Money laundering in a Virtual World

Clare Chambers-Jones

Introduction

Virtual currencies are a key aspect of anti-money laundering (AML) regulation. This chapter investigates the United Kingdom's (UK) approach to virtual worlds and their virtual currencies, determining whether this currency system is included in national and international money laundering definitions and regulations. Virtual worlds can be a safe haven for criminal activity, such as money laundering, and the lack of sufficient regulation in the UK is one of the pivotal points currently being discussed at regulatory and governmental levels. The chapter is divided into several parts. First, it looks at virtual worlds, their definitions and identifies how virtual currencies are considered to be a money laundering risk. The chapter moves on to provide evidence that money laundering does take place within virtual worlds and as such should be included in the virtual currency definition and regulations. The chapter then considers the approaches taken to prevent virtual currency money laundering and explores the UK's approach to money laundering regulations. The chapter further considers approaches of other countries compared to the UK, and concludes with an analysis and reflection of the UK's approach to regulating virtual worlds and money laundering.

Virtual worlds

Virtual worlds and their economies are not the same as virtual currencies, like Bitcoins, which are cryptocurrencies, but they are both forms of virtual currency.[1] Virtual worlds are computer based platforms where environments are created and people simulate real or fantasy lives. Within these virtual worlds, economies, societies and personal relationships develop. Therefore, virtual worlds are a type of microcosm of life that is lived in digital pixels and spans a multitude of different jurisdictions. Virtual worlds in this context are discussed as a possible location for money laundering to take place.

[1] For discussion of Bitcoin, see ch.9 (Egan) in this collection.

This is not the same as using digital or cryptocurrencies as a means of money laundering because this takes place in the real world even if the currency is a virtual currency. The process of the two is different. One uses the virtual environment as a location of criminal activity, whereas virtual currency money laundering uses the internet or other electronic payment systems to disguise or hide the proceeds of crime. However, the two are connected and should be considered as akin to each other.

A useful definition of virtual currencies comes from the European Banking Authority (EBA) which states that virtual currencies are "defined as a digital representation of value that is neither issued by a central bank or a public authority nor necessarily attached to a Fiat Currency, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically".[2] Therefore, virtual currencies that are used within virtual worlds, such as Linden Dollars in Second Life are considered to be the same as other digital currencies such as Bitcoins. Second Life is a 3D immersive platform based environment game/world which has developed a culture and economy of its own. Its economy is based on the in world currency, the Linden Dollar, named after Linden Labs, the technical development company which owns the platform. This form of virtual world is popular amongst gamers but also academics and health care professionals that can use the environment as a base for learning and education. It can also be used by criminals as a means of conducting illegal activity[3]. A virtual world according to Castronova is a computer programme with three defining features: interactivity; physicality and persistence.[4] Bell defines virtual worlds as "a spatially based depiction of a persistent virtual environment, which can be experienced by numerous participants at once who are represented within the space by avatars".[5]

This chapter focuses on these virtual world currencies and how the existing UK AML laws do not apply to them. Policy makers in the UK are only just beginning to discuss and consult on the necessary guidelines for safeguarding virtual currencies such as Bitcoins, but it is unclear as to how these regulations apply to virtual worlds such as

[2] European Banking Authority, Opinion on virtual currencies. EBA/Op/2014/08. 4 July 2014. p.11.
[3] Chambers-Jones, C. L. (2012) Virtual Economies and Financial Crime: Money laundering in Cyberspace
[4] E. Castronova, 'Virtual Worlds: A first-hand account of market and society on the cyberian frontier', CESifo Working Papers, No.618, December 2001; E. Catronova, 'On Virtual Economies', CESifo Working Papers, No. 752. July 2002.
[5] M.W. Bell, 'Towards a definition of virtual worlds' (2008) 1(1) Journal of Virtual World Research page range.

Second Life, World of Warcraft or to Facebook credits, which all fall under the EBA definition of virtual currencies. These forms of virtual currencies are different from where money is exchanged over the internet or mobile phone such as Paypal due to the type of currency which is used. Paypal uses fiat currency whereas virtual currencies need to be exchanged into fiat currency before they can be used in the real world.

Before defining virtual money laundering, it is prudent to determine what cybercrime is, as virtual money laundering falls under this umbrella term and has seen more legislative provisions.[6] Cybercrime "is one of the fastest growing areas of crime, as more and more criminals exploit the speech, convenience and anonymity that modern technologies offer in order to commit a diverse range of crimes."[7] One of the earliest detected virtual crimes was that of the virtual rape,[8] which took place in the LambdaMOO MUD.[9] The rapist, known as Mr Bungle, described the rape of another MUD user. However, his actions were insufficient for a successful prosecution. There is an academic bifurcation as to whether Mr Bungle's actions amounted to an actual rape capable of prosecution or whether it was insufficient because it lacked real world consequences. Brenner referred to the rape as a "true virtual crime",[10] whereas Dibble said that he "was fascinated by the concept of a virtual rape, but I was even more so by the notion that anyone could take it altogether seriously".[11]

Brenner explored what would enable a virtual crime to be successfully prosecuted, and she determined that the virtual crime would need to have real world elements.[12] Lessig opined that there could be a valuable link between actual rape and the LambdaMOO rape in cyberspace[13], but this opinion was criticised by Kerr who stated that the link "is tenuous at best. It is a link between a brutal rape and a fictional story

[6] See Council of Europe Budapest Convention on Cybercrime 2001 23/11/2001; and the Commonwealth Model law on Cybercrime 2002.
[7] Interpol. 'Cybercrime fact sheet', 2008. COM/FS/2008-07/FHT-02.
[8] J. Dribble, 'A Rape in Cyberspace', *Village Voice*, Vol XXXVIII, No 51, December 1993.
[9] MUDs are text based virtual worlds. For a discussion on this see Richard Bartle, *Designing virtual worlds*, New Riders, 1 Ed.) 3-21; Julian Dibble, *My tiny life: Crime and Passion in a Virtual World* (Holt paperbacks, 1998) 51-65; G. Lastowka and D. Hunter, 'Virtual Crimes' Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=564801 (last accessed October 10, 2016) at 14-21.
[10] S.W. Brenner, 'Is there such a thing as a virtual crime' (2001) 4(1) California Criminal Law Review 105-11.
[11] Julian Dibble, *My tiny life: Crime and Passion in a Virtual World* (Holt paperbacks, 1998) p.21.
[12] Brenner (n.10).
[13] L. Lessig, *Code and other laws of cyberspace* (Basic Books, 1999) 74-78.

of a brutal rape. Surely the difference is more striking than any similarity".[14] Although this argument can be considered credible, if there are real world effects stemming from in world action and crime then it is a real world crime and should be met with the same real world consequences. In this sense, virtual money laundering is a crime which takes place in the virtual world but has a true and real effect on the real world whenever dirty money is laundered via the virtual world environment.

Given the interest from law enforcement agencies as to whether crimes committed on the internet are real or not, there is a growing body of literature on the subject. Interpol, acting to combat virtual financial crime, states that, "the global nature of the Internet allows criminals to commit almost any illegal activity anywhere in the world, which makes it essential for all countries to adopt their domestic offline controls to cover crimes committed in cyberspace". [15] Therefore, Interpol is contending that to combat this new wave of criminal activity domestic governments should tailor their domestic real world laws to fit the crimes that are being carried out in cyberspace. To be able to commit virtual world money laundering real money must pass into the virtual world as virtual money and then be able to be extracted once laundered. Interpol has stated that virtual money is "money value represented by a claim on the issuers which is stored on an electronic device and accepted as a means of payment by others persons other than the issuer".[16] This definition allows virtual money to be treated as real money for money laundering purposes in law because the money can be used as fiat currency.

There are two types of virtual money - identified virtual money and anonymous virtual money.[17] Identified virtual money can be identified as belonging to someone and is linked to a withdrawal from a banking institution. In other words, it is traceable. Anonymous virtual money (or what is known as virtual cash) is untraceable. Once it is withdrawn, it leaves no discernible trace. There are plentiful criminal activities which can then take place with this money. For example, Interpol states that the main areas are: Unauthorised creation, transfer or redemption of virtual money; Criminal access

[14] O. Kerr, 'The Problem of perspective in internet law' (2003) 91 Georgetown Law Journal 357, 372-7.
[15] Kerr (n.14), pp.372-73.
[16] Interpol. 'Virtual Money'. 27 May 2010. http://www.interpol.int/Crime-areas/Financial-crime/Money-laundering accessed 11 October 2016.
[17] Ibid.

to computer systems being used to change illicitly the attribution of funds within the system; Criminal attacks on virtual money systems leading to a loss of virtual money value or loss of function on the virtual money system; Criminal misuse of virtual money systems for financial crimes or as a tool to subvert or misuse other financial systems; and Criminals may use virtual money to reduce the likelihood of capture for example, the cases of blackmail, kidnapping or extortion, where in the past; collection of money has been problematic for perpetrators. This is particularly significant for anonymous virtual money.[18]

The Fraud Advisory Panel describe virtual money laundering as where "[A] fraudster converts the proceeds of illegal activities into online currency, which is then used to purchase goods and/or services from you before being exchanged into real world currency."[19]

There are three traditional stages of laundering money: placing, layering and integration.[20] The first stage, placing, is to put the money (which is normally cash) into a place such as a bank. In the case of virtual money laundering this could be a PayPal account as well. The second stage, layering, is to ensure that the money does not raise suspicions. The criminal needs to carry out as many complicated and intricate transactions with the money so that any traces are hard to follow. The final stage, integration, is where the criminal combines the so-called dirty money with legitimate money, making the whole appearance of the money to be clean. From this very brief description, it is clear how virtual worlds, the virtual economy, and virtual money transfers lend themselves to the money laundering process. The dirty money can enter the virtual world through a pre-paid card, such as PayPal, where little identification is required. The money can be used to buy in world goods, through numerous accounts and then the criminal can sell these goods in world. The money from these investments in the virtual world can then be withdrawn from the world via an ATM or money account and the money appears to be from a legitimate source. It is therefore laundered.[21] In 2006, the Financial Action Task Force (FATF) highlighted concerns about the new

[18] Supra n. 15.
[19] Fraud Advisory Panel. 'Cyber Crime: Social Networking and virtual worlds', Issue 4, October 2009. ; and see Clarke Kiernan Solicitors LLP, Second Life, http://clarkekiernan.com/second-life accessed 11 October 2016.
[20] For a comprehensive review of money laundering see N. Ryder, *Money laundering – An Endless Cycle?* (Routledge, Oxon, 2012).
[21] N. Ryder, 'The Financial Services Authority, the Reduction of Financial Crime and the Money Launderer – A Game of Cat and Mouse' (2008) 67(3) Cambridge Law Journal 635-653.

method of electronic monetary transfers with a view to this being a new financial crime.[22] However, since this report by the FATF, little has been put in place to provide deterrence, nor any regulations to ensure successful prosecutions within the UK.

Virtual currencies and money laundering

To be able to launder money through the internet, there needs to be a method by which to do so. Money is therefore converted into virtual money, used within a virtual game, which has now converted the real money into a virtual in world currency, and so the means by which a criminal can launder the proceeds of crime is complete. There are various methods of using electronic money to facilitate money laundering; these are through an electronic purse, mobile payments, internet payment services, and through digital precious metals. An electronic purse is a pre-paid card, which looks like a credit or debit card. There is an electronic chip within the card which stores data as to how much money has been loaded onto the card. Money can be put on these cards at various tellers and shop stores. The cards can then be used to pay for goods and services, where accepted, which is to another electronic purse, but they leave no transaction record. Recently the major credit card companies are also providing these a means of new payment methods.[23]

The second method of payment is through mobile and wireless telecommunications. These mobile payments mostly require financial institutions as part of the transaction. However, this can be avoided should the mobile payment go through a broker account. The broker accounts are normally pre-paid with cash and operate in the same way as an electronic purse. This will then lend itself open for money laundering because of the lack of verification of identification and lack of trace,ability. The third method is through internet payment, which "rely on an associated bank account and use the internet as a means of moving funds to and from the associated bank account or they operate entirely on the Internet and are indirectly associated with a bank account".[24] When the payments are not associated with a bank account then there is again a lack

[22] Financial Action Task Force, *Report on New Payment Methods* (Paris: FATF/OECD, 2006).
[23] For more information on electronic purses please see: S. Stepney, D. Cooper, and J. Woodcock, An Electronic Purse: Specification, Refinement and Proof (Oxford University Computer Laboratories, Technical Monograph PRG-126, 2000) Available at: http://www-users.cs.york.ac.uk/susan/bib/ss/z/prg126.pdf (last accessed October 10, 2016).
[24] H. Desguin, 'Money laundering through virtual games'. Strategic assessment. Florida Department of Law Enforcement, Office of Statewide Intelligence, October 2008. p.17.

of identification and traceability required for the process to occur. Furthermore, most providers will accept cash and may not want to participate in money laundering regulations because of the red tape that will be required to be completed before the completion of a transaction.

The final method is through digital precious metals whereby digital precious metal brokers allow customers to purchase digital precious metal on the world commodity market at market prices. By using a broker, there is again another level of anonymity and lack of traceability for the transaction. As Desguin states, "the basis for using digital precious metals is to make online transactions possible without regard for underlying currencies or access to foreign exchange".[25] The result is to enable the laundering of the proceeds of crime.

Why is virtual money an effective mechanism to launder the proceeds of crime? One of the main reasons advocated is that "digital currencies provide an ideal money laundering instrument because they facilitate international payments without the transmittal services of traditional financial institutions".[26] Many "digital currencies are privately owned online payment systems that allow international payments".[27] Furthermore, an additional feature of virtual world money is where digital currency is used to buy real world metals, which can then be traded. The people that buy the metals with digital cash are allegedly linked to the real commodities stock market. These digital currencies are as bespoke as any real world currency. As the US Department of Justice National Drug Intelligence Centre states "each digital currency functions as a transnational currency however none are recognised as currencies by the US government".[28]

Another problem of digital currencies is anonymity, which is "a heavily marketed characteristic of the digital currency industry".[29] This allows the cybercriminal an extra layer of protection when laundering money. Some issuers of digital currency do require some form of identification, but because this is facilitated via the Internet, the

[25] Desguin (n.24), p.18.
[26] US Department of Justice National Drug Intelligence Centre, *Money laundering in digital currencies* (June 2008), p.1. Available at: https://www.justice.gov/archive/ndic/pubs28/28675/28675p.pdf (last accessed October 10, 2016).
[27] US DoJ (n.26), p.1.
[28] US DoJ (n.26), p.1.
[29] US DoJ (n.26), p.3.

documents can be scanned or e-mailed or faxed, allowing for easy doctoring. The means of putting real money into digital money is plentiful and each allows the criminal a chance of an easy method of laundering. For example, the money launderer can deposit cash to the issuers exchange bank account, thus the money is not traceable. Secondly, exchanges also accept wire transfers or postal money orders also allowing another layer of difficulty in determining the source of the original money. Thirdly, money can be transferred via electronic money orders, cheques, and online banking transfers, all of which again are hard to determine the true source of the money. Fourthly, money can be transferred into the exchanges via pre-paid cards, and money can be withdrawn.[30]

The use of advanced technology allows the cybercriminal further anonymity and networking ability.[31] The use of Internet Protocol (IP) addresses identifies the user to their computer and therefore their actions allow identification of cyber criminals. However, there are various ways around this identification such as using mobile devices including mobile phones that are internet enabled; hijacking wireless networks, encrypted chat rooms and using public internet access points. It is reported that "because digital currency is increasingly misused to purchase drugs and other illicit materials that are sold online, the proceeds of that activity are essentially pre-laundered".[32] Additionally, some digital exchanges allow for transactions to be unlimited in value, which allow drug trafficking to occur in ready abundance.[33] The criminals can launder larger amounts, with total anonymity using fewer transactions.[34] The US government acknowledges that there are regulatory loopholes which must be closed in relation to digital currencies and money laundering.[35] However, regulatory action from one nation is currently insufficient. There must be a joined up multi-national regulatory position that is devised to prevent further cyber financial crimes and money laundering.

[30] US Department of Justice National Drug Intelligence Centre, *Prepaid stored value cards: A potential alternative to traditional money laundering methods* (October 31, 2006). Available at: https://www.justice.gov/archive/ndic/pubs11/20777/20777p.pdf (last accessed October 10, 2016).
[31] US DoJ (n.26), p.4.
[32] US DoJ (n.26), p.4.
[33] US DoJ (n.26), p.6.
[34] US DoJ (n.26), p.6.
[35] US DoJ (n.26), p.6.

One other major problem is the confusion of terms as indicated at the start of the chapter. Virtual money and digital money are not the same thing, but governments use the terms interchangeably and as such cause confusion over the legal status of the crime. Digital currencies such as Bitcoins are being encompassed into anti-money laundering strategies, whereas virtual worlds are not being discussed as an environment where money laundering can take place, at least outside the academic arena.[36] This is because of a lack of detailed knowledge of virtual worlds and also digital currencies.

There are several major problems associated with regulating virtual money laundering: the issues of anonymity of transactions and digital and real world account details through online transactions; the lack of jurisdiction surrounding these transactions and how they interact with the real world; that there is a trading feature associated with the real world, namely that of digital cash, which too interacts with the real world; and the issue of payment methods from the real world to the virtual world causes a link and relationship between the two worlds. These four issues link the virtual to the real, and vice versa, allowing the continuum of the real into the virtual and will be discussed in detail now.

Analysis of Money Laundering Cases in the Virtual World

Many virtual worlds such as Second Life have their own economy. They have their own monetary exchanges, and real world money can be inputted into the virtual world and used to buy commodities such as clothes, building and experiences. Therefore, these virtual worlds can be used by criminals as an environment in which to commit virtual financial crimes, including money laundering. The next section provides a review of several cases where virtual money laundering has occurred. The section does not cover digital cryptocurrencies where money laundering has taken place, for example Liberty Reserve, as this is outside the scope of this chapter.

[36] See Chambers-Jones, C. L. Virtual Economies and Financial Crime: Money laundering in Cyberspace 2012, and Stokes, R. (2012) Virtual money laundering: the case of Bitcoin and the Linden Dollar, Information and Communications Technology Law, 21:3, p221-236.

Gold Farming

Gold farming is a form of online employment which is popular in China and other Asian countries as the fastest form of new occupation. Heeks purports that "it employs hundreds of people and earns hundreds of millions of dollars annually".[37] Gold farming is said to be the production of virtual goods and services for players of online games, and it is this production and selling of goods which can be open to abuse by money launderers and financial criminals. Gold farmers are usually employed as part of a group and controlled by a conglomerate of people. The gold farmers make hundred and thousands of different virtual goods and services which are then sold within the online game. The selling of these goods produces an income of online currency. With many online worlds now having their own currency (e.g. Linden Dollars in Second Life) and currency exchanges, money can then be exchanged for real world money. Gold farming is now such a large enterprise it has been determined as its own economic sub-sector. However, there has been little academic research into the phenomenon and very little legislative discussion.

Gold farming can be traced back to 1997 and the introduction of "real money trading" (RMT) where it can be seen that the first trades for real money were undertaken for goods and services within the virtual worlds. RMT was something of a northern hemisphere phenomenon and did not really penetrate China and Asia until 2001/2, when it has been suggested that US traders saw the opportunity to outsource trading to lower-income venues such as Mexico and Asia. Gold farmers make money by sitting and playing online games, making and selling online goods and services and this is done in three ways. First, they sell in game currency. This is very much the same as the real world currency exchange where it is possible to buy and sell virtual money at different rates and if done correctly can result in profits on the exchanges. Secondly, gold farming can be what is known as 'power levelling', which is where the gold farming firm is given the user name and password of the player who wants to achieve a certain level in the game but does not want to do it themselves. Money is then paid to the gold farmer who plays as the user and attains an agreed level or status

[37] R. Heeks, 'Current Analysis and Future Research Agenda on "Gold Farming": real world production in developing countries for the virtual economies of online games', (Development Informatics Groups, Institute for Development Policy and Management, University of Manchester, 2008). Available at: http://hummedia.manchester.ac.uk/institutes/gdi/publications/workingpapers/di/di_wp32.pdf (last accessed October 10, 2016).

within the game. The third way is by selling in game items for virtual money. The gold farmer buys or creates goods and services which are then sold for a profit in game. The money is then exchanged for real world money.

Within the above three scenarios, there is the obvious potential to launder money through the gold farming mechanisms. For example, the gold farming firm which employs these outsourced lower paid employees could be using criminal money to fund the gold farming activities. Once the money has gone through the virtual game and been exchanged back into the real world through a bank or PayPal then it appears to be legitimate. There is little control and monitoring over gold farming, though South Korea has in theory[38] banned virtual currency trading.[39] Conversely, it is reported that the Chinese government has invested heavily in gold farming as it appears to be the new trend of online employment enabling more people to earn a living, albeit in modest proportions.[40] Gold farming can benefit many in society where employment is hard to come by; gold farming however can also, as iterated above, be exploited by fraudsters and criminals. There is little that can be done in terms of a response. For example: if there is fraudulent or criminal activity, the activities can be reported to the game developers. In some cases, where gold farmers are found to be making money, they can be downgraded to lesser roles within the game, this is called nerfing. Accounts can be banned; the game developers can patch the hole in the game which allows this activity. In more serious cases, the IP address of the gold farmer can be banned and blocked. Similarly, channels used for marketing and sales can be blocked. Finally, legal action can be taken against gold farmers if sufficient evidence can be found and jurisdiction established.[41]

Therefore, gold farming is not a legal activity, nor one which is condoned within the gaming industry, and it contravenes the terms and conditions which the MMORPG developers have set out. The users must sign and agree to End User Licence Agreements (EULA) and also the Terms of Service (TOS) and Terms of User (TOU).

[38] Heeks (n.37).
[39] U-G Yoon, 'Real money trading in MMORPG items from a legal and policy perspectives' (2008) 1 Journal of Korean Judicature 418-477.
[40] Jin G. 'Chinese Gold farmers in the game world', Consumers, Commodities & Consumption, 7(2) May 2006. t https://netfiles.uiuc.edu/dtcook/www/CCCnewsletter/ 7-2/jin.htmaccessed 26 May 2011.
[41] Heeks (n.37).

These agreements typically set out the prohibition of conducting activities such as gold farming or those similar to gold farming. Governments are divided in their attitudes to the legality of gold farming. The Chinese government has clearly defended the rights of the gold farmers to make money and to earn a living in employment, yet the US is strongly against the use of gold farming specifically because it opens up yet another avenue for money laundering and financial crime.

Virtual Money Inc.

In 2008, the owner of Virtual Money Inc[42] was indicted, convicted, and sentenced to 45 months in prison for drug trafficking and money laundering. Robert Hodgins is the owner and CEO of the virtual pre-paid cards[43] which have come under scrutiny in the US over the lack of regulation surrounding the fledgling industry. Hodgins is currently on the run from the police,[44] and the case remains open. However he is said to have laundered drug money through Virtual Money Inc on pre-paid cards from Colombia. In 2010, federal prosecutors announced five convictions of drug related money laundering in relation to the Virtual Money Inc case, known as VM. VM is said to have been part of the AdSurfDaily and other auto surf companies. One of those convicted, Juan Merlano Salazar, of Medellin, Colombia, pleaded guilty in U.S. District Court in Connecticut to 11 counts of money-laundering and one count of conspiracy to commit money laundering. He is facing a 240-year prison sentence and a $6 million maximum fine.

Attorney turned launderer

Ken Rijock is an attorney turned launderer but who know works with law enforcement agencies in advising policy on catching virtual money launderers. He described virtual

[42] United States Court of Appeals for the Tenth Circuit v Frank H Reynolds. No. 11-6064 (D.C. No. 5:10-CV-00832-C) (W.D. Okla). 1 September 2011.
[43] For a good discussion on prepaid cards see: C.J. Linn, 'Regulating the cross-border movement of prepaid cards' (2008) Journal of Money laundering Control 146.
[44] PatrickPetty.com. (2010) Update: Robert Hodgins still wanted by Interpol; co-defendant in narcotics probe with link to AdSurfDaily case sentence to prison; Colombian drug Business used dame debit card as ASD. http://patrickpretty.com/2010/08/15/update-robert-hodgins-still-wanted-by-interpol-co-defendant-in-narcotics-probe-with-link-to-adsurfdaily-case-sentenced-to-prison-colombian-drug-business-used-same-debit-card-as-asd/ accessed 11 October 2016.

money laundering as “the perfect crime”.[45] He cautioned that, “there is no way law enforcement can even enforce the laws, because they don’t apply”.[46] One of the main reasons he believed that virtual money laundering is a crime of the future is because of the ease of laundering the money without detection or repercussions. He gave an example as to how virtual money laundering works:

> “A drug dealer using fake IDs opens numerous virtual bank accounts through online games. He deposits money into those virtual accounts through ATMs. The criminal’s online persona buys, say, virtual real estate from a co-conspirator – or even from one of his other accounts – and transfers payment to the seller’s virtual account. The seller can then convert the virtual currency into real money through a virtual money exchange and withdraw it from an ATM or a bank”.[47]

Rijock further stated that it is impossible to police and counter the criminal act because there is a total lack of clarity over the legal position of virtual worlds. Greg Short, director of Web presence for San Diego, California-based Sony Online Entertainment agree-d: “The legal system doesn’t extend here, there really aren’t any laws that govern what happens in them”.[48]

The above examples of virtual money laundering cases demonstrate that the crimes are in fact real and have impact in the real world. They also show how poorly existing legislation works with these virtual crimes, and how complex it is for law enforcement agencies to manage them. International cooperation and more joined up bespoke legislation is needed to combat this developing crime.

Legal Perspective

[45] Monroe, B. ‘Virtual worlds clear and present danger for money laundering’, 26 April 2007, Fortent. http://www.world-check.com/media/d/content_pressarticle_reference/Virtual_Worlds_Clear_and_Present_Danger_for_Money_Laundering.pdf accessed 11 October 2016.
[46] Ibid.
[47] Supra n.45.
[48] Supra n.45.

The main regulatory body for financial services in the UK is the Financial Conduct Authority (FCA).[49] Their Handbook for regulatory and compliance guidance provides information for financial institutions on proactive anti-money laundering procedures. This falls under the Systems and Controls[50] part of the handbook, in particular 6.3.[51] Virtual currencies are not yet covered by the FCA guidance and compliance, and, as such, the UK AML framework also does not apply to virtual currencies. In comparison to other countries, the UK is in a state of flux as to how to regulate virtual currencies. In contrast, the US is starting to adopt various regulations which are aimed at preventing money laundering. These are based around monetary exchanges, know your customer provisions, and taxation rules.

The FCA published information on virtual currencies in its AML report 2013/14.[52] The report stated that presently virtual currencies are not regulated by the UK or EU,[53] but that the FCA, and government will monitor the situation closely due to high profile cases such as Liberty Reserve where virtual currencies had been used as a means of money laundering.[54] Once again virtual currencies are only seen by governments in terms of crypto currencies rather than encompassing all virtual currencies - such as Linden Dollars or other virtual world currencies - where money laundering has taken place over a number of years. The FCA report highlighted that the EBA and the FATF had published reports providing some guidance in terms of definitions and potential money laundering and terrorist financing risks, as well as a risk based guidance approach for firms.[55]

[49] See Financial Conduct Authority, *Financial Crime: A guide for firms. Part 1: A firms guide to preventing financial crime* (April 2015). Available at: https://www.handbook.fca.org.uk/handbook/document/FC1_FCA_20150427.pdf (last accessed October 10, 2016). For more on Money laundering and the FCA see: Financial Conduct Authority (2016) Money laundering and Terrorist Financing. https://www.the-fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing (last accessed October 10, 2016).

[50] FCA Handbook. Systems and Controls. Available at: https://www.handbook.fca.org.uk/handbook/SYSC/3/1.html (last accessed October 10, 2016).

[51] Section 6.3 is available at: https://www.handbook.fca.org.uk/handbook/SYSC/6/3.html (last accessed October 10, 2016).

[52] Financial Conduct Authority, *Anti Money Laundering Annual Report 2013/14* (July 2014).

[53] For discussion in the context of Bitcoin, see ch.9 (Egan) in this collection.

[54] FCA (n.74), p. 12. **please confirm cross-ref when complete.

[55] FATF, *Virtual currencies: key definitions and potential AML/CFT risks* (Paris: FATF/OECD, 2014); FATF, *Guidance for a risk based approach. Virtual currencies* (Paris: FATF/OECD, 2015); European Banking Authority, 'EBA opinion on virtual currencies' EBA/Op/2014/08. 4 July 2014.

The FATF has acknowledged that virtual currencies such as Bitcoins are an important emergent payment system as well as posing a money laundering and terrorist financing threat to the world.[56] The purpose of the 2014 FATF report was to provide a common definition from which legislators and regulators can work to combat money laundering and terrorist financing risks. The definition of virtual currencies proposed by the FATF ignored the currencies used by virtual worlds and concentrated on whether it is a medium of exchange, a unit of account and a store of value.[57] The EBA however does encompass virtual worlds as coming under the definition of virtual currencies.[58]

The FSA noted some potential risks of virtual currencies, namely the anonymity issue of virtual currencies where transactions take place over the Internet where little anti-money laundering controls can take place, such as know your customer due diligence.[59] Further potential issues relate to the jurisdictional reach of transactions involving complex infrastructures which make it very difficult for anti-money laundering and terrorist financing compliance and supervision.[60] Additionally the FATF report notes that the rapidly changing nature of decentralised currencies makes it very difficult for regulation to keep pace with the technology and infrastructure.[61]

The FATF reported in 2015 that only convertible virtual currencies - ones which can be converted into real world currencies - pose a money laundering threat.[62] This definition thereby excludes virtual world currencies which cannot be exchanged from the virtual world to the real world. However, it does encompass some virtual world currencies such as Linden Dollars.

The EBA's report in 2014 provides the most comprehensive and inclusive definitions and risks associated with virtual currencies. This is because it does not exclude virtual

[56] FATF, *Virtual currencies: key definitions and potential AML/CFT risks* (Paris: FATF/OECD, 2014)p.3.
[57] Ibid, p.4.
[58] European Banking Authority, 'EBA opinion on virtual currencies' EBA/Op/2014/08. 4 July 2014.p.10.
[59] Financial Services Authority (2003) Reducing Money laundering Risk. Discussion paper 22. http://www.fsa.gov.uk/pubs/discussion/dp22.pdf accessed 2 September 2016; Gov.Uk. (2013) Money laundering regulations. Your responsibilities. https://www.gov.uk/guidance/money-laundering-regulations-your-responsibilities accessed 2 September 2016.
[60] FATF (n.78), p.10. *please confirm cross-ref when done.
[61] FATF (n.78), p.10. *please confirm cross-ref when done.
[62] FATF, *Guidance for a risk based approach. Virtual currencies* (Paris: FATF/OECD, 2015)p.6.

world currencies and also provides a list of over 70 potential risks that the currencies exhibit.[63] The EBA directly comments on the money laundering and terrorist financing risks posed by virtual currencies.[64] The report notes that, as virtual currencies do not require personal identification and take place peer-to-peer, the risk is high that money laundering could occur. They also note that, due to the lack of a third party intermediary, there are no reporting mechanisms available. The report also notes that due to the transactions being based online, there are jurisdictional issues related to the lack of borders within the Internet. As such the risk that money launderers and terrorists could use these currencies as a means of financing criminal activity is high.[65]

The potential risks have been clearly outlined and countries are working towards applying anti-money laundering and counter-terrorist financing regulations to virtual currencies.

Different countries have dealt with regulating virtual currencies in different ways. For example, Australia is in a transition to encompass virtual currencies into their anti-money laundering legislation, the Anti Money Laundering and Counter Terrorism Financing Act 2006.[66] The UK is somewhat lagging behind others when historically their progressive and forward-thinking regulation has demonstrated the government's knowledge of criminal activity in this area. In 2015 the UK Government stated that it intends to apply anti-money laundering regulations to virtual currency exchanges.[67] Canada is taking a risk-based approach to dealing with virtual currencies and in 2014 amended its anti-money laundering/ counter terrorist financing regulations to treat those engaged in dealing with virtual currencies as money service businesses.[68] China, requires any business involved in virtual currencies to comply fully with anti-money laundering and counter-terrorist financing regulations.[69] Hong Kong has taken a very cautious approach and not conceded that virtual currencies fall under anti-money laundering or terrorist financing regulations but has reminded its citizens of the

[63] EBA (n.80). *please confirm cross-ref when done.
[64] EBA (n.80), p.32.
[65] EBA (n.80), p.32-33.
[66] Anti-Money Laundering and Counter Terrorism Financing Act 2006. Act No. 169 of 2006. For discussion of the Australian AML framework, see ch.11 (Chaikin) in this collection.
[67] Supra n.81, p.21. **see comment in text above, re supra.81, and the FATF report. If reference here, and subsequently, is all to FATF report – can you update the cross ref.
[68] Supra n.75, p.15.
[69] Supra n.75, p.15.

criminal dangers that virtual currencies may pose.[70] Italy has taken a very strict approach and has specified that virtual currencies are not legal tender and warned financial intuitions against dealing in any form of virtual currencies. A reminder of anti-money laundering regulations was also given to financial intuitions.[71] Russia too has taken a strict approach issuing guidance which states that any transactions involving virtual currencies will be viewed as a potential engagement in illegal activity. To prevent money laundering from occurring in virtual currencies the Russian government has drawn up a Bill banning electronic monetary surrogates and electronic money surrogate's transactions.[72] Singapore has dealt with the issue of mitigating money laundering risks in virtual currencies differently again, as they have decided to regulate virtual currencies intermediaries and pass laws which are aimed at preventing the risks. These new regulations have not yet been implemented.[73] Switzerland has also issued guidance on encompassing virtual currencies transactions within existing money laundering regulations.[74] This is in contrast to South Africa, where there are currently no laws or regulations governing virtual currencies and their use, and as such virtual currencies are not legal tender which offers users degrees of safety when using them.[75]

From the above survey, it is clear that different jurisdictions deal with virtual currencies and the implications for anti-money laundering regulations differently. Given the cross border nature and money laundering disdain for jurisdictional lines of virtual currencies, these variances of approaches pose huge problems for international regulators. International cooperation and regulations are needed to ensure money laundering risks are mitigated and consumers are safe in their monetary transactions where virtual currencies are being used legitimately. This can only be achieved when there are benchmark standards globally on how virtual currencies are treated.

[70] Supra n.75, p.18.
[71] Supra n.75, p.19.
[72] Supra n.75, p.19.
[73] Supra n.75, p.19.
[74] Supra n.75, p.20.
[75] Supra n.75, p.20.

Analysis and Reflection

The UK's position is tenuous at best in terms of understanding, monitoring and regulating virtual money laundering. This diffidence arises for several reasons. There are no precise and delimitative definitions of what constitutes a virtual currency. The EBA, FATF and FCA all see virtual currencies as composing of different things. The most comprehensive is the EBA which does include currencies emanating from virtual worlds as long as they can be exchanged for real world currencies. The FATF and FCA neither provide guidance for this distinction nor include virtual world currencies as being part of virtual currencies. Governments, domestically and internationally, need to agree on a uniform definition in order to provide clear and comprehensive regulation. Without such then there are black holes and confusion. There is enough confusion and bifurcation of opinions as to whether virtual currencies should be regulated or not, without a lack of a suitable definition as to whether they include virtual world currencies.

A further issue stemming from the above is that without including virtual world currencies within the virtual currencies definition, a vast array of different environments are being ignored by the anti-money laundering regulatory landscape and as such pose a potential and real threat to anti-money laundering and terrorism financing laws. Virtual worlds can and do have criminal activities taking place within them, and the lack of regulation allows criminals a safe harbour for their illegal transactions. In short, virtual world environment are being ignored because of the lack of understanding of what they are and how they work. The monetary exchanges are also not being included within virtual currencies monetary exchanges because of virtual worlds being excluded from the definition of virtual currencies.

The piecemeal approach to legislation is not just confined to the UK but applies internationally as well. There is a lack of international agreement as to how to tackle and regulate virtual currencies. In some instances, monetary exchanges are being encompassed under the anti-money laundering regulations, some countries tackle the taxation issues, but none include virtual worlds within their definition of virtual currencies and potential regulations for anti-money laundering issues.

Therefore, although virtual currencies are coming to be seen as a potential money laundering risk, including virtual world currencies, The very definition of virtual currencies is *ad hoc* at best. The EBA does include virtual worlds within its definition and this is to be welcomed, but countries such as the UK need to make a definitive statement that virtual world currencies fall under the virtual currencies definition and as such become subject to relevant anti-money laundering regulations. Without a clear and precise statement, domestically and internationally, virtual worlds will continue to be a safe haven for money laundering and terrorist financing.

Selected Bibliography

Bell, M. W. ‘Towards a definition of virtual worlds’, Journal of Virtual World Research, Vol. 1. No. 1. July 2008, ISSN: 1941-8477.

Brenner, S. W. Is there such a thing as a virtual crime’, 4 Cal Crim. Law Review, 1, 105-11, (2001).

Castronova, E. ‘Virtual Worlds: A first-hand account of market and society on the cyberian frontier’, CESifo Working Papers, No.618, December 2001.

Catronova, E. ‘On Virtual Economies’, CESifo Working Papers, No. 752. July 2002.

Desguin, H. ‘Money laundering through virtual games’. Strategic assessment. Florida Department of Law Enforcement, Office of Statewide Intelligence, October 2008. p.17.

Dribble, J. ‘A Rape in Cyberspace’, Village Voice, Vol XXXVIII, No 51, December 1993.

European Banking Authority. (2014) EBA opinion on virtual currencies. EBA/Op/2014/08. 4 July 2014. https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf accessed 2 September 2016.

FATF (2014) Virtual currencies: key definitions and potential AMONEY LAUNDERING/TF risks. June 2014. http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-amoney laundering-cft-risks.pdf accessed 2 September 2016.

FATF (2015) Guidance for a risk based approach. Virtual currencies. June 2015. http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf accessed 2 September 2016.

Financial Conduct Authority (2016) Money laundering and Terrorist Financing. https://www.the-fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing accessed 2 September 2016.

Fraud Advisory Panel. ‘Cyber Crime: Social Networking and virtual worlds’, Issue 4, October 2009. http://www.fraudadvisorypanel.org/new/pdf_show.php?id=119 accessed 15 July 2010.

Lastowka & Hunter, Virtual Crimes New York Law School, (pending publication) at 14-21.

Lessig, L. ‘Code and other laws of cyberspace’, Basic Books. 74-78, (1999).

Yoon. U-G. ‘Real money trading in MMORPG items from a legal and policy perspectives’. Social Science Research Network. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1113327 accessed 26 May 2011.