Journal of
Virtual Worlds Research
ISSN: 1941-8477

Legal and Governance Challenges

September, 2013
Volume 6, No. 3

Volume 6, Number 3
Legal and Governance Challenges
September 2013

Journal of Virtual Worlds Research
jvwresearch.org ISSN: 1941-8477

Volume 6, Number 3
Legal and Governance Challenges
July 2013

Blazing Trails: A New Way Forward for Virtual Currencies and Money Laundering

Michael Bombace
Washington and Lee University School of Law, VA, USA

Abstract

Virtual currencies grew up in virtual worlds. They were a central element in the game experience. They remain so and now represent a widespread form of value exchange on the Internet. They are an increasingly effective way to monetize games. Because of their versatility within games as part of game play and as a monetization method, they are a central tool of innovation for game developers. In tandem with their rise in use and complexity come anti-money laundering concerns. Their use for illegal acts is predicted to grow. Because of their still nascent state there is a window of opportunity to get regulation right and balance the cost of constraining innovation and online trade with the benefits of addressing anti-money laundering concerns. There is now some urgency because of recent regulatory guidance issued by the Financial Crimes Enforcement Network, a bureau of the United States Treasury Department.

This paper presents a new approach. First, a data retention policy that includes identity authentication requirements. Second, restrictions on the use of payment systems at a high risk for abuse. Third, a safe harbor granting criminal and civil immunity for good faith efforts by game companies to help reduce the cost of compliance. Absent from this proposal are suspicious activity reports, which are expensive and place a burden that is handled better, and already done, by payment systems that connect to game companies, such as PayPal, and traditional services such as bank accounts or credit cards. Virtual currencies are an important tool for game developers that in turn provide real economic development and creativity that require unique treatment in the law. Regulation will occur—the question is how it will be crafted. This paper presents a path forward in that discussion.

1. Introduction

Virtual currencies are a familiar topic in virtual world literature (Hamari & Lehdonvirta, 2010; Castronova 2008; Duranske, 2008; Castronova, 2001). They are also a familiar topic in anti-money laundering literature (Chambers-Jones, 2012; Landman, 2009). This paper advances a new narrative that builds upon these two perspectives on virtual currencies. The first view is of virtual currencies as an important tool of innovation for game developers (Hamari & Lehdonvirta, 2010, p. 23). The second view is of virtual currencies as a current and growing financial channel for criminals to exploit (Chambers-Jones, 2012, pp. 112-114). Merging these two viewpoints effectively is vital for both, and the goal of this paper. That goal is given a sense of urgency given recent regulatory developments.

Virtual currency regulation is forming in the United States with the Financial Crimes Enforcement Network's (FinCEN) recent interpretive guidance ("Guidance") on the application of current anti-money laundering regulations to virtual currencies (Guidance, 2013). The Guidance is not binding but provides a roadmap for future regulations and enforcement actions by FinCEN (Regulatory Releases, 2013). FinCEN is a bureau under the Department of Treasury tasked by Congress to protect the United States financial system from illicit use and money laundering (Mission, 2013).

The author draws an important distinction between virtual currencies and digital currencies missing in the Guidance. This paper classifies currencies that are not government backed, not part of a game mechanic, and exist online as digital currencies. Virtual currencies then are those linked to a virtual economy and/or used to monetize a game. Digital currencies are freestanding online currencies that act primarily as a money transfer service among people and entities. This paper focuses on virtual currencies in virtual worlds and other games.

The proposed solution includes three requirements applicable to all forms of virtual currencies. First, data retention logs. Second, enhanced user authentication. Third, restrictions on the use of payment systems at a high risk for abuse. In return for these requirements, game developers would receive civil and criminal immunity from misuse of their virtual currency to offset the cost of compliance. This safe harbor would be subject to a good faith requirement by game developers in implementing the requirements above and cooperating with law enforcement. This paper presents this solution first as a form of self-regulation for the game industry as the regulatory space is still forming in the United States. Self-regulation can help game companies shape the upcoming conversation with FinCEN, other regulators, and potentially limit more restrictive regulations. This is underway with other digital currencies such as Bitcoin, Ripple, and Ven (DATA, 2013). FinCEN appears open to the importance of balancing the costs and benefits of regulations (Remarks, 2013).

This paper proceeds in three parts. Part One provides the reader an overview of virtual currencies, anti-money laundering (AML) policies, and where virtual currencies fit into the AML space. Part Two addresses FinCEN's Guidance. Part three details the author's solution.

2. Virtual Currency Overview

A helpful organizing metric to understand virtual currencies comes from a report released in October of 2012 from the European Central Bank ("ECB Report") titled, "Virtual Currency Schemes" (ECB Report, 2012). Virtual currencies come in three general forms. First, a fully closed system where virtual currencies are earned and used within the game but cannot be purchased or sold outside of the game, ("closed system"). Second, a system where government currencies can be used to purchase virtual currencies (cashed into), but can't be cashed back out of ("partial system"). Third, a convertible system where consumers can cash into and out of a virtual currency, ("open system) (ECB Report, 2012).

This typology is echoed in law with the online contracts game companies create and users must sign in order to access and play a game. This paper relies on these three categories only as a general guideline because they simply do not flush with the economic reality of virtual currencies. Virtual currencies are purchased and used by players largely without regard to whether they are closed, partial, or open. The porous nature of these distinctions is highlighted below.

Virtual currencies under all three systems are company issued, in-game currencies. They are ultimately just a piece of code that a game developer creates to facilitate game play and monetization of the game. Developers fit the currency to the game, such as pieces of gold in fantasy based games or tailored currencies to particular games, such as Empire Points for Zynga's Empires and Allies (Empires & Allies, 2013). They help build brands through name recognition, such as World of Warcraft Gold, instead of simply using government currencies. Virtual currencies also allow for a more consistent game narrative by not using real money. Virtual currencies therefore keep the game story, and therefore game play, consistent (Hemant, B. 2012, May 7, video conference). Creating and maintaining a coherent experience is important for game play but also monetization. This is a central reason why game developers prefer virtual currencies to advertisements, as ads are difficult to effectively place in games and can disrupt game play (Warren, 2011).

The decision of how to monetize a game highlights an important narrative in the game community, which is that virtual currencies are a central piece in game mechanics. This is true for a virtual economy in a Massively Multiplayer Online Role Playing Game (MMORPG) like World of Warcraft, or a mobile, flash-based game like Farmville (Lehdonvirta, 2005). Both are types of virtual worlds that rely heavily on virtual currencies because they power virtual economies and game stories. They get customers to pay for games in the growing free-to-play (F2P) market, also referred to as Freemium (Warren, 2011). The F2P market allows free play of a game either up to a certain level, or with limited access to tools, story lines, or characters within the game. To continue playing, or to enjoy the game more deeply, money is required (Pham, 2012). This usually comes in the form of exchanging real money for virtual currency via a credit card, bank account, or electronic wallet (e-wallet) such as PayPal (SWTOR: Launch FAQ, 2013).

The F2P model benefits customers because it gives them flexibility in their game experience. They are not locked into a subscription or forced to look at ads. Game developers can make more money as well (Smith, 2012). Because of the joint benefit to players and developers, much of the game space is shifting to a F2P model (Nunneley, 2012), and thus placing virtual currencies into a more central role for game developers and players. The F2P model finds its roots in the early growing pains of virtual worlds.

Early on virtual currencies were largely closed systems, such as the gold coins of Ultima Online (UO), captured by Julian Dibbell in "Play Money" (Dibbell, 2006). Dibbell tells a first-hand account of laboring in a medieval, fantasy based virtual world crafting armor and selling animal pelts to make a living. The ability to exchange between players, or peer-to-peer exchange (P2P), was a central design of this subscription-based game. Trading armor and gold within a game basically demands it. And so the very sweat of his virtual and real brow drove value creation, and real economic impact and analysis (Dibbell, 2006, p. 13). Dibbell presented a gripping story about how a virtual world participant could possibly earn a real living.

The reason this is so compelling today, seven years later, is that virtual worlds were shown through clear evidence to be more than just a game. Their economies generated not just hours of entertainment for people, places to collaborate and forge close bonds (Boellstorff, 2010), but also real,

calculable economic activity (Castronova, 2001). And virtual currencies drove, and continue to drive, much of that economic and creative activity.

Much of the buying and selling of virtual currencies and items occurred on secondary markets outside of purview of the game developer, for example eBay (Dibbell, 2006, p. 47). The closed system of UO did not stop the flow of money and value into the game as players could purchase gold outside of the game on eBay or other third-party markets. This activity is referred to as real money trading (RMT), which is the inflow of government currency into virtual worlds for virtual currency and virtual property (Dibbell, 2006, pp. 11-12), and usually outside of the expressly banned or generally opposed external influx of real money (Duranske, 2008, pp. 35-37).

This influx of money caused serious concern over game play for those not engaged in "paying to win" (Castronova, 2006). The flow of real money into games drove the implementation of partial virtual currency systems. These partial systems are now very common as they are money generators for game developers and allow them to make money on activity that used to only generate revenues for third parties like eBay or Internet Gaming Entertainment (IGE) (IGE, 2013). Examples of partial systems include all of Zynga's offerings, such as Farmville and Empires and Allies, and the newest major virtual world MMORPG, Star Wars The Old Republic (SWTOR).

One of the most interesting developments in the game space involves Entropia Universe (Entropia). Entropia's virtual currency, Project Entropia Dollars, ("PEDS"), is an open loop system with a fixed exchange rate between PEDs and dollars. MindArk, the developer behind Entropia, operates in Sweden. One of the best examples of their success is what players spend on virtual goods with their PEDs. For example, several purchases have been made in Entropia over $100,000 with the largest in 2010 when a player, Jon Jacobs, sold a virtual resort for $635,000 (Chiang, 2010). This is not just game play, but a virtual world that attracts significant trust.

Entropia's success with PEDs and game development in general drove MindArk to attempt to provide more financial services for their players. Sweden's financial authority, Swedish Financial Supervisory Authority (SFSA), conducted a review of Entropia. SFSA awarded MindArk with a banking license after a full analysis of the offices of MindArk and the components of game play. The requirements for the banking license were almost fully met before MindArk even applied (Simmons, D. 2013, April 2, Skype interview). A deeper analysis of virtual worlds as banks based on their offering of banking services, such as interest payments on deposits, is beyond the scope of this article. What is relevant to this paper is that game developers are capable of monitoring their systems effectively. They can readily adhere to strict requirements imposed by regulators.

And what's more is that a technologically advanced state is willing to grant a banking license to a virtual world based on their internal systems. Those safeguards cost a considerable amount of money, for example data logs that reach back approximately five years (Simmons, D. 2013, April 2, Skype interview), but that is part of the cost of doing business. Unfortunately the inherent costs of business are barriers to entry. Further increases in those costs without offsets will harm a vibrant and innovative industry.

Even well managed virtual currencies are a cause of concern for AML professionals. Where people congregate and money flows, illicit actors are likely to exploit gaps within those systems (Chambers-Jones, 2012; Landman, 2009). AML goals must apply to all virtual currencies to stop and prevent illicit activity, as well as provide stability to those systems to ensure greater transparency and integrity (Remarks, 2013).

2.1 Anti-Money Laundering Overview

This paper focuses on anti-money laundering goals and policies (AML) because the AML space is one of the dominant concerns within the broader financial crimes topic, also termed threat finance (Stringer, 2011). AML goals are also the dominant focus of FinCEN and its recent Guidance.

Money Laundering is the process of taking money earned through illegal means, for example drug trafficking, and using a process to conceal the origin of that money and in the end have it look legitimate. The goal is to prevent identification of the actors involved, their illegal activities, and to keep the proceeds of illegal activity. This process is characterized by three stages: placement, layering, and integration (FATF, 2013).

Placement is the introduction of illegal funds into the broader economy. Specifically, when illegal funds are placed into an entry point for the formal, regulated economy. For example, taking cash from the sale of fake driver's licenses or drugs and buying a gift card to play a virtual world. These gift cards can be purchased at several stores in person, such as Wal-Mart.

Layering is the effort to conceal the source of the funds. This is achieved by repeatedly transferring funds to create either a complicated audit trail, or by terminating an audit trail altogether. This can be achieved by moving funds from a bank account to a prepaid card, or an e-wallet such as PayPal. It can also be done through the purchase of a gift card in cash. Layering is the most important part of money laundering because this is where law enforcement is most affected in its identification and tracking efforts. This is where data retention logs and user authentication are so important because otherwise, law enforcement is at a complete loss to connect the dots of exchange.

Integration is the placement of seemingly legal money back into the broader economy. This is also a critical juncture for law enforcement specifically in the virtual currency context because transactions can be tracked by coordinating with, or relying on, game operators. Server logs detail transactions and conversations within the game. They also detail what payment system or bank account a user selected to cash in and out of the game from (Simmons, D. 2013, April 2, Skype interview).

2.2 Virtual Currencies and Money Laundering

Discussion of how virtual currencies can be used to launder money is old, as is whether it is even an issue (Chambers-Jones, 2012; Reider-Gordon, 2012; Moses, 2011; NDTA, 2010; Koster, 2007). For example, in 2008 and 2009 a group of Chinese and Korean players defrauded other virtual players and laundered the proceeds back into mainland China through several front companies. The estimated amount of funds is $38 million as that is the amount wired from Korea to Hong Kong over 18 months. (Chambers-Jones, 2012, p. 125). The current inquiry facing FinCEN and game developers is the extent of the problem and how best to handle it—the focus of this paper.

First, the global percentage of money laundering with virtual currencies is currently placed at 1% (Moses, 2011), and that figure includes both virtual game currencies and digital currencies such as Liberty Reserve. Liberty Reserve was a digital currency, web-based money transfer system. FinCEN found them to be a money-laundering hub (Notice of Finding, 2013). Liberty Reserve was the successor to e-gold, another web-based money transfer system that permitted little to no authentication and served as a go-to channel for illicit actors online. Liberty Reserve is now under indictment and had their domain name seized.

Virtual currency money laundering is a complicated process and is carried out, where it is even found, by sophisticated criminals (Chambers-Jones, 2012, p. 125). Law enforcement has the problem of

figuring out just how big the iceberg really is. The 1% estimate is just that, an estimate. Understanding why virtual worlds are compelling for money laundering is important as the solutions proposed need to address those benefits. Virtual worlds are available as meeting locations anywhere in the world with an Internet connection. Many virtual worlds can be setup with fake account information, such as fake email addresses, and can act as a central point of exchange and collaboration (Roche & Ar-Raqib, 2009, pp. 121-22, 140).

There are four central concerns then for the misuse of virtual currencies in games. First, the importance of a record is to identify what transactions have occurred. Relevant details include individuals involved, when the transaction occurred, for how much, and with what systems (bank account, game gift-card, or credit card). Second, whether a user is properly authenticated. Third, what are the channels that connect to the virtual world? Are there digital currencies, web-based money transfer systems such as Liberty Reserve that are accepted by the virtual world? Fourth, how is the game designed to alter how transactions take place? Is there P2P exchange within the game? Some games handle the currency exchange between government currencies and virtual currencies while others rely on external systems not directly associated with the game developer. Some developers actively ban and close accounts that engage in RMT, where others passively allow it. These distinctions matter and go to good faith efforts to comply. Much of the decision to allow RMT is a business decision based on the desired experience for the end user.

3. FinCEN's Guidance

The Guidance, as it relates to game developers, is an interpretive guide to how current regulations apply to entities administering or exchanging virtual currencies. The Guidance focuses only on open virtual currency systems, and therefore, arguably, not closed or partial systems. It does fortunately make specific note of "transfers of value between persons" (or P2P transactions), a central element in the porous nature of virtual currency distinctions. A virtual currency money services businesses (MSB) is any person or business that engages in transmitting money (Guidance, 2013). MSBs must register with FinCEN and fulfill certain obligations. Those include the filing of suspicious activity reports, implementing an AML program, and maintaining records (Guidance, 2013; Remarks, 2013).

The author is concerned that regulators will not address virtual currencies properly, either for AML goals or the game community. The Guidance is fortunately a first step and FinCEN appears to be open to dialogue (Remarks, 2013); however, the Guidance is now the baseline and shapes the debate in a very fundamental way. The Guidance is worrisome for two reasons.

First, the Guidance will place a heavy cost upon virtual world and digital game developers who use an open loop currency. The use of an open loop currency is not as widespread as a partial or closed loop system, but it removes from the developer's tool kit an important option. The particular burden is the filing of suspicious activity reports (SARs). SARs require a full compliance team and experts in the virtual currency field. These are not small costs. Large institutions such as Citibank, PayPal, or Western Union spend millions to track money flows and stay compliant. Granted they have more to track, but virtual worlds and digital games often operate at the fringe of profitability (Olivetti, 2013; Goldfarb, 2012). These game companies are not focused on money services like digital currency operators are. They are in business for their players. Therefore they should be treated differently.

Related with the concern of cost is that developers may be concerned about the open definition of convertibility in the Guidance given the economic realities of virtual currencies in games as detailed already. The boundaries between closed, partial, and open are incredibly porous. In the game context, it

is clear these definitions are increasingly meaningless due to the complex system of virtual currency exchanges, P2P transfers, and grey market activity (Chambers-Jones, 2012, pp. 35-6; First Meta, 2013; Castronova, 2006; Dibbell, 2006). Because of this, game developers may simply abandon virtual currencies all together to avoid regulatory cost.

The second major concern also involves the narrow focus on open, or convertible virtual currency systems. The Guidance does this because convertible currencies provide a higher risk profile for illicit use because they are easier to funnel money through. This approach breaks down though with analysis of P2P transactions and external exchanges.

The Guidance then places a high regulatory burden with mandatory reporting for game developers that use open loop currencies. Because the economic reality of virtual currencies often blur the lines of what exactly is a convertible currency, it is clear the definition needs to be clarified. Further, AML regulations need to include closed and partial systems because they remain an AML concern (Heeks, 2008, pp. 60-61). Oftentimes game developers do not have a choice in whether their currency is converted, such as with Blizzard and their active policing of RMT, and cheating in general, for example in World of Warcraft (Fairfield Nexus Crystals, 2011; Heeks, 2008; Symantec, 2007).

4. A New Path

The goal of this paper is to merge both narratives on virtual currencies into a new approach. The solution proposed achieves this by addressing the concerns raised above by the Guidance. The proposal below is straightforward and includes three requirements for game developers: Data retention logs (DRLs), enhanced user authentication, and restriction on payment systems that are at a high risk of abuse.

Maintaining records is one of the three main goals of FinCEN's. The need for a data trail is vital to identify and track illicit use (Stringer, 2011). For game developers this is nothing new and widely implemented because of the importance of game analytics, or big data (Rose, 2013). Game developers have to figure out how the game is used, where the system breaks down and can be exploited (Dibbell, 2006, p. 114), and what is going on in order to maximize their in-game currency (Gupta, 2013). Data is already saved to a large extent (Simmons, D. 2013, April 2, Skype interview; Timmer, 2009). DRLs are proposed at two years for open, partial, and closed systems with P2P exchange in game. The requirement drops to one year for only closed systems with no P2P exchange possible as that type of system presents the lowest risk factor and therefore the lowest need for a longer DRL. This guideline comes from the broad practice of data retention by game companies already (Simmons, D. 2013, April 2, Skype interview; Timmer, 2009), and ongoing argument over DRLs. For example, the European Data Retention Directive. It requires the storage of up to two years of certain transaction and that those records be made available on request to law enforcement to address serious crimes and terrorism (European Union, 2006). The two-year mark is used as a benchmark based on the precedent of the European Data Retention Directive.

Arguments against DRLs usually center on the duration, their invasion of privacy, and their effectiveness (Masnick, 2013; EDRI, 2011). DRLs for game developers are different than those for Internet Service Providers (ISPs) or Telecommunications companies (Telcos). DRLs for games are qualitatively different from DRLs for ISPs or Telcos because games have a more engaging and constant interaction with users (Rose, 2013). The extent of game DRLs, their use particular to virtual worlds, and the ethical issues, are detailed excellently elsewhere (Fairfield, 2010).

The reality is that game developers retain extensive logs of all in-game activity, particularly transactions with virtual currencies, and payment systems connected to the game. The granularity of these records is incredibly fine and helps game developers to detect gold farmers, and fraudulent activity (Simmons, D. 2013, April 2, Skype interview; Lim, 2013). These records help game developers prevent illicit activities, and upon proper procedures, a data trail for law enforcement when requested (Chambers-Jones, 2012, p. 125; Morris, 2011).

A critical part of useful data, for AML goals specifically, is effective authentication. Authentication, as opposed to identification, is a deeper level of ensuring a person is who they say they are (Bradley, 2010). It is also the most important security problem for networks online (Schneier, 2000, p. 68-72). It comes in two forms, whether in the game context or otherwise online. First, authentication of a user when they set up an account. This can include a name, email address, and a credit card linked to an account. Second, the repeat access of a user, such as when a user logs on to a service after account creation. Both are important for the safety and security with AML compliance, but also safe and secure game play. The second authentication point is particularly prevalent with regards to credit card fraud and account hacking where users find their accounts drained of virtual currency or goods (Account Hacked, 2011).

If a person can sign up for a game and play without entering any personal information, or can easily create a fake identity, then a DRL is not helpful. This issue is commonly referred to in the AML community as Know Your Customer requirements (KYC). The solution argued for is not a silver bullet, but the need for authentication over identification, and higher levels of authentication. These are all expensive, but fortunately the cost is coming down. A great example is Out of Band Authentication (OOBA), such as security keys that generate a one time password (SWTOR: Launch FAQ, 2013), which is the same concept as two-step authentication that Google, Apple, Facebook, and Twitter now use given the extent of damage that can occur from Knowledge Based Authentication's (KBA) weaknesses (Honan, 2012). Another form of authentication is Dynamic Knowledge Based Authentication (DKBA). This improves upon KBA, where KBA asks questions already entered by the user and does not solve the problem of a fake initial identity. KBA is oftentimes invasive, and people enter fake information, are turned away entirely, and worse, can be cracked with some basic research (Honan, 2012).

DKBA implements an ever-changing series of questions based on public records. For example, a user signing up for a new account, or logging in later (depending on how an account is setup with a game), answers a question about their original mortgage amount, or where they have not lived based on a list of random cities where they have. DKBA is also referred to as "out-of-wallet" questions (Bradley, 2010).

The last piece advanced is perhaps the most important for achieving one of the main goals of FinCEN's, and the AML community generally—shutting down channels for illicit use. If a game only accepts payments from certain companies, and those companies actively comply with AML programs, then the game is far safer than if it allows payments from entities with weak or no AML programs, for example Liberty Reserve. Trust relationships with payment services that are reputable and safe is good business (Simmons, D. 2013, April 2, Skype interview; Donahue, A. 2013, April 12, Skype interview). Most companies are in business to make money and provide a great service to their customers. A central part of that is compliance with law and regulations that are clear and make sense. Business heads of gaming companies, and payment gateway systems such as Payelp, do not want to put their companies at risk (Simmons, D. 2013, April 2, Skype interview; Donahue, A. 2013, April 12, Skype interview).

By limiting high-risk payment systems, such as the now infamous Liberty Reserve (Finberg, 2013), game developers can significantly limit themselves from ever being connected to illicit money flows. This includes use of platforms with payment systems linked and required, such as Facebook (Facebook Payments Inc.) and Google (Google Payments Corporation) Both entities have games plug into their platform. These platforms are very similar to the payment systems that stand-alone games such as Entropia rely on, for example Visa or MasterCard. Facebook Payments Inc. and Google Payments Corporation along with PayPal, Visa, and MasterCard engage in risk-based KYC and SARs filing already and are well equipped to handle the cost.

These three requirements address the dominant concerns of maintaining effective records, and most importantly, protecting channels from illicit activity without overburdening those legitimate channels. The final piece advanced is a safe harbor provision providing both civil and criminal immunity from misuse of the game developer's virtual currency. This is needed to cement cost savings and provide a compelling incentive for game companies to adhere to these best practices. Game companies would have to make good faith efforts with their DRLs, identity requirements, and use of compliant payment systems. The safe harbor would require regulations from FinCEN, or more significantly, Congress to amend the existing AML legal framework. It is more likely that FinCEN would create a regulatory safe harbor than Congress would create a statutory one. The likelihood of the safe harbor is not pursued in this paper, only the recommendation for it. The cost of compliance and uncertainty of regulations are hurdles for game developers that a safe harbor provision would address. This safe harbor would be an important element to build a relationship with FinCEN and game developers.

A final consideration is that FinCEN provides for exemptions. Whether a person is a money transmitter, such that they need to register with FinCEN as a MSB, is a matter of facts and circumstances,[1] (Guidance, 2013). This is not adequate for game developers because the proposals above are needed for both AML goals and game developers. An exemption would remove needed information for FinCEN, such as effective records, trusted payment network connections, as well as omit the benefit of the cost savings of the safe harbor, should it be granted.

5. Conclusion

The emerging approach to virtual currencies is a mix of positive and negative developments. The emerging approach does accept the reality of virtual currencies, particularly game currencies, as a medium of exchange. It misses the unique and distinct attributes of virtual game currencies. Because virtual currencies in games are driven in large part by how users interact with them, whether legally, through grey market activity and websites, or illegally, AML regulations must adapt. There is a real benefit to law enforcement with expanding regulations to the broader game space. At the same time this imposes a very real cost on game developers. A balance must be struck between the benefits of virtual currency regulations and the cost imposed. The proposal herein is a step in that direction. The proposal begins as a form of self-regulation, as the Guidance is not final, though given precedential weight should further legal action take place (Regulatory Releases, 2013). There is the chance for an ongoing dialogue to shape this space (Remarks, 2013).

Virtual currencies have unique attributes because of their existence online and as part of a game. They can be controlled, tracked, and studied to a level that government currencies simply cannot. Because of these unique attributes and their growing use in games, the law must reflect this reality or it will restrict the innovative potential that virtual currencies offer as well as games more broadly, all in the

[1] The exact location of these exemptions is in the Code of Federal Regulators, 31 C.F.R. § 1010.100(ff)(5)(ii)(A)–(F).

name of security. The decision between advertisements, subscriptions, and virtual currencies as a monetization strategy should ultimately be a choice for developers to make and not one driven by poorly crafted regulations.

References

Account Hacked During a Deployment, (Oct. 1 2011), *Threadmeters*, Retrieved on April 22, 2013 at http://www.threadmeters.com/v-4HY8/Accout_Hacked_during_a_deployment/.

Boellstorff, T. (Mar. 22, 2010) Coming of Age in Second Life: An Anthropologist Explores the Virtually Human. Princeton University Press.

Bradley, B. (Nov. 12, 2010). Knowing the Difference Between ID Verification and ID Authentication. MicroBilt. Retrieved on June 27, 2013 at

http://www.microbilt.com/blogs/identity-verification-and-authentication/knowing-the-difference-between-id-verification-and-id-authentication.aspx.

Castronova, E. (Dec. 2001), *Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier* 5–6 (CESifo, Working Paper Series No. 618, 2001) Retrieved on April 23, 2013 at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=294828.

Castronova, E. (2006). A Cost-Benefit Analysis of Real-Money Trade in the Products of Synthetic Economies", info, Vol. 8 Iss: 6, pp. 51 – 68.

Castronova, E. (2008). Synthetic Worlds: The Business and Culture of Online Games, University of Chicago Press.

Chambers-Jones, C. (2012). Virtual Economies and Financial Crime: Money Laundering in Cyberspace. Cheltenham, UK: Edward Elgar Publishing Limited. 35, 36, 112-114, 125.

Chiang, O. (Nov. 13, 2010) Meet the Man Who Just Made A Half Million From The Sale of Virtual Property. Forbes. Retrieved on June 23, 2013 at http://www.forbes.com/sites/oliverchiang/2010/11/13/meet-the-man-who-just-made-a-cool-half-million-from-the-sale-of-virtual-property/.

Dibbell, J. (2006), Play Money: Or, How I Quit My Day Job And Made Millions Trading *Virtual Loot*. New York, New York: Basic Books. 11-13, 47, 114.

Digital Asset Transfer Authority (July 30, 2013), Statement of the Committee for the Establishment of the Digital Asset Transfer Authority. Retrieved on September 14, 2013 at http://info.datauthority.org/.

Donahue, A. 2013, April 12, Skype interview. Interview with Albert Donahue (CEO of Payelp Global).

Duranske, B. (2008), *Virtual Law: Navigating the Legal Landscape of Virtual Worlds*. Chicago, IL: American Bar Association Section of Science & Technology Law. 35-37.

Empires & Allies, Empire Points, Retrieved on May 6, 2013 at http://empiresandallies.wikia.com/wiki/Empire_Points.

European Central Bank, Virtual Currency Scheme, (Oct. 2012), Retrieved on Feb. 18, 2013 at http://www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

European Digital Rights (EDRI) (Sep. 26, 2011) Letter to The European Commission to Provide Evidence on the Need for Mandatory Data Retention Law. Retrieved on June 27, 2013 at http://www.edri.org/files/dr_letter_260911.pdf.

European Union, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, EU Journal, L. 105.

Fairfield, J. (2011) Nexus Crystals: Crystallizing Limits on Contractual Control of Virtual Worlds. *William Mitchell Law Review*, *38*, 43.Fairfield, J. (2012). Avatar Experimentation: Human Subjects Research in Virtual Worlds, *U.C. Irvine Law Review, 2*, 695.

FATF Report: What is Money Laundering? *Financial Action Task Force* Retrieved On May 11, 2013 at http://www.fatf-gafi.org/pages/faq/moneylaundering/.

FATF Report: Money Laundering Using New Payment Methods (Oct. 2010) Financial Action Task Force. Retrieved on June 22, 2013 at http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf.

Finberg, R. (Jun. 19, 2013) Is WebMoney the Next Liberty Reserve? *Forex Magnates*. Retrieved on June 27, 2013 at http://forexmagnates.com/is-webmoney-the-next-liberty-reserve/.

FirstMeta Exchange. Retrieved on June 26 2013 at http://firstmetaexchange.com/home.Goldfarb, A. (July 17, 2012) Layoffs Hit Star Wars: The Old Republic Studio. IGN. Retrieved on June 26, 2013 at http://www.ign.com/articles/2012/07/17/layoffs-hit-star-wars-the-old-republic-studio.

Guidance. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (March 18, 2013). Department of the Treasury Financial Crimes Enforcement Network. Retrieved on March 19, 2013 at http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

Gupta, V. Social Gold page on Slide Share. Retrieved on June 27, 2013 at http://www.slideshare.net/socialgold.

Hamari, J. and Lehdonvirta, V. (2010) Game Design as Marketing: How Game Mechanics Create Demand for Virtual Goods. *International Journal of Business Science & Applied Management*, *5* (14), 23.

Heeks, R. (2008) Current Analysis and Future Research Agenda on "Gold Farming": Real-World Production in Developing Countries for the Virtual Economies of Online Games. *Development Informatics Group paper no. 32*. Retrieved on April 19, 2013 at http://www.sed.manchester.ac.uk/idpm/research/publications/wp/di/documents/di_wp32.pdf. 60-61.

Hemant, B. 2012, May 7, video conference.Video conference with Hemant Bhanoo (Technical Staff at Google – Payments, books, and adwords). Discussion focused on work as Principal Engineer at Jambool, Inc. (acquired by Google). Jambool was a virtual currency payments product company.

Hindman, B. (Apr 5, 2013) MMObility: How The Mobile Market is Trying to Change MMOs. Massively. Retrieved on June 26, 2013 at http://massively.joystiq.com/2013/04/05/mmobility-how-the-mobile-market-is-trying-to-change-mmos/.

Honan, M. (Aug. 6, 2012), How Apple and Amazon Security Flaws Led to My Epic Hacking. Wired. Retrieved on June 19, 2013 at http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/.

Internet Gamine Entertainment. IGE. Retrieved on June 26, 2013 at http://www.ige.com/.Koster, R. (Jan., 3, 2007), The Risk Community Noticed Virtual Money Laundering, Retrieved on February 24, 2013 at http://www.raphkoster.com/2007/01/03/the-

risk-community-noticed-virtual-money-laundering/.Landman, S. (2009) Funding Bin Laden's Avatar: A Proposal for the Regulation of Virtual Hawalas Note, *William & Mitchell Law. Review*. *35*, 5159. 5172.

Lehdonvirta, V. (2005). Virtual Economics: Applying Economics to the Study of Game Worlds. Proceedings of the 2005 Conference on Future Play, Lansing, MI, October 13-15, 2005. Available at SSRN: http://ssrn.com/abstract=1630302.

Lim, N. (June 24, 2013). Big Data and Games – Part 1 – Why Ask Why. Gamasutra. Retrieved on June 27, 2013 at http://www.gamasutra.com/blogs/NickLim/20130624/194556/Big_data_and_games__part_1__why_ask_why.php.

Masnick, M. (May 29, 2013) Danish Police Admit That Data Retention Hasn't Helped At All. TechDirt. Retrieved on June 27, 2013 at https://www.techdirt.com/articles/20130523/02542423184/danish-police-admit-that-data-retention-hasnt-helped-all.shtml.

Mission, Financial Crimes Enforcement Network, Retrieved on June 22, 2013 at http://www.fincen.gov/about_fincen/wwd/mission.html.

Morris, S. (Mar. 18, 2011), British Hacker Jailed over £7m Virtual Gaming Chips Scam, The Guardian, Retrieved March 20, 2013 at http://www.guardian.co.uk/technology/2011/mar/18/hacker-jailed-gaming-chips-scam.

Moses, A., (June 23, 2011), Secret Money: ABC Virtual Currency Racket Probe. Sydney Morning Herald. Retrieved on March 20, 2013 at http://www.smh.com.au/technology/technology-news/secret-money-abc-virtual-currency-racket-probe-20110623-1ggp6.html.

National Drug Threat Assessment 2010 Illicit Finance Unclassified, (Feb. 2010). U.S. Department of Justice National Drug Intelligence Center. Retrieved on March 27, 2013 at http://www.justice.gov/archive/ndic/pubs38/38661/finance.htm#Top.

Notice of Finding That Liberty Reserve S.A. Is a Financial Institution of Primary Money Laundering Concern (May 28, 2013). Financial Crimes Enforcement Network. Retrieved on June 25, 2013 at http://www.fincen.gov/statutes_regs/files/311--LR-NoticeofFinding-Final.pdf.

Nunneley, S., (Mar. 6, 2012), SOE: SWTOR the "Last Large Scale MMO" to Use Subscription Business Model. Video games 247. Retrieved on June 1, 2013 at http://www.vg247.com/2011/09/20/soe-swtor-the-last-large-scale-mmo-to-use-subscription-business-model/.

Olivetti, J. (Mar 21, 2013) MMO Devs Most in Danger of layoffs, Study Claims. Massively. Retrieved on June 26, 2013 at http://massively.joystiq.com/2013/03/21/mmo-devs-most-in-danger-of-layoffs-study-claims/.

Pham, A. (Mar. 27, 2012). League of Legends: Find Your Champion. Los Angeles Times. Retrieved on March 20, 2013 at http://herocomplex.latimes.com/2012/03/27/league-of-legends-find-your-champion/#/0.

Regulatory Releases. Financial Crimes Enforcement Network. Retrieved on June 30, 2013 at http://www.fincen.gov/news_room/rp/rulings/html/regrelease.html.

Reider-Gordon, M. (2012). Real World Risk in Virtual World Gaming: Virtual Conferences, Money Laundering, and the Hidden Risks to Game Companies. Navigant. Retrieved on June 3, 2013 at http://www.navigant.com/insights/library/disputes_and_investigations/2013/world-risk-virtual-world/.

Remarks of Jennifer Shasky Calvery (Director of Financial Crimes Enforcement Network) (June 13, 2013) Virtual Economy: Potential, Perplexities and Promises (United States Institute of Peace), Retrieved on June 22, 2013 at http://www.fincen.gov/news_room/speech/pdf/20130613.pdf.

Roche, E., Ar-Raqib, A. (2009), Virtual Worlds Real Terrorism, Den Haag, Netherlands: Aardwolf Publications. 121, 122, 140.Rose, K. (Mar. 13, 2013) Gaming Companies at the Forefront of Hadoop and Big Data. Horton Works. Retrieved on June 27, 2013 at http://hortonworks.com/blog/gaming-companies-at-the-forefront-of-hadoop-and-big-data/.

Schneier, B. (2000), *Secrets & Lies: Digital Security in A Networked World*. New York, New York: John Wiley & Sons, Inc. 68-72.Simmons, D. 2013, April 2, Skype interview. Interview conducted over Skype with David Simmons (CEO of MindArk) and John Bates (Business and Marketing for MindArk).

Smith, C. (Mar. 20, 2012) Freemium and the Virtual Goods Phenomenon: Interview with Sanjay Sarathy. The Guardian. Retrieved on March 20, 2013 at http://www.guardian.co.uk/media-network/media-network-blog/2012/mar/20/freemium-virtual-goods-sanjay-sarathy.

Stringer, K. (Spring 2011), Tackling Threat Finance: A Labor for Hercules or Sisyphus? Parameters. Retrieved on May 9, 2013 at http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2011spring/Stringer.pdf.

SWTOR: Launch FAQ, Star Wars the Old Republic. Bioware. Retrieved on June 23, 2013 at http://www.swtor.com/info/faq/game.Symantec Internet Security Threat Report. (2007) Symantec.Retrieved on June 19, 2013 at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_exec_summary_09_2007.en-us.pdf.

Timmer, J., (Feb. 15, 2009), Science gleans 60TB of behavior data from Everquest 2 Logs. ARS Technica. Retrieved on April. 30, 2012 at http://arstechnica.com/science/news/2009/02/aaas-60tb-of-behavioral-data-the-everquest-2-server-logs.ars.

Warren, C. (Aug. 16, 2011), Virtual Currency Beats All Other Kinds of Mobile Game Purchases. Retrieved on March 20, 2013 at http://mashable.com/2011/08/16/mobile-game-in-app-purchases/.