taken a more proactive approach. Second life for example, does not allow users who have been registered for more than forty-five days from trading more than $2,000 worth of virtual currency inside of a thirty-day period.[65] Further still, in August of 2007 Second Life banned gambling following an Federal Bureau of Investigations ("FBI") examination into virtual casinos.[66]

---

[61] Id.
[62] Id.
[63] Id.
[64] See Grimmelman, supra note 19.
[65] See, Rosette, supra note 17, citing Second Life, http://www.secondlife.com
[66] See, Adam Pasick, FBI Checks Gambling in Second Life Virtual World, Reuters, Apr. 4, 2007, available at, http://www.reuters.com/article/technologyNews/idUSHUN43981820070405?pageNumber=1&virtualBrandChannel=0; see also, Rachel Konrad, "Second Life" Bans Gambling, ABC News, Aug. 2, 2007, available at, http://abcnews.go.com/Technology/story?id=3440536&page=1; see also, Posting of Robin Linden on Official Second Life Blog, available at http://blog.secondlife.com/2007/07/25/wagering-in-second-life-new-policy/ .

While it is likely that Second Life's invitation to the FBI and the subsequent abolishment of gambling was spurred by political pressure, they nevertheless took critical steps to prevent illegal activity, and in this specific matter cut off a potential route for money laundering.[67]

Relying exclusively on regulation and enforcement by internal administrators or owners would not however, be a practical solution. Beyond the problem of policing an economy of such volume, certain technologies may stand in the way of effective reporting. Initially, Linden Lab required users to provide a valid credit car or Paypal account, or to respond to a cell phone SMS text message, in order to open an account.[68] As it stands now, and how it has been since June 6, 2006 users can create an account with nothing more than an e-mail address.[69] In the event that authorities are in search of a suspicious transaction from likely terrorists, Linder Labs would be unable – assuming that the user registered after June 6, 2006 – to provide even so much as a name. While there might still be the potential that Linden could provide the user's IP address a variety of software companies have widely commercialized programs that allow users' computers to generate a new IP address each time they sign on.[70]

---

[67] See, Susan W. Brenner, Fantasy Crime: The Role of Criminal Law in Virtual Worlds, 11 Vand. J. Ent. & Tech. L. 1, at 59 (2008) (In 2007 Europol and the United Kingdom's Serious Organized Crime Agency voiced concerns that criminal ands terrorists were using Second Life to launder money. Only a few months prior, Britain's Fraud Advisory Panel identified a growing risk of theft, fraud, money laundering, and tax evasion in virtual worlds. In 2008, after Second Life had abolished gambling, U.S. Attorney General Michael Mukasey stated that Second Life, and other virtual communities, had created new avenues for money laundering.).

[68] See, Posting of Robin Linden to Second Life Blog, https://blogs.secondlife.com/community/features/blog/2006/06/28/update-open-registration

[69] See, Posting of Wagner James Au, http://gigaom.com/2007/07/04/second-life-avatar-sued-for-copyright-infringement/; see also, Second Life, Registration Page, available at https://join.secondlife.com/?ref=eurobestshop.info (link provides the actual page prompted upon a person seeking to register in Second Life and demonstrates that only an email address is required).

[70] See, Posting of Wagner James Au, supra note 70; see also, CNET download search "Hide IP", http://download.cnet.com/1770-20_4-

Virtual world administrators and operators are not without options. Assuming that a virtual world in fact has currency and furthermore a currency exchange operating, both the structure of the exchange and a currency cap can serve as effective tools to combat money laundering. Certain online worlds have established exchange rates which will rapidly deteriorate as the amount of virtual currency sold increases.[71] Consequently, if a money launderer was attempting to transfer virtual currency back out into real world currency, whether he decided to do so all at once or spread over several transactions, the cash out value would be significantly reduced. Naturally, as the cash out value decreases the efficiencies of virtual world money laundering seize to exist. Alternatively, a virtual world, as Second Life has already done, can place a cap on the amount of money a registered user can exchange in a given time period.[72] Given the relative ease with which a person can register a user in Second Life one has to pause to think whether this cap is effective, in any way, at deterring money laundering. Commentators are quick to note that these methods are nothing more than undersized patches to a gaping hole. As the economies of these virtual worlds grow, larger transactions will be possible without having a dramatic shift in exchange rates thereby allowing more money to be transferred with a much higher efficiency.[73]

Virtual world money laundering even at its most basic level clearly can provide an efficiency related attractiveness to potential money launderers. As the methodology

---

0.html?query=hide+IP&tag=srch&searchtype=downloads&filterName=platform%3DWindows&filter=platform%3DWindows (A simple search into CNET for software that can hide, alter, and/or mask a user's IP address returns 102 products that might be of use many of which are available for free trials periods); see also, Gourlay & Taher, supra note 14 ("Intelligence sources said that although communications traffic though Second Life could in theory be monitored, often the only means of tracking an individual is by tacing the user's IP address – the physical location of a computer in the real world – but even this can be faked.")

[71] See Boyd, supra note 48, at 5.

[72] Id.

[73] Id.

becomes more technical, assuming it is not already, these efficiencies could increase beyond their already impressive level. The more technologically savvy criminal might employ the use of "bots" to assist his operations. A bot is a computer controlled entity functioning within a virtual world designed to simulate a human player that operates through pre-written command language or potentially low level artificial intelligence.[74] Bots have already been used to perpetrate online crimes in the virtual world Lineage II.[75] While using bots in a money laundering context would prove more complex than a petty theft ring there is no reason to think it impossible or unlikely.

The Courts: Early Signs of a Receptive "Bench"

Discussion of various applicable regulatory regimes to thwart money laundering and fraudulent investment schemes in virtual worlds would be of little merit if the judicial systems themselves were unwilling or unable to enforce. Case in point, neither the Nightfreeze, nor the EIB bank scam has led to any punishment of the perpetrators.[76] In both instances a major defense has been that they were part of a game and therefore, anyone that invested in the schemes did not, and by definition could not, lose anything of real value.[77] Furthermore, many virtual worlds state that the risk and trust necessary to operate in their "laizze-faire" style regulated worlds are a critical and identifying component of their product's experience to its users.[78] Ultimately, the question is: when,

[74] Jeffrey Bardzell, Markus Jakobsson, Shaowen Bardzell, Tyler Pace, Will Odom, Aaron Houssian, Virtual Worlds and Fraud: Approaching Cybersecurity in Massively Multiplayer Online Games, available at www.digra.org/dl/db/07311.42219.pdf.

[75] Ian Douglas, Virtual Criminals are Just Human, Telegraph.co.uk, Nov. 15, 2007, available at http://blogs.telegraph.co.uk/technology/iandouglas/3625241/Virtual_criminals_are_just_human/ ("A gang of teenagers made automated characters (known as 'bots') to live in the game, attack real characters and steal their money. In 2005 Lineage II artifacts were tradeable on eBay, so this was real violence, real theft, real crime, just perpetrated through a computer.").

[76] See, Boyd Supra note 72, at 6-7.

[77] Id.

[78] Id.

if ever, does a game become, for legal purposes, a real investment of real value albeit into virtual items from virtual worlds? The answer to this question will likely be fertile grounds for debate and controversy. To the extent it is not answered by legislative bodies around the world, certain judiciaries have already started to provide insight into the matter.

The 1st Cir. provides vital guidance for the United States courts specific to, whether they are willing to view a game as having real world significance. In SEC v. Sg Ltd., 265 F.3d 42 (1st Cir. 2001) defendant, Sg Ltd ("Sg") offered a website which hosted an "investment game" where virtual investors used offline currency to purchase shares offered by Sg in virtual companies that had no real world equivalent.[79] Sg advertised that investors could buy and sell at posted prices and to do so was without risk because prices would inevitably continue to rise.[80] Sg eventually suspended trading activity and with it the ability of any investors to withdraw funds from the game.[81] The SEC eventually filed suit alleged the "game" was within the definition of an "investment contract."[82] Predictably, Sg proffered the "game defense" positing that none of what the virtual investors lost had any real value.[83]

The District Court of Massachusetts beneath it maintained the SEC had failed to meet the summary judgment burden. The court stated that all the transactions were in the context of a game and that while participants were looking for financial gain the scenario more closely resembled gambling than an investment scheme.[84] The district court

[79] See, SEC v. Sg Ltd., 265 F.3d 42 (1st Cir. 2001).
[80] Id.
[81] Id.
[82] Id.
[83] Id.
[84] See, SEC v. Sg Ltd, 142 F. Supp 2d 126 (Dist. Mass. 2001).

provides, albeit in a well written manner, an opinion implicitly endorsing the game defense. On appeal the 1st Cir. then only had before it the issues of whether the SEC had alleged sufficient facts to survive summary judgment.[85] Reversing and remanding, the Circuit held that the SEC had in fact alleged sufficient facts to survive summary judgment.[86] In so doing the viability of the game defense is no doubt undercut as the context of an online game was insufficient for the court to view Sg's actions as nothing more than gambling but ultimately the viability of the game defense was left, on an explicit level, untouched.[87] Importantly however, the court did take the time to note that Sg's website disclaimers regarding the "rules of the game" would not be enough to dismiss the SEC complaint.[88] In doing so, the court takes a clear stance demonstrating a willingness to look beyond gaming disclaimers and to the actual actions of the parties involved and the seriousness of the consequences even when occurring in a virtual world.[89] Despite SEC v. Sg Ltd potential impact on the ability to secure convictions against virtual crime in the real world, the United States on an international level is behind the curve.[90]

---

[85] See, SEC v. Sg Ltd, supra note 79.

[86] Id.

[87] Id. (The court ultimately found that the SEC had alleged facts which, if proven, satisfied the three-part Howey test and supported its assertion that the opportunity to invest in the shares described on defendant's website constituted an invitation to enter into an investment contract within the jurisdictional reach of the securities laws.).

[88] Id.

[89] See, Boyd, supra note 75, at 7.

[90] See, Eric Weslander, Virtual-Reality Crimes Present Literal Challenge for Real-Life Police, LJWorld.com, Nov. 12, 2006, available at http://www2.ljworld.com/news/2006/nov/12/virtualreality_crimes_present_literal_challenge_re/ (Providing the example of Carissa Hill. Mrs. Hill, a resident of Lawrence, Kansas, called the local police in early 2006 because her avatar had been stolen by an online scam artist who had stolen another online character's identitiy in the game. In the scam Hill had been cheated out of Linden dollars as well and not knowing what else to do called the local police. The police, however, were unable to provide any assistance having no understanding of what to do or how to handle the matter.)

Virtual worlds are very much a global phenomenon as such examination into the more progressive laws and judicial actions taking place in other countries can serve as good indicator of what is to come on a wider scope. China has developed law designed to regulate and protect virtual interests.[91] Indeed, multiple convictions have already been secured against perpetrators of virtual theft. In 2003 a user of the game Red Moon filed suit against the game operators.[92] The user had, at great personal expense and, over a lengthy period of time gathered an array of virtual weapons, that rendered him invincible within the game.[93] A hacker then broke into this user's account and proceeded to pilfer the hard earned weaponry.[94] The user contacted Red Moon's operator who promptly refused to provide any information regarding the hackers identity.[95] In court the gaming company argued that virtual properties were simply "piles of data" without any real world value.[96] The court held that the user was entitled to compensation, in this instance in the form of the administrators returning the stolen weapons.[97]

---

[91] See, Jamie J. Kayser, Note, The New New World: Virtual Property and the End-User License Agreement, 27 Loy. L.A. Ent. L. Rev. 59 (2006).

[92] Id., at 66-67.

[93] See, Id.; see also, Jay Lyman, Gamer Wins Lawsuit in Chinese Court Over Stolen Virtual Winnings, TechNewsWorld, Dec, 19, 2003, available at http://www.technewsworld.com/story/32441.html?wlc=1269359633 (reporting that the user in this instance has amassed an arsenal of virtual biological weapons which allegedly was the culmination of more than two years of work and an investment of $1,200 USD).

[94] See, Kayser, supra note 87, at 67.

[95] Id. (It should also be mentioned that the user contacted the police in this instance as well. Despite the more progressive stance China seems to have taken on virtual property theft, and implicitly against the "game defense" theory, the police did not provide any assistance to the user in this instance. Exactly why this is the case is uncertain.)

[96] See, Lyman, supra note 89 (Interestingly the article further demonstrates that value that users of the virtual worlds place on the property and items they attain in game by citing a rash of real-world gang killings in Asia the causes of which stem from a popular game "Lineage.").

[97] See, Kayser, supra note 87, at 67; see also, Joshua A.T. Fairfield, Virtual Property, 85 B.U. L. Rev. 1047, at 1084 (2005) (the case, Li Hongchen v. Beijing Arctic Ice Technology Development Co., was decided by the Beijing Second Intermediate Court who is apparently well known for its decisions in the field of intellectual property)

Foreign governments, who because of the incredible popularity of virtual world games in their countries, have made what appears to be best efforts to address the problems of virtual crime. The Chinese Public Safety Ministry issued an advisory letter to law enforcement on how to handle and punish the theft of virtual property[98]. As early as 2004, South Korea alone had recorded over 10,000 arrests for theft of virtual property, a great deal of which resulted in convictions.[99] In the countries with the highest levels of participation in virtual worlds government, law enforcement, and more importantly, the judiciaries have taken an unequivocal stance that virtual property is of real value and that the game defense is not viable.[100]

The Feasibility of Applying Existing Regulation to a Virtual World

The plausibility, and some might argue inevitability, to the application of existing regulatory regimes to virtual worlds to get a hold of money laundering and securities violations ought be common sense. As we have seen virtual worlds, at least those which present potential problems, have duplicated with precision the capitalist market structures of developed real world nations. While the regimes to be explored bellow might appear

[98] See, Fairfield, supra note 93, at 1085 (It seems that Chinese authorities had little choice but to issue the letter given the rising increasing amount of virtual theft. Around the same time period as the Arctic Ice case the Beijing Evening News reported the sentencing of two 17-year-old boys for the theft of virtual property. Police in Chengdu were also investigating the theft of roughly RMB 50,000 worth of virtual equipment. Numerous other complaints of theft of virtual property had been filed, and the number of incidents is rising month by month.).

[99] Id., at 1088 ("A recent BBC article reported that South Korean police received 22,000 cybercrime complaints related to virtual property in the previous year - over half the total number of cybercrimes reported in South Korea. [216] A Korean newspaper recently noted that 10,187 South Korean teenagers were arrested for theft of virtual property in a single year - over 28 per day.").

[100] Id., at 1087 (South Korea and Taiwan, two of the world's most "wired" nations have developed significant legal framework for virtual crime. South Korea is commonly described as the world's "most wired society," with the greatest per-capita adoption of broadband connections. Taiwan has developed a useful and comprehensive body of case law protecting virtual property from forcible or fraudulent expropriation. Taiwanese law requires the victim of theft of virtual property to file a police complaint before prosecution can proceed. But even with that caveat, Taiwanese jurisprudence boasts hundreds of cases on virtual property covering theft, fraud, and even robbery. Since 2003, the cause of action of theft has been revised to include the taking of another's electronic record without cause. Prosecutions under this revised statute have become routine.).

somewhat disparate relative to each other, their working in concert is critical to making virtual worlds a secure financial environment. As the EIB bank scam demonstrates banking institutions are becoming, if not already, accepted business inside the presently unregulated virtual worlds. While EIB was a short lived scam the potential for money laundering or the facilitation of securities fraud might well increase with a more established and permanent virtual bank.

Money Services Businesses

The Bank Security Act ("BSA") enacted in 1970 enables the Secretary of Treasury to issue regulatory measures which require certain reports and disclosures be made by operations fitting the provided definition of a "financial institution."[101] As might be expected, financial enterprises such as banks, securities firms, and insurance companies are subject to different, and more stringent, regulation than non-financial institutions.[102] The BSA currently regulate a great deal of depository institutions, among them banks, credit unions, casinos, securities brokers and dealers, and money services businesses ("MSBs").[103]

The BSA mandates that financial institutions maintain continuous and detailed record keeping and reporting systems.[104] In so doing, the BSA has the financial institutions themselves create and keep the paper trail that serves the dual purpose of deterring illegal activity and assists law enforcement in their investigations.[105] The

[101] Financial Crime Enforcement Network, Regulatory: Overview, http://www.fincen.gov/reg_main.html [hereinafter FINCEN Reg.].
[102] See, Rosette, supra note 17, citing, Caroline Bradley, Banks in Online Games, International Finance Blog, http://intfin06.umlaw.net/?p=105.
[103] See, FINCEN Reg., supra note 97.
[104] See, Comptroller's Handbook, supra note 37, at 1.
[105] Id.

ultimate objective of the BSA's regulations is to prevent financial institutions from being used by criminals to hide, deposit, or transfer illegal funds.[106]

In a continued effort to control money laundering the Secretary of Treasury issued a series of rules to apply to the actions of MSBs.[107] In 1999 the Secretary ruled that "a business that meets one or more of the definitions of a type of MSB is an MSB" and therefore would need to comply with the applicable BSA requirements as an MSB generally, its specific type of MSB, and as a financial institution in general.[108] MSBs are defined as institutions handling business transactions including money orders, money transfers, check cashing, traveler's checks, currency dealing, currency exchange, and stored value.[109] It would seem that both online virtual banks and virtual currency exchanges (sanctioned or non-sanctioned) would nearly fit within the defined sphere of an MSB. At the very least even a rudimentary online virtual banks' activities of taking deposits, making loans, and transferring funds would facially satisfy the definition of "money transmitters."[110]

The regulatory measures ought under the BSA in general, and the MSBs more specifically, make difficult the laundering of money though virtual worlds. Among the requirements for MSBs they are required to develop and implement an anti-money

---

[106] Id.

[107] See, FINCEN Reg., Am I an MSB?, available at, http://www.fincen.gov/financial_institutions/msb/amimsb.html; see also, 31 CFR Ch. 1 Part 103 – Financial Record Keeping and Reporting of Currency and Foreign Transactions, Subpart A (uu) (this will provide the complete regulatory definition of "money services businesses.").

[108] Id.

[109] Id.

[110] Id.; see also, FinCEN Ruling 2004-3 – Definition of Money Services Business (Money Transmitter/Currency Dealer or Exchanger), August 17, 2004, available at, http://www.fincen.gov/news_room/rp/rulings/html/fincenruling20043.html ("any other person engaged as a business in the transfer of funds," is broad enough to encompass various types of money transmission including physical transportation of funds.")

laundering system ("AML") compliance system.[111] Certain MSBs are required to maintain a list of any agents they have.[112] In addition, if an MSB has suspicion, knowledge, or reasons to suspect any transaction as non-legitimate and it includes aggregate funds of $2,000 or more it must file a Suspicious Activity Report ("SAR") with the Secretary of Treasury.[113] Importantly, an MSB that provides a money transfer of $3,000 or more, or currency exchange of $1,000 or more to any customer within a period of 24 hours must maintain a record of that transaction.[114]

MSBs and other qualifying institutions, operating under the BSA, face penalties for non-compliance. Depending on the specific factual circumstances a financial institution can be required to submit up to five reports to the government. A reporting violation can carry with it civil and criminal liability.[115] Furthermore, section 314(b) of the PATRIOT Act permits financial institutions that have already provided notice to the Department of Treasury to share information with the federal government in order to identify and fend off activities that may involve money laundering or terrorism.[116] Lastly,

---

[111] See, FINCEN Reg., Money Services Businesses Home Page, available at http://www.fincen.gov/financial_institutions/msb/index.html.

[112] Id.

[113] Id.; see also, FINCEN Reg., Money Services Businesses Suspicious Activity Report (SAR), available at, http://www.fincen.gov/financial_institutions/msb/msbsar.html (the website provides the more expansive definition of what suspicious activity consists of: (1)Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity, or (2) is Designed to evade the requirements of the Bank Secrecy Act, whether through structuring or other means, or (3) Serves no business or apparent lawful purpose**,** and the reporting business knows of no reasonable explanation for the transaction after examining all available facts.).

[114] Id.

[115] See, FINCEN Reg., SAR Reporting Penalties, available at, http://www.fincen.gov/financial_institutions/msb/definitions/penalties_A.html ; see also, 31 USC §5313, available at, http://www.law.cornell.edu/uscode/31/usc_sec_31_00005313----000-.html; see also, 31 USC §5321, available at, http://law.justia.com/us/codes/title31/31usc5321.html ; see also, 31 USC §5322, available at, http://trac.syr.edu/laws/31/31USC05322.html.

[116] See, FINCEN Reg., US PATRIOT Act Information, available at, http://www.fincen.gov/statutes_regs/patriot/index.html.

it should be noted that the BSA contains pertinent language regarding foreign-based transactions.[117] Due to the fact that virtual worlds are often global in their reach the threat of money laundering from outside the boarders of the United States are most critical.[118]

The application of MSB requirements through the BSA to virtual worlds, just as it is in the real world, would not render money laundering impossible. It would however, significantly affect the efficiencies with which money laundering could be done and thereby the impetus to do so within these virtual communities. Money laundering in virtual worlds is viable precisely because of these regulations not having been implemented. Admittedly, MSB regulation is only one piece of a more complicated puzzle in preventing virtual worlds from being taken advantage of by money launderers. For regulation to truly be effective it will require the tracking of money flows, monitoring transactions, and taxation or some taxing authority of personal and business income generated in virtual worlds.[119]

Application of Securities Regulation to Virtual Worlds

The term "investment contract" operates as one of the SEC's most useful terms. Serving as a catch-all, the term extends securities laws to the non-obvious financial arrangements. Courts have been liberal in their interpretation of what satisfies as an "investment contract" limiting its reach, on a general sense, only to where there is no

[117] See, Comptroller's Handbook, supra note 100, at 7-8.

[118] See generally, Financial Action Task Force, About FAFT, available at, http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1_1,00.html ("The FATF monitors members' progress in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism.").

[119] Posting of kdawson to Slashdot, Virtual Economies Attract Real-World Tax Attention, available at, http://games.slashdot.org/article.pl?sid=06/10/16/1747235 (there has been some indication that some US and other overseas regulatory bodies are taking the initial steps towards the regulation of online income. For example, people who cash out of virtual economies by converting their assets into real world currencies are not required to report those incomes with the IRS or relevant tax authority.).

perceived investment interest/value.[120] As we have seen, the notion that what is invested in a virtual worlds is without "real value" has largely been rejected and, to the extent it retains any foothold its grip is tenuous at best.

The current test to determine whether a particular financial instrument is an "investment contract" and therefore a security was set forth in SEC v. W.J. Howey Co., 328 U.S. 293 (1946). The established test states that an "investment contract" is: (1) the investment of money; (2) in a common enterprise; (3) with the expectation of profits derived solely from the efforts of others.[121] In addition, the court stated that this test must be applied in light of the economic realities of the transaction; the substance of the transaction will govern its form.[122] The broad definition and interpretation by the courts demonstrates quite clearly that to the extent the test is satisfied the SEC will regard that product an investment contract and thereby a security.[123]

This expansive "investment contract" test taken together with the previously discussed SEC v. Sg Ltd. indicates that the substance over form framework will continue to persist in virtual worlds as well. While the court did not answer the ultimate question of whether the users of the website were paying for an investment or a game the court did

---

[120] See, United Housing Foundation Inc. v. Forman, 421 U.S. 837 at 851 (1975) (holding that shares in a non-profit cooperative housing corporation were not a security because there was no potential for realizing either dividends or capital appreciation).

[121] See, SEC v. W.J. Howey Co., 328 U.S. 293, at 298-99 (1946) (setting for the present day, three pronged, test for "investment contract").

[122] Id. ("The arrangements whereby the investors' interests are made manifest involve investment contracts, regardless of the legal terminology in which such contracts are clothed, The investment contracts in this instance took the form of land sales contracts, warranty deeds, and service contracts.").

[123] To give an idea of how wide the Howey test has been applied, and why its is likely courts willing to find them to exist even in a virtual setting, consider the following: Smith v. Gross, 604 F.2d 639, 641 (9th Cir. 1979) (finding an investment contract where the seller of earthworms promised to repurchase them and market them to farmers); Miller v. Cent. Chinchilla Group, 494 F.2d 414 (8th Cir. 1974) (finding an investment contract existed in a chinchilla breeding resale agreement); SEC v. Koscot Interplanetary Inc., 497 F.2d 473 (5th Cir. 1974) (investment contract existed in the context of a pyramid scheme for selling cosmetics).

provide some insight to what it would be likely to do.[124] As previously discussed, the First Circuit looked past the posted online disclaimers regarding the financial instruments and the parties' actions. While subtle, this move has prompted many commentators to confidently state that the court would have, and will if need be in the future, not honor a game defense while applying the Howey "investment contract" test.[125]

A Word of Caution When Regulators Come Knocking on the Virtual Door

The verbatim application of existing regulation to virtual worlds might well have some chilling effects to the economies of virtual worlds. For example, if securities laws were to be applied to virtual worlds in the exact same way that they are in the real world the end result might not be a desired one.[126] More specifically, if the SEC were to require registration of offerings in virtual worlds it would have a significant chilling affect on virtual economies. The cost of registration is most often hundreds of thousands of dollars while the amount raised in a virtual world public offering is significantly less. An IPO that occurred on the Second Life Capital Exchange offered nearly 600,000 shares at $L5.[127] This offering, depending on the exact exchange rate, generated between $11,000 – 12,000 which would be wholly insufficient to cover the prevailing cost of going public.[128] Ultimately, the enforcement of certain securities laws will deter business

---

[124] SEC v. Sg Ltd., 265 F.3d 42 (1st Cir. 2001).

[125] See, Boyd Supra note 75, at 6-7; see also, Shannon L. Thompson, Article, Securities Regulation in a Virtual World, 16 UCLA Ent. L. Rev. 89 (2009) (stating that the courts willingness in Sg Ltd. to continue to choose substance over form increase the likelihood that real world laws will be applied to virtual worlds).

[126] See, Thompson, supra note 102, citing, Benjamin Duranske, Commentary: Virtual Law Firm Hired by Virtual Company in "IPO" Stage, Virtually Blind, Jan. 6, 2008, http://virtuallyblind.com/2008/01/05/virtual-firm-hired/ (providing the specifics for the example that follows in the text above).

[127] Id.

[128] Id.; see also, David Orloff, The Price of Going Public, Orange County Business Journal, May 29, 2000, available at, http://www.allbusiness.com/north-america/united-states-california-metro-areas/1062563-1.html (IPOs can cost a company anywhere from $100,000 to a few million dollars. Including the

development, the raising of capital, and in the end the viability of continued expansion of virtual economies.[129]

Part IV: A Final Word for Our Virtual Regulators To Be

To conclude then, while this paper does advocate a quick and strong application of existing regulatory regimes it does not support such application blindly. The small scale that virtual world economies operate upon – at least relative to the economies the regulations were designed for – necessitate a thoughtful selection and adaptation of regulations. For those people charged with making these decisions they ought focus most upon those regulations that will deter and complicate schemes designed to defraud users or establish institutions to facilitate money laundering with an eye towards the unwanted potential that overbroad regulation will do much harm to a new and potentially invaluable resource in virtual worlds.

underwriter's fee, going public can cost a company up to 15% of the total amount raised in the real world economy. The amount of money raised in a virtual setting pales in comparison and as such makes it largely impossible to accomplish. In this article the expert interviewed concluded that he would find it hard to conceive a paper going public for anything under $100,000.).

[129] See, Duranske, supra note 104.