TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Department of Law

Raiko Pajula

ONLINE MULTIPLAYER IN-GAME ASSETS AND THE MISUSE OF THEM

Master's thesis

Programme in Law, specialization Law and Technology

Supervisor: Agnes Kasper, PhD

TALLINN 2018

I declare that the I have compiled the paper independently

and all works, important standpoints and data by other authors

have been properly referenced and the same paper

has not been previously been presented for grading.

The document length is 18085 words from the introduction to the end of conclusion.

Raiko Pajula ……

(signature, date)

Student code: 162871HAJM

Student e-mail address: Raikopajula@gmail.com

Supervisor: Agnes Kasper, PhD:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

Contents

AML - European Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

EULA - End user license agreement

GDPR - European General Data Protection Regulation

MMOG - Massively Multiplayer Online Game

OFSP - Online Financial Service Provider

ABSTRACT

Online multiplayer games have become multi-billion-dollar businesses. Since Internet has no borders, the traffic flows from one continent to another. The same principle stands in online multiplayer games, as many players of the game can connect to the game network in different places in the world, thus creating a community. When there are no borders and people all around the world can connect to a game, there are certain problems to be faced.

Online multiplayer gamers discovered that their in-game assets had real world value, they started to make money out of it. The reason why players would spend money on an in-game asset, for example a sword or a better helmet, is to gain advantage in the game itself.

Some people make a living out of the demands of other players and their focus is only on the leveling of characters and collecting valuable in-game assets. At the beginning of this phenomenon, companies reacted furiously, because they did not want a new marketplace, that was not in their control, to form and start making huge profits. But some companies saw a profit out of this new trend. Some companies made an official marketplace themselves, that has all the same actions and offers in it, the companies made revenue from their marketplace and they could control it in some matter.

Marketplaces became very popular and some gamers started to make a living through selling in-game items. With popularity in marketplaces and the frequency of transactions lured in people, who wanted to take advantage of the marketplace and use their illegal money to anonymously launder it clean.

This paper analyzes the aspects on money laundering through online multiplayer games in-game assets, bring out different methods and examples and how law enforcement can react to those new methods.

The research question, this paper intends to answer is, what legal gaps prevent prosecution of money laundering using online multiplayer in-game assets.

Key words: money laundering, end users license agreement, online multiplayer games, in-game assets, marketplace, AML, Estonian legislation.

1. INTRODUCTION

Online multiplayer games have become multi-billion-dollar businesses.[1] Since Internet has no borders, the traffic flows from one continent to another. The same principle stands in online multiplayer games, as many players of the game can connect to the game network in different places in the world, thus creating a community.[2] When there are no borders and people all around the world can connect to a game, there are certain problems to be faced. In this paper, some of the problems concerning online multiplayer games are looked at. More precisely, how online multiplayer games are used to launder money using the games in-game assets.

Actions, that most people see as immoral actions are classified as cheating in online worlds. In this paper, cheating is considered as using one's actions to hide illegally obtained money and using online multiplayer games and in-game assets to make the money seem legally obtained. This can happen in this paper aim, and it poses new moral and legal questions[3] that this paper intends to answer.

Internet access and use is widespread and continues to attract more people each day.[4] A survey conducted by Forester Research Inc. looked over 30,000 people in the United States in January and February 2010 and found that for the first time ever, the average household spends as much time online as it does watching TV offline, with a growth of 121 percent since 2005.[5] To show that the United States is not the only country, where online activity and gaming included, becomes more popular every year. A survey that was conducted in China by the China Internet Network Information Center in 2006 and found, that 120 million Chinese played at least one online game.

---

[1] Constantiou, I., Legarth, M. F., Olsen, K. B. (2011). What are users' intentions towards real money trading in massively multiplayer online games? – *Electron Markets*, Vol. 22, 105-115, p. 105.
[2] Yan, J. J., Choi, H.-J. (2002). Security issues in online games. – *The Electronic Library*, Vol. 20, No. 2, 125-133, p. 125.
[3] Wu, Y., Chen, V. H. H. (2013). A social-cognitive approach to online game cheating. – *Computers in Human Behavior*, Vol. 29, 2557-2567, p. 2557.
[4] Pyrooz, D. C., Decker, S. H., Moule Jr, R. K. (2015). Criminal and Routine Activities in Online Settings: Gangs, Offenders, and the Internet. – *Justice Quarterly*, Vol. 32, No. 3, 471-499, p. 472.
[5] Wang, Q.-H., Mayer-Schönberger, V., Yang, X. (2013). The determinants of monetary value of virtual goods: An empirical study for a cross-section of MMORPGs. – *Information System Frontiers*, Vol. 15, 481-495, p. 481.

Furthermore, the study found that people spent 7,3 hours per week on average and 21 percent of the participants played more than 10 hours a week.[6] These surveys show that online activity and more precisely, online gaming is increasingly more popular every year. This means that more individuals are attracted to all the activities online and this has a double edge effect. More people means more activity and therefore more traffic to monitor by the authorities and game developers. Acting as a cover, criminals can use the traffic, to mask their intentions and actions. If criminals would be the only few, who actively use the Internet, they would be caught immediately, but when there are millions of honest users using the Internet, they can mask their activities so that they are hard or almost impossible to detect.

This thesis will provide legal analysis of online multiplayer in-game assets and money laundering. Focus shall be put on Estonian and European legislation and how, if at all, they regulate or apply to virtual environment. European Union legislators have continued the efforts to combat money laundering, through persistent legal updates, that every European Union Member State must follow.

This paper will analyze the end users license agreements (hereinafter EULA), that sets out the rights and obligations of game developers and players. As a case study, the author will use one of the most popular games EULA as an example to analyze whether EULAs should convey all rights and obligations between the game developer and players.

To further improve this paper legal context, the author of this paper will analyze multiple court cases, which are similar and found in different jurisdictions and compare them to the European Union Member States court decisions and laws. The legal analysis will mainly focus on the European Union legislation(s) and take Estonian legislative acts as reassurance that both legal aims are bound together.

[6] Kshetri, N. (2009). The evolution of the Chinese online gaming industry. – *Journal of Technology Management in China*, Vol. 4, No. 2, 158-179, p. 158.

The methodology used in this paper consists of analysis of different legal texts and articles. Additionally, thesis reviews different court cases and court opinions around the world within the scope of thesis' research aim.

The aim of the research is to highlight and find a way to prosecute money laundering, that is done with an online multiplayer games asset. The research task is to draw attention and understand how money laundering is done with multiplayer game in-game assets.

The research question this masters' thesis aspires to answer is the following:

What legal gaps prevent prosecution of money laundering using online multiplayer in-game assets?

This paper will be divided into five different main chapters. The first chapter will give a short description of online multiplayer games and what are in-game assets. The second part will focus on the existence and effect of end users license agreement and why it should not be used in this paper. The third chapter will analyze money laundering through in-game assets and give appropriate examples from academic articles and court cases. Furthermore, this paper will analyze how the Estonian and European Union legal regimes manage to set rules on money laundering with in-game assets. The author of this paper will give his own view how to better counter money laundering through online multiplayer games and in-game assets.

2. BACKGROUND OF ONLINE MULTIPLAYER GAMES AND IN-GAME ASSETS

Difference between virtual worlds and physical worlds is that, the real world can be defined as activities that exist purely in a real physical space, where humans interact. A virtual world is everything that exists in the digital space only. In this paper, virtual worlds are defined as an avenue for social interaction and a venue for hundreds of thousands of people to join in existing scenarios, all in digital space. Virtual world games are dynamic environments where individual game players can personalize their game experience through the collection of in-game assets, where they have different quests to complete and interact with other game players. These virtual world games usually have an active ecosystem, that provides players with additional game dimensions that are related to the game.

It is important to note, that the virtual world game environment, the interaction between game players is controlled and maintained by the developers of the game, not the players themselves.[7] This is the key for creativity and creation of such environments and the cause of problems, that underline virtual money laundering.[8]

Game developers make virtual games more personal to players and give them more personal approach and experience to the game, by allowing things such as unique game characters and allowing players game-characters use virtual in-game assets. These actions help game players to develop more personal and psychological bond to the game. The attachment, the player develops to the game, as well as to the game character and the virtual possessions the player owns, holds a psychological value for the player and on other side, it holds real world monetary value, a side of the game that can have a negative effect to both players and the game.[9]

[7] Patterson, N.C., Hobbs, M. (2010) A Multidiscipline Approach to Governing Virtual Property Theft in Virtual Worlds. – *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience*, IFIP Advances in Information and Communiaction Technology, Vol. 328, 161-171, p. 161.
[8] *Ibid,* p. 162.
[9] *Ibid,* p. 162.

Through technological improvements and greater processing power, network connectivity increased, game developers started to develop and design larger multiplayer games. Although at the beginning they still were limited to textual descriptions, the difference then was that players could only interact with each other on a limited basis. The first online multiplayer games were developed as non-commercial, as they were developed by gamers themselves.[10] As computer hardware improved, so did game graphics and designs.

The development of computer hardware brought by a new era of computer games. Commercial games were being developed and through increasing broadband connectivity, individual household had stable Internet access. Through time and development, commercial games became more complex, with a huge variety of different themes, a wide array of races, creatures and objects. Some games were developed as more of a social contact point, rather than quest and action oriented. These virtual worlds became places where one was able buy and sell virtual items for real world money as well. [11]

One of the biggest successes in multiplayer games is a game called *World of Warcraft*, the game developer has claimed, that they have more than 8 million game subscribers all around the world. The game features a large open map, that players can roam around. The storyline consists of two different factions of alliances. These alliances are at constant war with each other and the game players act out these conflicts as quests. Although all quests are not aimed against the other alliance, the constant battling draws the attention of players and keeps them at the game. Due to the fact, that the number of players in *World of Warcraft* is so high, the sheer mass of players makes the game more complex virtual economy.[12]

2.1. Individual experience in online multiplayer games

When an individual wants to play an online multiplayer game, they first must purchase a copy of the game. Today, the game developers have designed the game copy on a virtual platform

[10] Kennedy, R. (2009). Law in Virtual Worlds. – *Journal of Internet Law.* Vol. 12, Issue 10, 3-10, p. 10.
[11] *Ibid*, p. 4.
[12] Manninen, T., Kujanpää, T. (2007). The Value of Virtual Assets – The Role of Game Characters in MMOGs. – *International Journal of Business Science and Applied Management,* Vol. 2, Issue 1, 22-33, p. 24.

as well as physical disks. This has improved the sales of games because an individual does not have to go to a store or order a physical disk online, rather they can purchase a digital key for the game online and download the game from the developer's website.

When the game is bought, the buyer must install the software and connect to the Internet. Before the individual can play the game, he/she must design an avatar or choose a character. This is a virtual representation of the player itself in the virtual world. The players choices determine the avatars physical characteristics and skills, attributes the avatar has. This means that the player chooses how the avatar looks like, what are its skills and abilities. This selection narrows the avatars abilities, for example, the player must choose if their character is strong or fast. [13]

When the creation of the avatar is complete, the avatar is then placed in the virtual world, where the player controls its movements and actions. The player can interact with other players through the avatar and the game function designed by the game developer. At the beginning of the game, the avatar has little or no money, very few attributes and abilities and the player must invest time and, in some games, monthly subscription fees, in order to be able to engage in the games activities.[14]

In the game, an avatar can obtain property in virtual objects. These virtual objects can be obtained through completing quests, killing creatures, battling with other players. For players, the action of collecting, exchanging and consuming resources is vital in most online games. They help the player to achieve better results and gain skill points, that improve the avatars levels.[15] Through these actions, the player gains more powerful in-game assets and better skill to get higher scores and participate in more tedious quests.

[13] Kennedy, R. (2008). Virtual rights? Property in online game objects and characters. – *Information & Communications Technology Law*, Vol. 17, No. 2, 95-106, p. 98.
[14] *Ibid*, p. 98.
[15] Webber, N. (2014). Law, culture, and massively multiplayer online games. – *International Review of Law, Computers & Technology*, Vol. 28, No. 1, 45-59, p. 47.

These virtual objects or in-game assets have the same features as objects in physical world, as they do not fade after each use and are not run on one computer, rather in the servers. These virtual assets share every attribute with physical property, even though they do not exist in the physical world.[16]

The game character has exclusive ownership over the asset, right of persistence, right to transfer the asset under certain conditions and the asset trade is supported by a currency system. Avatar can sell the property within the game to other avatars or to the games merchants, that have been put there by the game developers and who are programmed to buy and sell the in-game assets. Avatars can have bidding wars between each other, to buy the in-game asset from another avatar, this action has the same characteristics as physical auctions.[17]

These trading's generally take place in defined and well-known marketplace areas in the game itself.[18] But in some cases, these marketplaces and trading posts are in the gray area, where game developers cannot control the environment and thus can lead to money laundering utopias, that this paper aims to bring out, analyze and suggest legal actions to counteract these illegal activities.

2.2. Background of in-game assets and trading

Most multiplayer online games do not require much skill to master the game as they are rather easy to play but require a lot of time and effort to rise onto a higher skill and ability levels. This opened a new dimension of the game. Game characters, experience levels and items started to be sold by players themselves in marketplaces that are not governed by the game developers.

[16] Adriana, A. (2010). Beyond griefing: Virtual crime. – *Computer law & Security review,* Vol. 26, 640-648, p. 641.
[17] *Ibid,* p. 642.
[18] *Ibid,* p. 642.

For example, companies such as *Gamepal.com*[19] developed marketplaces where they bought and sold characters, levels, in-game gold and other valuables, that can be used in the game. One of the games involved was *World of Warcraft*. In the marketplace, a character of level 50-60 can be valued between $200 and $400 US. [20]

Marketplaces give players a shortcut, if they find leveling and low-level quests boring and give them the solution to buy a higher-level character and participate in a higher-level activity.[21] This of course affects the game developers negatively, because player will not invest their time and thus subscription fees in the game, but rather buy a high-level character and jump to the top of the game.[22] This is called real-money trading and it has grown in popularity in recent years.

Some people make a living out of the demands from the market and they focus is only on the leveling of characters and collecting valuable in-game assets. At the beginning of this phenomenon, companies reacted furiously, because they did not want a new marketplace, that was not in their control, to form and start making huge profits. But some companies saw a profit out of this new trend. Some companies made an official marketplace themselves, that has all the same actions and offers in it, the companies made revenue from their marketplace and they could control it in some matter. [23]

Other companies made currency directly convertible to real-world currency or made an in-game debit card that allowed players to access game money in the real world.[24] For example, a game called *Lineage Online*, the virtual currency exchange rate was 2,500 virtual currency to $1 US in August 2002.[25]

---

[19] Gamepal. Available at: http://www.gamepal.com/content.php Last accessed: 11.03.2018.
[20] Manninen, T., Kujanpää, T. (2007). The Value of Virtual Assets – The Role of Game Characters in MMOGs. – *International Journal of Business Science and Applied Management*, Vol. 2, Issue 1, 22-33, p.29.
[21] *Ibid*, p. 29.
[22] Taylor. T. L. (2002). „Whose Game Is This Anyway?": Negotiating Corporate Ownership in a Virtual World. – *Proceedings of Computer Games and Digital Cultures Conference*. Frans Mäyrä. Tampere. Tampere University Press, 227-242, p. 231.
[23] Kennedy, R. (2009). Law in Virtual Worlds. – *Journal of Internet Law*. Vol. 12, Issue 10, 3-10, p. 4.
[24] *Ibid*, p. 4.
[25] Chen, Y.-C., Chen, P. S., Hwang, J.-J., Korba, L., Song, R., Yee, G. (2005). An analysis of online gaming crime characteristics. – *Internet Research*, Vol. 15, No. 3, 246-261, p. 247.

Some games have microtransactions developed in the game itself, these are small transactions players can purchase from the developers themselves and it contains some small in-game asset that the player can use. The argument that microtransactions can boost the players commitment by increasing the players degree of investment[26] is in the author's opinion an overestimate, rather it is another way for developers to make money.

In the authors opinion, in-game assets like game-gold can be used to make a profit by the players and small transactions that have been put in the game by the developers are just a way to make more money out of the game. With the rise in gaming popularity, many have found it as a way to move criminal activities out of the physical space and into virtual, which gives rise to game-related crimes.

Other examples of virtual assets sold in places like *eBay*[27] and other similar web sites have proven that the value of in-game assets exceeds in some cases real property value. A virtual representation of Amsterdam in a game *Second Life* was sold for $50,000 US and a virtual space station in a game *Project Entropia* was sold for $100,000 US.[28] These numbers should show how virtual game assets have grown in value and when such currency changes hand, it will normalize in the gaming community, these actions can mask the criminal side of things.

Money laundering with a large quantity then does not shine like a bright star alone in the exchange rates or does not pop up as the most expensive thing bought or sold. In the authors opinion, when legal exchanges amount to so high numbers, criminals can use it to mask their own actions and it would not bring suspicions to others as illegal activities rather than normal actions of players, who are wealthy and want to buy a virtual property or other virtual assets.

Understanding, which trade or action in the virtual world is done with illegal intent and which is done by an honest player will be extremely difficult for the game developers and law

[26] Uysal, A. (2016). Commitment to multiplayer online games: An investment model approach. – *Computers in Human Behavior*, Vol. 61, 357-363, p. 362.
[27] eBay. Available at: https://www.ebay.com/ Last accessed: 11.03.2018.
[28] Kane, S. F. (2008). Virtually Lawless: Legal & Economic Issues in Virtual Worlds. – *The Computer & Internet Lawyer*, Vol. 25, No. 6, 13-24, p. 14.

enforcement. This is due to the fact, that most actions in the virtual world can be done anonymously.[29] Making it difficult to identify the person or even the country, they reside.

In online games, the assets, for example: virtual swords, equipment or cosmetic designs, are limited and virtual asset development costs money, time and energy. These markets flourished with new means of finding the right combination or right design for some players liking and for others, as means to hide their valuables or to quickly get rid of stolen in-game assets.[30]

Although not all games provide an official outlet or even if they do, players can still turn to secondary marketplace for better prices or faster response. The difficult part is to determine the value of those marketplaces as most of them are black markets, not sanctioned or even permitted.

In this paper, the key focus will be on the in-game assets and how they are used to launder money in those black markets[31]

Game developers face another obstacle with in-game assets. The side of bankruptcy or other means of going out of business, can lead to massive court cases due to damages they caused to their game players. When the game has developed in-game assets that are worth a lot of money and they are all lost due to the companies' closure, the developers can be sued, if they do not compensate their players for their loss.[32] Players in the virtual games hold property, that may have monetary value and thus the developer must consider the players side as well, when facing closure.

[29] Luppicini, R. (2014). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. – *Global Media Journal – Canadian Edition*, Vol. 7, Issue 1, 35-49, p. 36.
[30] Chen, Y.-C., Chen, P. S., Hwang, J.-J., Korba, L., Song, R., Yee, G. (2005). An analysis of online gaming crime characteristics. – *Internet Research*, Vol. 15, No. 3, 246-261, p. 247.
[31] Kennedy, R. (2009). Law in Virtual Worlds. – *Journal of Internet Law.* Vol. 12, Issue 10, 3-10, p. 6.
[32] MacInnes, I. (2006). Property rights, legal issues, and business models in virtual world communities. – *Electronic Commerce Research*, Vol. 6, 39-56, p. 47-48.

3. END USER LICENSE AGREEMENTS AS TOOLS FOR CONTROLLING GAME ENVIRONMENTS

To start off with this chapter, it is necessary to define the end users license agreement and explain, why it is not as effective and controlling as game developers hoped it would be.

EULA regulates the relationship between the players and game developers as it regulates their rights, obligations and responsibilities. Further, the reader shall be introduced to most important aspects of EULA while highlighting the cons of this agreement. Especially when it comes to money laundering aspects.

To start with the EULA, it is important to look further, how legislators have seen multiplayer game disputes, that arise between game players themselves or players against game developers. There is a so called "magic circle" which is stated by the multiplayer game researchers. It states to an artificial context that is created by the rules of the game and therefore it is separate from the real world.[33] This concept between fantasy realm of the virtual worlds of computer games and the non-virtual worlds was originally derived from a Dutch philosopher Huizinga and the "magical circle" meant that everything done in a computer game setting in not real and therefore cannot be sanctioned in the real world by real law.[34] In this sense, game developers have created EULAs to regulate games. This is the developer's way of law, saying that the "magic circle" is not broken and all in-game regulations are done by the EULA.

EULAs are virtual contracts, that all players must agree, before they can play the game or even enter the games environment. When a player clicks the agreement box, they waive a

[33] Constantiou, I., Legarth, M. F., Olsen, K. B. (2012). What are users' intentions towards real money trading in massively multiplayer online games? – *Electron Markets,* Vol. 22, 105-115, p. 108.
[34] Strikwerda, L. (2012). Theft of virtual items in online multiplayer computer games: an ontological and moral analysis. – *Ethics and Information Technology,* Vol. 14, 89-97, p. 91.

significant amount of their rights, including right to own the fruits of labor, right to assemble, right to free speech.[35]

Almost every virtual game has a clause in their EULA, that requires players to assign the rights of all property created in-game to the developers of the game.[36] For example, the EULA of *Blizzard Entertainments* game *World of Warcraft* states:

"With the sole exception of the Licensors' Games, Blizzard is the owner or licensee of all right, title, and interest in and to the Platform, including the Games that are produced and developed by Blizzard, Custom Games derived from a Blizzard, Accounts, and all of the features and components thereof. The Platform may contain materials licensed by third-parties to Blizzard, and these third-parties may enforce their ownership rights against you in the event that you violate this Agreement."[37]

With the required acceptance of the EULA, players give away significant rights that may hold value for players stating that all association with the players accounts and attachments with the accounts belong to Blizzard. The acceptance includes all virtual items that are present in the game, ranging from currency to weapons, armor and pets. The exclusion of player ownership highlights the difficulties associated with in-game asset money laundering.

Taken from this example EULA, many argue that there is no need to look further than the EULA, because it controls what can and cannot be done and who has the ownership over virtual assets in the virtual world.

In a court case *Bragg vs Linden Research, Inc.* made an interesting and changing effect to the EULA. Linden Research, Inc. (hereinafter Linden) owns a game called *Second Life* and the

[35] Grimes, S. M. (2006). Online multiplayer games: a virtual space for intellectual property debates? – *New media & Society*, Vol. 8, No. 6, 969-990, p. 981.
[36] Adrian, A. (2010). Beyond griefing: Virtual crime. – *Computer law & Security review*, Vol. 26, 640-648, p. 642.
[37] BLIZZARD END USER LICENSE AGREEMENT Available at: http://us.blizzard.com/en-us/company/legal/eula Last accessed: 14.03.2018.

developers argument against the individuals claim, was to refer to the EULA, which stated that individuals account belongs to *Linden* as their property and they can do whatever they would like, for example close the account without cause or compensation to the player.

The reason, why the court did not agree with the statement, because *Lindens* other advertisement stated against their initial argument. This is because *Linden* advertised that all Intellectual Property rights that a player has in the game, so to say everything a player designs or builds in the game, belong to the player. To this, the court stated, that *Second Life* EULA is unusable and therefore could not be the basis of dismissal of the court case.[38]

As this case is a small victory for the players, who wish to have more rights in the virtual world, the bigger problem is mainly to the developers, who can see that the almighty EULA does not defend them in every situation and the need for change may be needed.

Companies' faith in EULAs to protect them from litigations, by stating that virtual in-game assets do not have monetary value, may also bring an end to the overall use of EULA. When courts find that EULAs are too one sided, favoring the developers and taking away basic rights from the players and that the virtual in-game assets, that players have obtained during playing the game hold value to the players or the theft of the virtual in-game assets from the players was caused by a security flaw.[39]

When we take the rights of players, that they must forfeit to play the game may exceed the moral line. Developers argument that they wish to protect their investments and the game itself while controlling foul language is noble, the argument might not stand for long.

[38] Kane, S. F. (2008). Virtually Lawless: Legal & Economic Issues in Virtual Worlds. – *The Computer & Internet Lawyer*, Vol. 25, No. 6, 13-24, p. 16.
[39] Patterson, N.C., Hobbs, M. (2010) A Multidiscipline Approach to Governing Virtual Property Theft in Virtual Worlds. – *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience*, IFIP Advances in Information and Communication Technology, Vol. 328, 161-171, p. 169.

As technology is improving and everything is moving to the digital age, the EULA might not stand against the rights of individuals. Courts may soon find a different route, focusing more on the protection of the individual player and therefore be more invested in the disputes. This in turn will cause the EULA to be modified or outright banned by the courts.

When monetary value is placed in the argument and the developers argue that they forbid copying in-game assets, to preserve the value and rarity, the same principle can overturn the EULA. As monetary value comes from players trading the in-game assets for real money, the argument comes from the players. As the trading of in-game assets can be seen as an exchange of the right to use the in-game asset.[40]

Therefore, taking from the EULA that is in effect right now, the players do not infringe it. Developers on the other hand do not see this as the right to use rather, they see it as infringement of their right of ownership, as they point out in the EULA that they own all the property in the virtual world and therefore they forbit the exchange for real world money.

Copyright infringement, meaning that exchanging the in-game assets for real world money, can be overturned by the courts as well. As trading in-game assets does not require copying, making the argument invalid by the developers.[41]

Other values that makes EULA invalid are moral values, right of ownership through time and effort. Additional values, that the EULA takes away from the players are non-monetary values, for instance freedom of speech or right to privacy, as the EULA states that all recordings belong to the game developer. For this, the author argues, that EULA is too one sided and only protects the developers from every infringement.

[40] Kennedy, R. (2008). Virtual rights? Property in online game objects and characters. – *Information & Communications Technology Law,* Vol. 17, No. 2, 95-106, p. 100.
[41] *Ibid*, p. 100.101.

When taking account, the time and effort many players have put to one game, the players should have the right to decide the outcome of their in-game assets. As mentioned before, the court case between a player and *Linden* has brought up many debates. Players argue, that they have put time and effort in the game, to develop some virtual in-game assets and therefore should have property rights over the asset.[42]

To look through the moral value side, the author sees the EULA as a failing argument on the developers' side, as the investment of time and effort, through countless hours of playing the game, to reach a high level, that gives the player social hierarchy, will eventually turn the tables around.

Overturning the EULA is necessary in this masters' paper, as otherwise there would be little debate about the subject of money laundering and in-game asset theft. The EULA states, that all in-game property belong to the game developer and they forbit trading in-game assets to real world money. If that statement would stand, every action that will be analyzed in this paper would be void and the obligation of catching money launderers would fall on the shoulders of the game developers, but this would put too much pressure on the game developers and as stated before, the EULA prohibits players from using their basic rights.

The upcoming sections will analyze money laundering through in-game assets without the game developers' protection of EULA.

[42] MacInnes, I. (2006). Property rights, legal issues, and business models in virtual world communities. – *Electronic Commerce Research,* Vol. 6, 39-56, p. 52.

4. STRATEGIC WAYS HOW TO LAUNDER MONEY IN AN ONLINE GAME

With the advances in technology and as it is increasingly more accessible for individuals, making multiplayer games more popular, criminals have found a new way of doing old things in a different environment.[43]

With the increase in players and thus activity in the multiplayer games, the risk for criminal activity will rise.[44] As criminals will understand that regular players will generate enough traffic in the games servers, to leave them unnoticed or mitigate the risk.

In this part of the paper the author will show a few examples on how money laundering is done through online multiplayer games, describe, how they are achieved and, in the end, show how game developers and governments can counter these actions.

Criminal activity started in the multiplayer online community from the point, where online multiplayer in-game assets started to have value. As soon as people started to understand that in-game assets had monetary value and there are honest users with the intent to trade assets and make money, criminals started using the same tactics to launder money.[45]

It is estimated, that in 2007, the overall aggregate gross domestic product of the major massively multiplayer online games is between 7$ billion and 12$ billion US.[46] Another study found, that 62,2 percent of the total in-game cash flow was free money, that is money that

[43] Pyrooz, D. C., Decker, S. H., Moule Jr, R. K. (2015). Criminal and Routine Activities in Online Settings: Gangs, Offenders, and the Internet. – *Justice Quarterly*, Vol. 32, No. 3, 471-499, p. 475.
[44] Rughinis, C., Rughinis, R. (2014). Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union. – *Computers & Security*, Vol. 43, 111-125, p. 114.
[45] Blackburn, J., Kourtellis, N., Skvoretz, J. (2014). Cheating in Online Games: A Social Network Perspective. – *ACM Transactions on Internet Technology*, Vol. 13, No. 3, Article 9, 9-9:25, p. 9:2.
[46] Kennedy, R. (2008). Virtual rights? Property in online game objects and characters. – *Information & Communications Technology Law*, Vol. 17, No. 2, 95-106, p. 98.

players have put in the game through other methods than buying the game or buying merchandise from the developers. [47]

Furthermore, the study found that, 93,4 percent of the free money is likely related or connected with virtual black markets.[48] These studies show how large money trading in the virtual worlds is and in the authors opinion, most of the money is not achieved through honest trade or investments, but through money laundering.

Further analysis aims to show how simple and anonymous it is to launder money in a virtual world using in-game assets as tools for money laundering.

Money laundering stands for the process where criminals veil the true ownership and control of the revenue of criminal conduct by making the revenue appear to have derived from a legitimate source.

To get a full overview of money laundering and how it is done in the virtual world, this paper will use The Estonian Money Laundering and Terrorist Financing Prevention Act as a legal definition to money laundering. Under the Estonian Money Laundering and Terrorist Financing Prevention Act money laundering is seen as any activity such as the conversion or transfer, acquisition, possession or use of property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such activity. Furthermore, the Estonian Money Laundering and Terrorist Financing Prevention Act widens the scope of money laundering by adding actions, such as the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such an activity."[49]

[47] Woo, K., Kwon, H., Kim, H.- C., Kim, C.- K., Kim, H. K. (2011). What Can Free Money Tell Us on the Virtual Black Market? - *ACM SIGCOMM Computer Communication Review,* Vol. 41 Issue 4. 392 – 393, p. 393.
[48] *Ibid,* p. 393.
[49] Rahapesu ja terrorismi rahastamise tõkestamise seadus §4 RT I, 17.11.2017, 38

As Sean F. Kane has mentioned in an article: Virtually Lawless: Legal & Economic Issues in Virtual Worlds, the International Criminal Police Organization, known as Interpol has defined virtual money as:

> ''Money value as represented by a claim on the issuer which is stored on an electronic device and accepted as a means of payment by persons other than the issuer. Virtual money is an encrypted code representing money, in the same way that paper money is only paper bearing certain characteristics such as graphics and serial number.

Accordingly, there are two types of virtual money:

1. Identified virtual money, which contains information revealing the identity of the person who originally withdrew the money from the bank. This can be traced through the economy, by the bank, or law enforcement personnel, in much the same way as credit cards.
2. Anonymous virtual money, meaning once it is withdrawn from an account, it can be spent or given away without leaving a transaction trail. Using blind signatures rather than non-blind signatures creates anonymous e-money.''[50]

This masters paper will focus on the second type of virtual money, how anonymous money is obtained and how criminals can use virtual worlds and in-game assets to launder money.

Money laundering consists of three stage process: placement, layering and integration. Placement stage is the initial entry of the illegal funds to the financial system. It usually consists of large sums of money, which is most likely cash. This part is difficult for the criminals, because the involvement of large sums of money may attract the attention of law enforcement and it is the breaking point, when criminals get caught in this process, there is a high chance that all their illegal funds will be seized or frozen.

[50] Kane, S. F. (2008). Virtually Lawless: Legal & Economic Issues in Virtual Worlds. – *The Computer & Internet Lawyer*, Vol. 25, No. 6, 13-24, p. 18.

After placement stage, there is layering. Layering methods are different, but all consist of multiple transactions, that are done to hide the origin of the assets. This process needs a thorough and well thought plan from the criminals, as it usually is the most international process of the three. As the money launderers start sending funds through multiple financial service providers, across multiple countries and multiple jurisdictions to evade detection and hide their assets all around the world. The mixture of different countries and jurisdictions help criminals, as some countries law enforcements do not cooperate with each other and the criminals can take advantage of it. Furthermore, criminals can exploit loopholes and inconsistencies in different legislations, making tracking them much harder for law enforcements.

The final stage of money laundering is called integration. This is the point; the funds have traveled across multiple financial service providers and different countries. Tracing the origin of the funds now may seem legal and in this process these funds are transferred back into the economy for criminals to use them for any purpose.[51]

Money laundering through online multiplayer games in-game assets is often committed over multiple jurisdictions which leads to problems both in legal assistance and investigations. Illegal use, interference or interception with computer systems or data is often difficult to track and thus reporting of cybercrime remains one of the main problems tackling this kind of money laundering. As with all crimes, money laundering leaves a trace of evidence, and in online money laundering, this evidence is in electronic format, that is electronic evidence. Which causes diverse legal and technical difficulties in securing and examining such evidence. Due to the length of this paper and the unique approach of money laundering as a subject, digital evidence will not be analyzed in this paper. As digital evidence connected to money laundering, using online multiplayer in-game assets would require extensive analysis through multiple legal systems and overturn several tactics, criminals can use, and which are mentioned in this paper.

[51] United Nations Manual. (2014). Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies. [Online:] https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf. Last accessed: 01.05.2018.

Money laundering in online games has the potential to allow large sums of money to be moved across national borders or even continents with little risk of detection. While traditional ways of money laundering have become difficult or impossible for the criminals, online money laundering has become a problem for the governments.

To illustrate, *Second Life* has a growing environment, that has made many legal experts worry. Because the lack of regulations in the games banks and stock exchange could provide a suitable place for money launderers and frauds to move funds around to avoid surveillance or gain attention the same way as they would do in real life.[52]

The Australian Transaction Reports and Analysis Centre in 2012 stated: "While the nature and extent for money laundering through digital currencies and virtual worlds are unknown, it is important to recognize their potential for criminal exploitation, particularly in response to tighter regulation of established or traditional financial channels."[53]

Money launderers are usually highly educated, with a university degree and with high skill levels. This makes them dangerous, as their skills would be used for illegal activity and through their actions, they can stay under the radar for law enforcement and know how to evade game developers' software, that would detect illegal activities.[54]

While the attention to money laundering has been drawn in 2012, there are little to no direct regulations in effect. In the upcoming sections, the author will bring out different aspects of money laundering and how they are done and through these different methods, the jurisdiction and legal aspects will arise.

[52] Irwin, A. S. M., Slay, J., Choo, K.-K. R., Lui, L. (2014). Money laundering and terrorism financing in virtual environments: a feasibility study. – *Journal of Money Laundering Control,* Vol. 17, Issue 1, 50-75, p. 52.
[53] *Ibid*, p. 51.
[54] Emerald Group Publishing Limited. (2014). Criminals move with the times: Money launderers and terrorism financers go online. – *Strategic Direction,* Vol. 30, Issue 6, 8-10, p. 8.

Virtual money laundering provides a large amount of anonymity, as the risks and chances of detection are reduced. This can be done in the online world only when the actor uses programs, to remove traces of their electronic identity and location every time they access the multiplayer game or website, where they can launder the funds. There are several free programs that people can download and use, to hide their internet usages. For example, Tor[55] is a program, that can be used in order to anonymously use the Internet. Although Tor does not guarantee full anonymity, it does reduce the likelihood for websites trace actions and data back to the user. If those precautions are not done, law enforcement and service providers can track their location and their actions, which may result in custody by the law enforcement.

Further, if money launderers do not use such programs to mask their actions, service providers and law enforcement can see their transactions and trace them, which results in the overall view of the money laundering scheme and their real-life identity can be discovered.

When criminals use all the aforementioned acts to hide their identity and their actions, there is still a chance of the service provider or game developer, to find some of their actions suspicious and they can close these accounts.[56] Closing a virtual multiplayer game account, that has suspicions of money laundering would not have the same effect as closing or freezing a bank account. Less severe consequences to the money launderer is achieved with multiple accounts, with multiple websites and traders.

In the online multiplayer game, money launderers would lose only a small amount of funds and service providers and law enforcement would have a difficult time to connect different accounts with one-another. If one or more accounts of the money launderer is frozen online, the person can open new ones and continue their activity.[57]

[55] Tor.[Online:] https://www.torproject.org/index.html.en. Last accessed: 01.05.2018.
[56] Emerald Group Publishing Limited. (2014). Criminals move with the times: Money launderers and terrorism financers go online. – *Strategic Direction*, Vol. 30, Issue 6, 8-10, p. 9.
[57] *Ibid*, p. 9.

Through the development of technical capabilities, it is now possible for multiplayer games to have commercial transactions with the games assets.[58] In order for a game to stay popular and compete with rival games, interaction between game players is not enough. Game developers designed the games to have in-game assets, for players to have a competition on who has the best armor or best weapon. This made the players stay in one game and play it more frequently and longer, making more profit for the game developers as well.

As this papers focus will be on online multiplayer in-game assets, the subject should not be compared to or thought of as the same as cryptocurrencies. The issue here is, that online multiplayer in-game assets are not just one virtual object or code. There are numerous different in-game assets, from in-game gold, that some games allow to use as a payment, to cosmetic designs and character equipment, that does not reflect a certain monetary value. That does not mean that they do not have a monetary value, it is because their main purpose is to be used in the game as a tool, not as a selling product.

4.1. Popularity of trading in-game assets

Online multiplayer gamers discovered that their in-game assets had real world value, they started to make money out of it. The reason why players would spend money on an in-game asset, for example a sword or a better helmet, is to gain advantage in the game itself.

As mentioned before, many of the players, who would use real world money, to buy an in-game asset are educated working people. As they do not have enough time, to play the game to the extent where they have earned the wanted in-game asset, they turn to marketplaces or in-game trading markets to buy the wanted item.[59]

[58] MacInnes, I. (2006). Property rights, legal issues, and business models in virtual world communities. – *Electronic Commerce Research,* Vol. 6, 39-56, p. 45.
[59] Irwin, A. S. M., Slay, J., Choo, K.-K. R., Lui, L. (2014). Money laundering and terrorism financing in virtual environments: a feasibility study. – *Journal of Money Laundering Control,* Vol. 17, Issue 1, 50-75, p. 65.

Marketplaces became very popular and some gamers started to make a living through selling in-game items. With popularity in marketplaces and the frequency of transactions lured in people, who wanted to take advantage of the marketplace and use their illegal money to anonymously launder it clean.[60]

For example, a money launderer can purchase in-game items with their illegal money, transfer these assets to another account, trade these items in another marketplace with honest users and then resell the traded item for real world money back. Making the transaction seem legal and not rise suspicions of money laundering on the developers' side.

Although the before written example might prove to be too time consuming and only small amounts can be transferred through one account, the money launderers can open multiple accounts and even transfer some of the items between themselves to make up traffic. This model would be seen by the game developer as usual traffic and players changing items between themselves.

Even in the case where one account is frozen, and the user can not have access to it, they can simply make a new account and continue, the loss will be small and the possibility of the developer of connecting one account to another is highly unlikely.

Furthermore, the closure of one account will not affect the criminal in a monetary way, as most of the items will be sold or traded and the ones the account possesses in the time of the freezing would have little impact for the criminal.

Game developers themselves made the demand of trade markets so popular, as they effectively made the game more time consuming, for players to buy more monthly-subscriptions, which meant that players would need to invest more time to achieve the desired

[60] Patterson, N.C., Hobbs, M. (2010) A Multidiscipline Approach to Governing Virtual Property Theft in Virtual Worlds. – *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience,* IFIP Advances in Information and Communiaction Technology, Vol. 328, 161-171, p. 165.

result.[61] Players turned to the markets in order to buy the desired in-game asset or even found other players, who were willing to offer their services as booster. These are players, whose only goal in the game is to get a high enough character, in order to sell it or offer their services to level up other players characters.

4.2. Money laundering activities in marketplaces

Marketplaces popularity became a phenomenon since there are small risks, there are low transaction costs and the bargaining is entertaining. People enjoy the processes which may take place in a marketplace, where you can experiment on how high you can sell your items, and many see it as a hobby.[62]

This can mask the criminal activity, as honest users will try and experiment on selling high and buying low, criminals can use the same tactic to launder money. They can make a lot of accounts, buy low priced items and then sell it to accounts, where illegal money is placed for prices which exceed the market value of the item. With multiple accounts and daily transactions, large amount of money can change hands, without bringing up suspicions of illicit activities.

These actions would not be recognized by the market place owners as illegal activities or money laundering, rather than someone being a fool and buying a cheap in-game asset for a high price.

Some market place owners might not even have security measures in place, for example a red flag indicator, that would show if there is a transaction that would seem illogical, overpriced or overall suspicious. There are marketplaces, where illegal activities are welcomed, as the marketplace owners make a profit from every transaction.

[61] Harviainen, J. T., Hamari, J. (2015). Seek, share, or withhold: information trading in MMORPGs. – *Journal of Documentation,* Vol. 71, Issue 6, 1119-1134, p.1120.
[62] MacInnes, I. (2006). Property rights, legal issues, and business models in virtual world communities. – *Electronic Commerce Research,* Vol. 6, 39-56, p. 40.

In other words, when the owner sees, that their website is used to for large transactions, the fees are substantial and there is little chance of law enforcement interaction, the interference of activities would be highly unlikely. In this example, the marketplace is not owned by the game developers, rather than individuals, who saw the opportunity to open their own marketplace outside the game environment.

If a multiplayer game has a marketplace inside the game, where players can buy and sell their in-game assets for virtual money, this action can have setbacks. When a game itself has a bug or malfunction in the code, which benefits players.

For example, a pricing error, which caused players the opportunity to sell virtual items to the games marketplace at a higher price than they would have to pay to get them. This caused some players to shuffle back and forth with their items and make a lot of virtual money through that. When that virtual money has real monetary value, these players became very rich in a small amount of time.[63]

Mistakes and bugs can have devastating effects on the game economy and game developers' hands are tied in this situation. They themselves provided this environment, where players could misuse the marketplace and make a lot of money for themselves without any effort.

Many games and marketplaces lack regulations, there is no monitoring of financial activity, customer identification processes are nonexistent, and no report system is in place, that would indicate fraudulent behavior. Because multiplayer games have no borders, regulating a game would prove extremely difficult.[64]

As different countries have different view on online multiplayer games, regulating a game in a way that would suit for every legal aspect would prove impossible. The same goes to markets,

[63] Yan, J., Randell, B. (2005). A systematic classification of cheating in online games. – *NetGames,* ACM SIGCOMM workshop on Network and system support for games, 1-9, p. 4.
[64] Irwin, A. S. M., Slay, J., Choo, K.-K. R., Lui, L. (2014). Money laundering and terrorism financing in virtual environments: a feasibility study. – *Journal of Money Laundering Control,* Vol. 17, Issue 1, 50-75, p. 52-53.

as people can set up their own marketplaces in countries, where regulation on virtual assets in inadequate or missing completely, therefore they could not be prosecuted under that countries laws.

The non-existent red flag indicators or behaviors, which can alert the game service providers and law enforcement agencies on the presence of virtual money laundering may have its toll on the overall countering of virtual money laundering around the world. As in traditional money laundering, series of red flag indicators can be detected by financial institutions and law enforcement. As a result, actions and surveillance can be appropriately managed. The same would go to virtual money laundering, as red flag indicators can help law enforcement to start monitoring specific accounts, their transactions and their communications.[65] When overall red flag indicators are missing from the game, there are little to no chance of the game developer to see fraudulent behavior or act accordingly.

The problem of anonymity was analyzed before and described how money launderers can hide their true identity from service providers and law enforcement. There are simpler ways on how anonymity is achieved. The blame is on the game developers themselves, as they have not regulated customer identification methods adequately before the player can start trading virtual assets to real world money. This can lead to game developers accusing the wrong person of money laundering when the person in charge of money laundering has used false or stolen identity.[66]

Furthermore, the ease which it is possible to open new accounts and start financial activity is poorly regulated or there are only a few steps, that a criminal can bypass.[67] For example, most games require credit card number, to buy the monthly subscription for the game and in the meantime can be used as an identification tool for the game developers. Credit card numbers can be stolen, bought from the black market or criminals can even use a fall guy, who could

[65] Irwin, A. S. M., Slay, J., Choo, K.-K. R., Lui, L. (2014). Money laundering and terrorism financing in virtual environments: a feasibility study. – *Journal of Money Laundering Control,* Vol. 17, Issue 1, 50-75, p. 67.
[66] Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. – *International Journal of Law, Crime and Justice,* Vol. 47, 44-57, p. 51.
[67] Irwin, A. S. M., Slay, J., Choo, K.-K. R., Lui, L. (2014). Money laundering and terrorism financing in virtual environments: a feasibility study. – *Journal of Money Laundering Control,* Vol. 17, Issue 1, 50-75, p. 71.

deny everything and just be the front runner. These front runners only goal is to receive a payoff and help true mastermind hide their identity.[68] Simple regulations do not stop someone from gaining access to the game and use it to launder their funds.

Game developers would face difficulties on implementing more strict identification tools in the game. As there are no universal online identification tool in place. For example, requiring players to send a copy of an identification card to the game developers to verify their identity would scare off many new players. Additionally, the European General Data Protection Regulation (hereinafter GDPR) would impede collection of such data, because GDPR lays down very strict rules on processing of personal data.[69] It would make processing of identification card information high maintenance and costly for game developers.

Instead of stricter identification measures, game developers should advance their relationship with law enforcement. Notifying them immediately, when they have closed an account and send the information to the law enforcement. Law enforcement would have the complex situation on determining the correctness of the information, as mentioned before, criminals can use stolen identity cards to open accounts.

Money laundering schemes can use money mules. In traditional money laundering, money mules are used in many ways, as they will open bank accounts in their own name to be used to mask the traffic of the laundered money. They will receive some amount of money, which they will send forward to another person or withdraw and deliver it by themselves manually or send it by post. From this papers topic, money mules are used almost the same way. As they are account holders, who will receive virtual money or real-world currency, they will again send it forward to the next person or withdraw the money and send it in other ways. The money mules take a cut of the sum that is deposited in their bank account, thus earning through the transfer.

[68] Figueroa, N., Huillier, G. L., Weber, R. (2017). Adversarial classification using signaling games with an application to phishing detection. – *Data Mining and Knowledge Discovery,* Vol. 31, 92-133, p. 93.
[69] The European Parliament and the Council of the European Union (EU) No 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119/1, 04.04.2016.

Money mules are usually recruited through internet websites, that advertise work that can be done from home and all is needed is a bank account or they require the money mule to open an account in some virtual money trading marketplace. The people usually do not know who send them the money and they have little interactions with the organizers. If communication is present, it is done through channels that are difficult to monitor. Furthermore, the communication can be scrambled, by using stolen credit cards and using them to buy pre-paid phone cards that are used to communicate with the money mules. All instructions money mules receive, are the date, when the money will arrive, the destination it ahs to be sent and the amount they can take for themselves.[70]

When a money mule gets caught by the law enforcement, they usually do not know who sends them the money and who receives the money, after they have transferred it. Money mules are pawns in the money laundering operation, making them replaceable for the money launderers and little interest for the law enforcement. This phenomenon makes money mules ideal for money launderers, because even when a mule gets caught, their losses are minimal, but they will help them with one of the main actions in money laundering. They are the key part of layering.

As previously analyzed, criminals can use technical measures, to stay anonymous when conducting criminal activities. Money mules, who are hired through false advertisement or misconception rarely use the same techniques to stay anonymous online as criminals do. Because they were not aware the real motivation behind their hiring. As money mules can be monitored by law enforcement with little effort, law enforcement can track their movement online and track the money movement with smaller effort than criminals, who use technical means to hide their identity and money traffic. The author is on the opinion, that law enforcement would have a more successful investigation, when they track money mules and the money directed through them.

[70] United Nations Manual. (2014). Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies. [Online:] https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf. Last accessed: 01.05.2018.

Money launderers can make their own websites and marketplaces, which focus on in-game asset trading. Offering some small discounts for regular players to use their website and generate enough traffic in the website to mask their actions. Meanwhile, they themselves use multiple accounts and associates to buy or sell virtual items using money, they have acquired illegally. These websites can be set up in countries, where virtual money trading regulation is absent, giving them the security, that even if they would be found through another law enforcement agency or even international law enforcement agency, for example Interpol. They would not be prosecuted, because the website is located in a country, where such actions are not penalized.

Furthermore, criminals can use multiple servers to mask their real connection and when the connection runs through multiple continents and countries, it would be difficult for the law enforcement to keep track. Some countries may not even give the pursuing law enforcement the data they need, in order to keep track of the criminals, because the countries policies forbit it.

For example, running the connection through a Nigerian or Russian server would halt western law enforcements pursuits because these countries usually do not want to give out information about their servers and actions inside those servers. This is the problem with modern era. Internet has no borders and no limits, countries on the other hand have different approaches on virtual worlds and in-game assets.[71]

When different legal systems collide, there is little chance of finding common ground and agreeing on what and how it should be regulated. Even if an international agreement is constructed, it still would not be mandatory for every country to ratify it in their legal system. Therefore, it still leaves criminal the opportunity to use those countries servers to conduct their illegal acts and through that, stay away from law enforcement.

[71] Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. – *International Journal of Law, Crime and Justice,* Vol. 47, 44-57, p. 45-46.

As marketplaces in this paper focus on buying, selling and trading online multiplayer games in-game assets, there could be arguments towards those marketplaces being financial institutions and fall in the scope of national regulations that regulate financial transactions. In Estonia, there is a specific law, that regulates payment institutions and e-money institutions.[72]

Estonian Payment Institutions and E-money Institutions Act paragraph 6 and 7 regulate E-money and E-money institutions. By the definition, e-money has monetary value, is stored electronically, it expresses monetary claims against an issuer and it is issued at par value of the amount of the monetary payment received. Furthermore, it is used as a payment instrument to execute payment transactions and it is accepted as a payment instrument by at least one person who is not the issuer of the same e-money.[73] Marketplaces are venue for people, who believe that they are trading in monetary goods, because some or many in-game assets have value and therefore it could be considered to be an e-money and therefore marketplaces could fall in the scope of e-money institutions.

The author of this paper would not go as far as viewing these in-game assets as e-money. The main reason for this argument would be, the fact that in-game assets were not initially designed to have monetary value or have an impact of financial transactions. The main idea for in-game assets was more of a motivational and designer value and something to keep the players more interested and attracted to the game. In-game currencies had the same idea, as they were meant for interaction between the player and the merchant in the game itself.

Although many marketplaces deal with in-game currencies, exchanging them for flat currency, they would not fall in the scope of Estonian Payment Institutions and E-money Institutions Act paragraph 7, as it defines E-money institutions as public or private limited company whose core activity is the issuing of e-money in its name.[74] Under this definition, only game developers would fit within the scope of E-money institutions as described in the Estonian national law, as they are the only institutions, who can issue in-game currency.

[72] Makseasutuste ja e-raha asutuste seadus RT I 2010, 2, 3
[73] *Ibid.* § 6
[74] *Ibid.* § 7

There is another problem with the aspect of E-money institutions and their suitability with game developers. Mainly, game developers main goal is not to issue in-game currency as E-money on its name, rather than have players collect it from various quests and loot inside the game. The use of in-game gold was not meant as a trading item or valuable item and game developers would argue for it.

To conclude, it is rightful to say Estonia has national laws, that well regulate E-money and its institutions. Based on the argumentation written beforehand, it is clear that in-game assets nor game developers and marketplaces do not fit in the scope of Estonian Payment Institutions and E-money Institutions Act.

4.3. Example of money laundering

In the article "Money laundering and terrorism financing in virtual environments: a feasibility study" by Angela S.M. Irwin, Jill Stay, Kim-Kwang Raymond Choo and Lin Lui[75], the authors conducted a hypothetical money laundering scenario. They used over-the-counter prepaid Visa/MasterCard gift cards as tools to launder money.

The money launderer, hereinafter suspect, bought the gift cards with illegal money, then used the cards to purchase virtual credits from a Massively Multiplayer Online Game, hereinafter MMOG. When the credits were placed on multiple accounts, then the credits were sold back through an Online Financial Service Provider, hereinafter OFSP. OFSP are online websites, that facilitate buying and selling virtual items.

The OFSP transferred real world money to several PayPal accounts and through PayPal, money can be transferred to offshore bank accounts. They proved, that by purchasing prepaid gift cards, buying virtual currency and making the exchange back to real world money has a lot of anonymity because there are no banks involved, that could monitor their actions.

[75] Irwin, A. S. M., Slay, J., Choo, K.-K. R., Lui, L. (2014). Money laundering and terrorism financing in virtual environments: a feasibility study. – *Journal of Money Laundering Control*, Vol. 17, Issue 1, 50-75, p. 57-70.

They brought up a small setback with prepaid gift cards, to launder a substantial amount of money, they would need a lot of gift cards. This in mind they were still able to prove, that laundering money through the easy rout of buying gift cards, buying virtual currency with them and using an OFSP to turn it back into real world money would work, without anyone noticing their actions.

Of course, it should be mentioned that to launder more money and to lower losses, there should be a substantial amount of accounts involved in the transaction and many accounts should launder simultaneously, this helps lower the losses, when some of the accounts are found and frozen.

In their article, they analyzed how big the risk would be, if money laundering is done through their way. They stated, that when the OFSP has a weekly limit on deposits and there would be some anti-fraud software in place, the money transfers should not always be maximum. Therefore, the time it takes to launder resources would be longer. This can be bypassed, by using multiple third party virtual currency exchange sites.

When the virtual money is changed back to real world currency and transferred to a PayPal account, there come up other problems. As PayPal does not have limits on the amount of funds that can be transferred into them, there are limits on withdrawal of the accounts funds. There are two options, that the authors suggested how to get around that problem.

Firstly, they suggested on using multiple PayPal accounts and direct funds through them, this would minimize risks on account freezing and would mask the traffic of funds better, as the sums would not be exponentially large and therefore the likelihood of them being found by an anti-fraud software would be low.[76]

[76] *Supra nota,* p. 58-59.

The second suggestion would be to use a fall guy.[77] That is someone, who is in front of the operation and is the person, law enforcement aims. The person would not oversee the operations and would not understand anything that is going on, the person is there if anything goes wrong on the operation and law enforcement intervene. The people, who are actually behind the money laundering would not be caught and they can start it all over again.

The overall goal of money laundering schemes it to make it as difficult as possible for law enforcement to catch the criminals and to trace the original funds. Mitigating risk is achieved through multiple transfers. In the real world, the risk mitigation consists of using multiple banks, from one account to another and through multiple jurisdictions. But eventually the money travels to the suspects bank account and if it is red flagged, the law enforcement can piece the actions together. In the real world, the risk of getting caught, prosecuted and penalized is high.

In contrast, in the virtual world, using multiple accounts, micro-structuring, layering and placement techniques ensures, that even if the service provider becomes suspicious and freezes an account, the losses are minimal.

Furthermore, it would be difficult for service providers and law enforcement to find the connections between different accounts. Anonymous payment methods, using multiple service providers to layer the transactions and using multiple accounts mitigates the risk, that anyone can find the true origin of the funds.

In addition, virtual environment removes face-to-face contact between the account holder and service provider, therefore it is difficult to know, who is controlling the accounts, when there is no way to reliably identify the account holder. Even if an identification is needed to open up an account, the suspect can use fake or stolen information.

[77] *Supra nota,* p. 71.

At the end of the article hypothetical experiment, the authors did highlight, that for criminals to use this method of money laundering, they need to use precautions.[78] Use fictitious identity details, the use of a PayPal or similar merchant, software that conceals IP addresses of the account holder every time they log into their account or make a transaction, disable cookies as they can monitor the users' behavior and location. When making money transfers, the sum must wary and not be a substantial amount, use multiple service providers for money transfer and exchange. The methods described must be used every time, when the suspect makes a mistake and does not use those precautions, the risk is significantly higher of attracting attention from the service provider or law enforcement.

This scenario proved, how money laundering can be achieved through in-game assets, how criminals can take precautions and how to stay out of sight of the service provider and law enforcement. It must be mentioned, that the biggest drawback of this scenario was, the amount of money lost due to transaction fees. In their experiment, the authors found that money exchanges can eventually lead up to 18 percent loss of fund. Overall, this example is in the authors opinion one of the best to highlight the flaws in regulations and show the simplicity on how money laundering can be done with virtual assets.

United Nations Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies[79] reference a case study, where an international group of criminals transferred illegally-obtained money through a financial service provider to countries where they were habitant. There, the criminals withdrew the money and converted it into electronic currency through digital currency exchanger. The digital currency was then transferred to accounts held by the criminals by a financial service provider, who administered electronic currency in the countries involved. With the cooperation of a bank located in an offshore region, the financial service provider issued prepaid MasterCard's, which were attained anonymously and loaded with the electronic currency. These cards could be used worldwide in payment transactions and cash dispensers. Through this point by point action, the criminals had effectively concealed the flow of illegally obtained money and they

[78] *Supra nota*, p. 57-70.
[79] United Nations Manual. (2014). Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies. [Online:] https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf. Last accessed: 01.05.2018.

had access to the money directly and anonymously. Although this example uses cryptocurrencies, in the authors opinion, it is a good example on the efficiency and simplicity of online money laundering. Although this example uses cryptocurrencies, the same steps can be achieved with multiplayer games in-game assets, the steps would mostly be the same. As the criminals would convert the illegal money into in-game assets, trade those in a third party financial service provider to electronic or fiat money and then transfer said assets to an offshore bank account or through money mules to the criminal's own bank accounts. There are more complex patterns, that can emerge from this scenario, but the author believes that, when a simple scheme works, more complex strategy will work as well and may be more difficult for law enforcement to catch them.

4.4. How money laundering would work in online multiplayer games with in-game assets

Trading virtual assets for real world money is not only for the criminals, as mentioned before, honest users dive into the trading as well. Game developers would like to keep third parties out of the trading and therefore influence players on trading with the coded game merchant.

This method does not work, as honest players want to get a specific item, that the merchant may not sell. They turn to third party vendors, such as eBay, where a lot of in-game asset trading took place. Game developers did not look kindly upon this action and forced eBay to shut down the auctions on virtual in-game assets. This caused a counter action, as black markets emerged.

Black markets for virtual in-game assets, where there are no regulations and trading are done only through mutual trust.[80] Black markets work side by side and even compete with the game developers themselves, if the game developer has installed a trading market in the game. These markets compete with prices and different offers, as mentioned, they are poorly regulated and maintained.

[80] Kennedy, R. (2009). Law in Virtual Worlds. – *Journal of Internet Law,* Vol. 12, Issue 10, 3-10, p. 5.

Criminals, who own black markets can use them with ease, they can look at the developers' market value and offer cheaper prices, bringing more traffic and maintaining an anonymity of their own trades at the same time.[81] The trades can mask their intentions to launder money through buying and selling virtual items. Honest users would be the ones selling their items with a larger profit, the criminals gaining a virtual item and they can later sell onwards. They can use the developers own market to sell the item and therefore it would seem as they are honest users who just want to change their in-game assets.

Black markets are forbidden by the game rules and game developers work hard on catching players, who have acquired virtual in-game assets through a third party. Although it should be mentioned, that keeping an eye open for every unorthodox action would result the game going bankrupt, as it would require a lot of funds to have an overview on every transaction.

For example, Blizzard Entertainment, the company who owns *World of Warcraft* suspends temporarily or permanently accounts that have been suspected of third party trading.[82] On the other hand, Blizzard has said, that their game is played by millions of players. Therefore, the author is on the opinion, that Blizzard cannot have an overview of every suspicious transaction, because the traffic data would amount to huge numbers and as mentioned before, criminals can easily make a new account, if their old account is closed.

Legal actions were raised in the United States against gold farmers, where the main aspect of the dispute was virtual currency transformation to US dollars. The statement referred to companies, whose employees played *World of Warcraft* with the sole purpose of collecting in-game gold and selling it for real world currency. The argument persisted on the affect virtual gold selling has on the game and on the players. Unfortunately, the case was settled out of court and therefore there are no opinions from the court on that subject.[83]

[81] Xu, X., Yang, X., Lu, J., Lan, J., Wu, Y., Chen, W. (2017). Examining the effects of network externalities, density, and closure on in-game currency price in online games. – *Internet Research.* Vol. 27, Issue 4, 924-941, p. 930.
[82] Constantiou, I., Legarth, M. F., Olsen, K. B. (2011). What are users' intentions towards real money trading in massively multiplayer online games? – *Electron Markets*, Vol. 22, 105-115, p. 109.
[83] Kane, S. F. (2008). Virtually Lawless: Legal & Economic Issues in Virtual Worlds. – *The Computer & Internet Lawyer,* Vol. 25, No. 6, 13-24, p. 20.

This case still highlighted that selling virtual in-game assets becomes a problem when the currency is valued in the millions. This tactic could be achieved to launder illegal money, as criminals can higher gold farmers to harvest the in-game assets, sell the gold and transfer the money back to the criminals. The illegal money, that the criminals wanted to clean in the first place would be the payment for the gold farmers and in return, the criminals would get so-called clean money.

There was an incident in a game called *EVE Online*, where one player started an investment bank, offering a percentage of their investment back. This attracted huge attention in the game and many players put most of their fund in the bank. Some even traded real world money for the games virtual currency to invest in that bank. Eventually the bank creator vanished with the other players investments. The pressure that was put due to the theft to the developers was immense, but they could not delete the players account or return the investments to the rightful owners.[84]

Money launderers can open their own banks in games, of course if the game has that ability, and hide their assets there. When they wish to exchange the virtual currency to real world money, they can sell the virtual currency or start buying in-game assets, for instance buy helmets and swords and later use third party marketplaces to sell those items for real world money.

Some multiplayer games have anti-fraud systems in place, that look at players overall traffic, which may contain their movement, transactions and conversations. When money laundering is done in that game and the criminal uses accounts just to trade gold and in-game assets, the anti-fraud software will mark it as suspicious. This will bring on an investigation by the game developer and there is a high chance that the account will be closed.

To avoid having accounts closed frequently, there are other solutions that can mask the criminals' actions. These are called game bots, which are automated programs, that play the

[84] Adriana, A. (2010). Beyond griefing: Virtual crime. – *Computer law & Security review*, Vol. 26, 640-648, p. 646.

game on behalf of the human player.[85] Bots can mask the actions of money launderers and trick the anti-fraud system by acting as a player.

Bots can have other benefits for the criminals, as they can accumulate more in-game resources than human users, because they do not require breaks. This has the upside for the criminals, as it masks their true intentions and, in the meantime, generates more virtual income. Bots are usually bought or rented, which means that some investments by the money launderers is needed.

There are some drawbacks on bots, as they have few features, that newer anti-fraud software would eventually discover them. Namely they do not communicate with other players and many of them have repetitive movements, which can seem strange and something a human player would not do.[86]

In the author's opinion, these problems could be solved. The code that gives the bots commands, can be written in a way to have a few random movements from time to time and have specific written interactions that they say to other players. These simple changes would make detection much harder for the anti-fraud software and therefore keep the account in the game longer, giving criminals more time to use the account for illegal activities.

A well established and well-funded criminal organization can create a multiplayer game for masking their criminal activities and further help them launder money. Making a game requires large investments but owning a game and laundering money through that may make investigations and enforcement of the various current laws very difficult or even impossible.

The only way how to catch game developers themselves from money laundering is to use extremely thorough monitoring and reporting requirements. Thus, there needs to be a long and

[85] Kang, A. R., Woo, J., Park, J., Kim, H. K. (2013). Online game bot detection based on party-play log analysis. – *Computers and Mathematics with Applications,* Vol. 65, 1384-1395, p. 1384.
[86] Kang, A. R., Jeong, S. H., Mohaisen, A., Kim, H. K. (2016). Multimodal game bot detection using user behavioral characteristics. – *SpringerPlus*, Vol. 5:523, 1-19, p. 3.

devious investigation by the law enforcement to catch money laundering from the developers' side.[87]

In the authors opinion, a well-funded criminal organization would have little problem of making a multiplayer game, that would attract a lot of attention from the gaming community and by generating user traffic and popularity, the criminal organization can use the game platform to launder huge sums on money, without being noticed. Even if they attract attention from law enforcement, their servers can be located in countries, that do not fall in the law enforcements jurisdiction.

One subject, that will become an issue for law enforcement is accessing the files of a captured money launderer. Namely, to use the information provided in the criminal's possession against him/her in the court of law. There are multiple factors and programs that can hide or encrypt files in the criminal's computer or database. For this purpose, the author found that it would be necessary to show one example, how criminals can hide the data and money laundering traffic from law enforcement or make it extremely difficult for them to gain access to said information. Criminals can use virtual machines, which is a software that allows user to control an operating system as an application on their computer. This means that the software acts as an operating system inside the operating system. The catch is that the software's programs and data are not shown in the real operating system, while the user can see that the hard drive contains data, they do not have access to said data, without using the virtual machine software. Usually the virtual machine lets users encrypt the data used in the program. Therefore, it is possible to use an encrypted virtual machine for all money laundering activities and there would be no evidence of the use of such actions in the computers operating system.

All in all, the author believes that money laundering through virtual worlds and through the use of in-game assets has not been investigated thoroughly. As shown above, money laundering in virtual worlds requires criminals to use certain security aspects, for example IP

[87] Kane, S. F. (2008). Virtually Lawless: Legal & Economic Issues in Virtual Worlds. – *The Computer & Internet Lawyer*, Vol. 25, No. 6, 13-24, p. 19.

hider and fake identification documents. When they are used, catching a criminal in an online world will prove difficult, if not impossible.

This papers research task was to analyze, how money laundering is done with in-game assets This analysis should give the firm answer on how in-game assets are used today, to launder illegal funds all around the world. Given the example of money laundering with in-game assets and the step-by-step explanation in this paper sub-chapter 4.3. money laundering with in-game assets are extremely simple. Although it does have small setbacks, in the given example, the amount of money they lost due to transaction fees and the amount of money they could exchange was limited. But the author is on the opinion, that when a simple example, which was analyzed in the paper, works then a much more thought through plan would be more beneficial. Although the money laundering methods are described, there are insufficient methods provided for law enforcement agencies on combating this phenomenon. This is because the nature of territoriality and different definitions on money laundering and online multiplayer games in-game assets prevent unified legislation and legislations applicability.

The research question in this paper is what legal gaps prevent prosecution of money laundering using online multiplayer in-game assets. The upcoming chapter will include legal analysis from Estonian and European legislation. Given the explanations on how to launder money and what are the different scenarios criminals can use to hide their assets and launder them anonymously, the author is on the opinion that prosecution of money laundering in online multiplayer games is almost impossible if there is no unified definition of in-game assets in place. The reason is, that Internet has no limits, but countries have different legal systems and even similar legal systems may have laws that conflict with one another. Some countries do not have any regulations set in place when it comes to virtual money trading or virtual assets.

This combination of law and lawlessness has the effect of not regulating the overall virtual world systems and most of the obligations fall to the game developers, who may not have the right aim. By that, the author means game developers firstly want to defend themselves from

litigations and make a profit from the game, therefore most of their funds and energy would go into other aspects and criminals can exploit the gap.

Black markets, that trade in-game assets are not usually maintained by the game developers but individuals. They can use the online world as a mixture of different laws, different countries with diverse attitudes for virtual worlds.[88] Those individuals could use servers in countries that lack regulations or use multiple servers through multiple continents, hiding their true identity and masking their actions.

While the author is on the opinion that internet has no borders and due to that, limiting money laundering would be extremely difficult, there are some steps countries and game developers can take, to limit the actions of criminals. As stated before, catching a criminal in the virtual world is near impossible and their criminal activity location would not reflect their actual presence in that country, for that reason, the authors suggestions are preventive acts.[89]

Firstly, there should be more collaboration between game developers and online financial service providers. Information exchange between them would show which accounts act suspiciously, for instance some accounts rarely play the game but transfer huge amounts of in game currency or one account sells a lot of in-game currency to multiple online financial service providers.[90] Suspicious acts can be reported, and those accounts can be frozen by the game developers and the information sent to law enforcement for investigation.

Secondly, countries can start regulating and monitoring the sales of virtual items and the exchanges of in-game currency to real world money.[91] These regulations would need to be monitored sufficiently. This idea is still not bulletproof, as game developers and website

[88] MacInnes, I. (2006). Property rights, legal issues, and business models in virtual world communities. – *Electronic Commerce Research,* Vol. 6, 39-56, p. 47.
[89] Hiller, J. S., Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. – *Computer Law & Security Review,* Vol. 29, 236-245, p. 237.
[90] Emerald Group Publishing Limited. (2014). Criminals move with the times: Money launderers and terrorism financers go online. – *Strategic Direction,* Vol. 30, Issue 6, 8-10, p. 10.
[91] Kshetri, N. (2009). The evolution of the Chinese online gaming industry. – *Journal of Technology Management in China,* Vol. 4, No. 2, 158-179, p. 171.

owners can move their business elsewhere and this regulation should be a world-wide effort on containing and regulating money transfers in virtual worlds.

Thirdly, there should be an awareness programs set in place, to spread the information of the potential of money laundering through online games with in-game assets. These programs should be aimed to policy makers, showing the potential harm on such an unregulated field in the virtual world.[92] These awareness programs should cover every country in the world, to have an efficient outcome.

Further, while some game developers have already put in place, others lack certain indicators, that may help game developers to seize suspicious activities. For instance, when large sums on virtual currency is deposited in an account, but there is little, or no game play activity done in that account. Large amounts of currency is deposited regularly and then transferred out again or the account holder makes multiple accounts in one or more names and then deposits large sums in those accounts.[93] These actions should indicate to the game developer, that this account is used for illicit activities and therefore should be monitored closely.

Although these measures may indicate suspicious activities to the game developers, as written before in this thesis, criminals can use game bots, to show activity in the account and generate traffic, so that the developers' software would not flag it as suspicious activity, rather than normal game play.

[92] Donner, C. M. (2016). The Gender Gap and Cybercrime: An Examination of College Students' Online Offending. – *An International Journal of Evidence-based Research, Policy, and Practice,* Vol. 11:4, 556-577, p. 572.
[93] Irwin, A. S. M., Slay, J., Choo, K.-K. R., Lui, L. (2014). Money laundering and terrorism financing in virtual environments: a feasibility study. – *Journal of Money Laundering Control,* Vol. 17, Issue 1, 50-75, p. 71.

5. ESTONIAN AND EUROPEAN UNION LEGISLATION ANALYSIS ON MONEY LAUNDERING

5.1. Estonian Money Laundering and Terrorist Financing Prevention Act

As the author has argued, that internet has no borders, making prosecution difficult. There is still a need to analyze the Estonian and European legislation on tackling this unique problem.

The Estonian Money Laundering and Terrorist Financing Prevention Act paragraph 1 section 2 point 1[94] regulates the principles of assessment, management and mitigation of risks related to money laundering. The aim is to counter all money laundering types, including ones that are happening in the virtual world.

Paragraph 2 of the same Act[95] has a list of economic and professional activities, that must follow The Money Laundering Act. Point 10 of said paragraph, states that providers, who exchange virtual currency against a flat currency must follow the rules and regulations of this Act. The definition is suitable for this paper, as most game developers and black markets function as exchange services, where one aspect is exchange from virtual currency to flat currency. This paper focuses on the aspect of multiplayer game in-game asset money laundering, that will eventually lead to flat currency for criminals to use.

There is little analysis on the exchange between virtual currencies and this part will need to have further analysis. The author is on the opinion, that this Act does not regulate exchanges between virtual currencies and it will leave a major gap in the Estonian legal system when it is not regulated. There is a need to specify this Acts definition, to include service providers, who exchange virtual currency against virtual currency.

[94] Rahapesu ja terrorismi rahastamise tõkestamise seadus RT I, 17.11.2017, 2. § 1, section 2, point 1
[95] *Ibid.* § 2.

Paragraph 3 of The Estonian Money Laundering and Terrorist Financing Prevention Act point 9[96] defines virtual currency as means of value represented in the digital form, which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds. This definition may cause problems, when the issue of in-game assets rises. Namely the acceptance as payment instrument may cause issues revolving what can and cannot be subjected as payment instrument. Some online multiplayer games will give their players the opportunity to pay their subscription fees with the in-game currency, admitting that this in-game currency has monetary value, the same as flat currencies have. On the other hand, in-game assets include cosmetic designs and game elements, that are usable only in that game. For example, different types of armor, weapons and potions. These in-game assets should not be acceptable payment instruments, as their purpose is not to be payed with, but to be used in the game itself.

The author is on the opinion, that the definition is meant for cryptocurrencies and tokens, that are only in virtual form and designed as payment instruments. The issue with in-game assets, is that most of them are not developed for the purpose as a payment instrument, rather an asset to be used inside the game. As mentioned earlier, some online multiplayer games let their players pay their subscription fees in the games own currency rather than flat currency, for this reason, the author sees this game own currency as payment instrument that is acceptable in the sense of Estonian law. Making the line to understand what should fall in the scope of virtual currency by the Estonian law and what not, more of a gray area. Overall multiplayer games in-game assets should not fall in the scope of The Estonian Money Laundering and Terrorist Financing Prevention Act paragraph 3 point 9, because most in-game assets are not designed as payment instruments and the exceptions that fall in this scope do not outweigh all in-game asset meaning.

As analyzed before in this paper, most in-game assets have monetary value and players have the opportunity to sell and buy these assets for flat money. The fact that in-game assets have monetary value does not mean that they would fall in the scope of acceptable payment instrument. An analogy can be brought up, as someone who has bought a mobile phone can

[96] *Ibid.* § 3, point 9.

sell it to someone else, return in to the shop or pawn it in a pawnshop, but this does not mean that it would be an acceptable payment instrument, to go to a clothing store and pay with the mobile device.

Taking the definition from The Estonian Money Laundering and Terrorist Financing Prevention Act and the analysis beforehand, the author is on the opinion that online multiplayer in-game assets should not fall in this definition. Selling, buying and trading in-game assets should fall in the scope of Estonian Law of Obligations Act[97], more precisely to Chapter 11 Contract Of Sales and Chapter 12 Barter Agreement. As in-game asset trading in marketplaces and in the game should fall within the scope of the given law. As transactions done with in-game assets are no different than any other transaction with other goods, there is no need to analyze these transactions.

Estonian Money Laundering and Terrorist Financing Prevention Act Paragraph 9 section 1[98] defines the beneficial owner as a natural person, who makes a transaction, act, action, operation or step or otherwise exercises control over a transaction, act, action, operation or step or over another person and in whose interests or favor or on whose account a transaction or act, action, operation or step is made. Therefore, the money launderer, whose intent is to clean the illicit money would be the beneficial owner. The difficult part for law enforcement is to show, who is the rightful beneficial owner. Difficulty determining the beneficial owner comes from multiple angles, as money laundering with in-game assets do not have to reside in one jurisdiction or even in one continent. Masking the transactions, using multiple accounts and directing the flow on illicit money around the world would make pinpointing the original criminal extremely difficult.

As analyzed before, law enforcement would have difficulties gathering information and cooperation with other countries jurisdictions, therefore tracing the illicit goods will prove to be difficult. Moreover, criminals can mask their identities by using stolen identities, using technological advantages that mask their true place of origin and using money mules and front runners, who would not be the true beneficial owners.

[97] Võlaõigusseadus RT I 2001, 81, 487 Chapters 11 - 12.
[98] Rahapesu ja terrorismi rahastamise tõkestamise seadus RT I, 17.11.2017, 2. § 9, section 1.

This paper's author sees the definition being correct in money laundering situations, where online multiplayer in-game assets are involved.

Gathering information about beneficial owners in the concept of money laundering with in-game assets has another downfall for law enforcement. As multiplayer games popularity rises, so does the transaction traffic. As this paper has previously analyzed, security aspects and illicit action monitoring in marketplaces and financial service providers, who focus on trading with in-game assets is inadequate. When the lack of monitoring and fraud prevalence is missing, law enforcement would have difficulties determining which actions can be categorized as illegal activity and which are not. When transactions of both nature collide, to prove with certainty which actions are illegal, and which are the natural course of players exchange will get blurry. For example, when law enforcement agency is looking into a black-market site, that is focused on the trading of online multiplayer in-game assets and there are no red flag indicators or security standards set in the site that monitors and lets the owner know, which actions are done with illegal money or goods and which actions are done by honest users. The time and effort that the law enforcement would need to put in, to get an overview of the site would prove too difficult. As then, the only logical part is to force the marketplace owner to rise their security standards or take the site down. Both would bring little inconveniences to the money launderer, who uses this site, as they can turn to another site to continue their activity. Moreover, when a site does not have any user identification requirements, or those requirements are low, identifying the criminal by law enforcement would be difficult. This paper has analyzed, how criminals can mask their identities and stay anonymous online, therefore tracing their true identity will be time consuming and it has a chance of not revealing the true identity of the criminal.

Estonian Penal Code paragraph 394[99] has laid down punishments for money laundering. The law states that convicted to money laundering, an individual can be punished by a pecuniary punishment or up to five years imprisonment. When the same act has been done by a legal person, the punishment would be a pecuniary punishment. This paper is aimed on understanding and highlighting the new concept of money laundering done through and by online multiplayer games in-game assets. In the authors opinion, the Estonian Penal Codes

[99] Karistusseadustik RT I 2001, 61, 364 § 394

punishments are adequate, given that money laundering usually involves only financial illegal activities and do not comprise threats to human life.

One of the main issues with criminal law, is the principle of territoriality.[100] Money laundering through in-game assets differ from so-called traditional money laundering by the availability to act in any country in the world. The author has expressed his opinion, that Internet has no borders and money laundering with in-game assets takes place online, there is little to do to battle against it.

The question of territoriality can be divided by two separate scenarios. One is that the country, where the money laundering act is taking place has power to proceed criminal charges against the criminal. The second part would be that the country, where the criminal resides has the power to judge the criminal. In both situations, there are multiple outcomes, that can overrule the countries power. In the first scenario, when a criminal uses 3 different servers, located in different countries, the question rises on who has the power to claim that their jurisdiction has the power to judge the criminal.

Anonymity and technical means available for criminals to use, means that they can easily hide their true origin online. Using technical means to cover their IP address, use stolen identities and even travel the world by themselves, to not get caught by law enforcement. As mentioned, the second scenario would be difficult, as proving the criminal's residence can have drawbacks. For example, if the criminal lives in country A, where there are strict rules for money laundering and that country monitors activities with extreme precision. To avoid prosecution in country A, the criminal uses technical equipment to show everyone that he is laundering money in country B. In that country, online money laundering is not regulated and therefore the criminal's actions would not go against the law in country B. If country A finds out about the criminal, they have no jurisdiction to prosecute the criminal against actions done in country B. These overall jurisdictional questions need further analysis and an international agreement, where it is clearly stated, that online crimes committed in multiple jurisdiction

[100] Strikwerda, L. (2014). Should virtual cybercrime be regulated by means of criminal law? A philosophical, legal-economic, pragmatic and constitutional dimension. – *Information & Communications Technology Law*, Vol. 23, Issue 1, 31-60, p 54.

should be prosecuted in an international court, rather than a national court. Through this, all countries, who have evidence against the criminal, can step forward, present the evidence and the court would determine the punishment. The laws should be negotiated by every nation and therefore should have international applicability and be applied to every jurisdiction equally.

This international law would be a major step towards fighting against international money launderers, who use multiplayer online games and in-game assets as means to act out their crimes. This international agreement would require many countries to come together and work towards and harmonize their jurisdictions to achieve this one goal.

Even if money launderers are caught by law enforcement and the prosecution has given their indictment, the courts still need to bypass the magic circle[101]. As the author has previously analyzed the concept of magic circle and the meaning behind it, as game developers would create EULA's to combat the benefits of this circle and regulate in-game assets through that. Author has argued against the EULA, stating that they are too one sided and give no rights to the players of the game. Arguing against something does not automatically mean it is not used anymore and there is the possibility, that the courts would go against the prosecutors and decide that the magic circle is not broken and the EULA stands, bringing attention to the game developer and their right to demand compensation from the criminal on infringement of the EULA.

Fortunately, the European Union legislators have also worked towards unified approach to combat money laundering. In the next sub-chapter, the reader shall be introduced to the European Union wide directive which encounters and tries to tackle money laundering within the European Union Member States.

[101] *Supra nota,* p 38.

5.2. European Union Directive 2015/849

European Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (hereinafter AML) Article 3 point 3 has defined property as assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets[102]. Given the research and analysis in this paper, it is safe to assume, that online multiplayer game in-game assets fall in the scope of the given definition. As in-game assets are all in electronic form and they are easily transferrable over the Internet.

Article 13 of the Directive[103] sets out due diligence obligations for, in this paper, marketplaces and game developers, whose business model is trading with in-game assets. Due diligence measures shall include the following:

i. Identifying the customer through documents, data or information gathered from reliable sources.
ii. Identifying the beneficial owner with reasonable efforts with which every institution would have certainty that this is the true identity of the beneficiary owner.
iii. Gathering information about the nature and intent of the business relationship.
iv. Additionally, entities should have ongoing evaluation system, which allows to monitor the business relationship. This would also include dissecting transactions made between businesses.

Moreover, if a third party is entitled to act on the behalf of one business, within these transactions, obliged party should confirm that this third party indeed is the rightful person to make transactions within this relationship.

[102] THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (EU) No 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.
[103] *Ibid.* Article 13.

Due diligence is built up upon the idea of periodic, or even constant, check-ups which would allow to discover money laundering or terrorist financing at the moment of its inception, rather than letting it develop into large-scale financing.

In accordance with AML, each European Union Member State is required to ensure that all obliged subjects apply due diligence in accordance with applicable laws. While each nation is left to apply their own measures for such check-ups, each entity is left on their own to figure out to what extent they need to carry out the due diligence.

If marketplaces are considered to be obliged entities to carry out due diligence of their clients, they would have freedom to choose how deep into transactions nature they will go. The author of this paper argues that marketplaces would need more in-depth guidelines to carry out these assessments and help them to understand what risks inefficient due diligence might cause. Even if this obligation is put on marketplaces, only European Union entities would need to ensure adequate implementation of such measures.

Each European Member State should consider having its financial inspection agencies to draw up at least nation-wide guidelines. It is without a doubt that European Union wide instructions would be much more efficient to tackle money laundering crimes within the Union. However, it is clear that all nations across the world should work together to have these guidelines developed for the best result world-wide. As the author has previously stated, Internet has no borders therefor best results are achieved with strong and reliable collaboration between all countries and its governments.

Even though the European Union legislators have put together a great directive for classical businesses and money laundering scenarios, it failed to recognize the danger that is posed by Internet area. There are no specific clauses to help online marketplaces in tackling money laundering. It is clear that new Internet area would severely need more in-depth guidelines.

6. Conclusion

Online multiplayer games grow in popularity with each year, attracting attention from all around the world. Given the speed on technological improvements, there are few places in the world where Internet connection is limited. While the popularity is beneficial for game developers, it is a new way for criminals to act, without notice.

This papers analysis is divided into three parts. The first part analyzed the end users license agreement which sets out the relationship between the game developer and players, as the analysis was necessary to determine money laundering aspects with the use of in-game assets. Furthermore, it was concluded that EULA-s are too one sided and detrimental to the players, taking away their basic human rights.

The second part of the thesis analyzed how in-game asset trading became so popular and how some players started to make a living out of the market by monetizing the demand for the in-game assets. Through the rise of trading in-game assets and new marketplaces, the analysis of possible scenarios how money laundering can be done is described and evaluated.

With different legal and jurisdictional loopholes which can hinder investigations from law enforcement, including the lack of security measures set by the marketplace owners, has made the investigation of money laundering with in-game assets difficult.

The research task for this paper is to show how money laundering is done with in-game asset. The paper consists of an analysis of a previous research, in which researchers conducted one money laundering scenario, showing how simple and anonymous money laundering looks when conducted through in-game assets. The result of said research was to highlight the problems that law enforcement would face in this situation. Some of the methods, criminals can use are fictitious identity details, the use of a PayPal or similar merchant, software that conceals IP addresses of the account holder, disable cookies as they can monitor the users' behavior and location. Use multiple service providers for money transfer and exchange. The

author of the thesis came to the same conclusions, when analyzing money laundering regulations of Estonian and European legislation.

The research question of this paper was to analyze which legal gaps prevent prosecution of money laundering that is done with online multiplayer in-game assets. While the analysis conducted includes legal definitions and obligations from Estonian and European Union legislations, the author has concluded, that because Internet has no borders, there is a need for an international agreement to combat money laundering.

The necessity for supranational legislation concerning anti-money laundering is especially amplified due to the fact that the person conducting their business activities does not need to be in the same country or even in the same continent, because the Internet provides them with freedom and anonymity and the person can use specific programs to mask their actions. Therefore, identifying them by law enforcement would prove extremely difficult.

As international laws need to be set to regulate online money laundering, so does cooperation's between national law enforcements and marketplaces that trade in-game assets. Through cooperation and exchange of information, there is a chance to have sufficient investigations against criminals who use in-game assets for illicit purposes.

7. List of used sources

7.1. Articles

1. Adrian, A. (2010). Beyond griefing: Virtual crime. - *Computer Law & Security Review,* Vol. 26, Issue 6, 640 – 648. Elsevier Ltd.

2. Blackburn, J., Kourtellis, N., Skvoretz, J., Ripeanu, M., Iamnitchi, A. (2014). Cheating in Online Games: A Social Network Perspective. - *ACM Transactions on Internet Technology*, Vol. 13, Issue 3, Article 9, 9 – 15. Ed. Zimmermann, H.-D. ACM Inc.

3. Chen, Y.-C., Chen, P. S., Hwang, J.-J., Korba, L., Song, R., Yee, G. (2005). An analysis of online gaming crime characteristics. - *Internet Research*, Vol. 15 Issue: 3, 246 – 261. Emerald Group Publishing Limited.

4. Constantiou, I., Legarth, M. F., Olsen, K. B. (2012). What are users' intentions towards real money trading in massively multiplayer online games? - *Electronic Markets*, Vol. 22, 105 - 115. Springer-Verlag.

5. Criminals move with the times: Money launderers and terrorism financiers go online. (2014). *Strategic Direction,* Vol. 30 Issue: 6, 8 – 10. Emerald Group Publishing Limited.

6. Donner, C. M. (2016). The Gender Gap and Cybercrime: An Examination of College Students' Online Offending. - Victims & Offenders: *An International Journal of Evidence-based Research, Policy, and Practice*, Vol. 11:4, 556 – 577. Taylor & Francis Group, LLC.

7. Figueroa, N., L'Huillier, G., Weber, R. (2017). Adversarial classification using signaling games with an application to phishing detection. - *Data Min Knowledge Discovery*, Vol. 31, Issue 1, 93 – 133. Springer US.

8. Grimes, S. M. (2006). Online multiplayer games: a virtual space for intellectual property debates? - *New Media & Society,* Vol. 8 Issue: 6, 969 – 990. SAGE Publications.

9. Harviainen, J. T., Hamari, J. (2015). Seek, share, or withhold: information trading in MMORPGs. - *Journal of Documentation*, Vol. 71 Issue: 6, 1119 – 1134. Emerald Group Publishing Limited.

10. Hiller, J. S., Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. – *Computer Law & Security Review,* Vol. 29, 236-245. Elsevier Ltd.

11. Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. - *International Journal of Law, Crime and Justice*, Vol. 47, 44 – 57. Elsevier Ltd.

12. Irwin, A. S. M., Slay, J., Choo, K.-K. R., Lui, L. (2014). Money laundering and terrorism financing in virtual environments: a feasibility study. - *Journal of Money Laundering Control,* Vol. 17, Issue: 1, 50 – 75. Emerald Group Publishing Limited.

13. Kane, S. F. (2008). Virtually Lawless: Legal & Economic Issues in Virtual Worlds. - *Computer & Internet Lawyer*, Vol. 25 Issue 6, 13 – 24. Practising Law Institute.

14. Kang, A. R., Jeong, S. H., Mohaisen, A., Kim, H. K. (2016). Multimodal game bot detection using user behavioral characteristics. - *Kang et al. SpringerPlus(2016)*, Vol. 5:523, 1 – 19. SpringerPlus.

15. Kang, A. R., Woo, J., Park, J., Kim, H. K. (2013). Online game bot detection based on party-play log analysis. - *Computers & Mathematics with Applications*, Vol. 65, Issue 9, 1384 – 1395. Elsevier Ltd.

16. Kennedy, R. (2009). Law in Virtual Worlds. - *Journal of Internet Law*. Apr2009, Vol. 12 Issue 10, 3 – 10. Elsevier.

17. Kennedy, R. (2008). Virtual rights? Property in online game objects and characters. - *Information & Communications Technology Law*, Vol. 17, Issue 2, 95 – 106. Taylor & Francis Group.

18. Kshetri, N. (2009). The evolution of the Chinese online gaming industry. - *Journal of Technology Management in China*, Vol. 4 Issue: 2, 158 – 179. Emerald Group Publishing Limited.

19. Luppicini, R. (2014). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. - *Global Media Journal* -- Canadian Edition, Volume 7, Issue 1, 35 – 49. SAGE Publications.

20. MacInnes, I. (2006). Property rights, legal issues, and business models in virtual world communities. – Electronic Commerce Research, Vol. 6, Issue 1, 39 – 56. Springer Science + Business Media, LLC.

21. Manninen, T. Kujanpää, T. (2007). The Value of Virtual Assets – The Role of Game Characters in MMOGs. - *International Journal of Business Science and Applied Management*, Volume 2, Issue 1, 22 – 33. Directory of Open Access Journals.

22. Pyrooz, D. C., Decker, S. H., Moule Jr, R. K. (2015). Criminal and Routine Activities in Online Settings: Gangs, Offenders, and the Internet. - *Justice Quarterly*, Vol. 32:3, 471 – 499. Taylor & Francis Group.

23. Rughinis, C., Rughinis, R. (2014). Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union. - *Computers & Security*, Vol. 43, 111 – 125. Elsevier Ltd.

24. Strikwerda, L. (2012). Theft of virtual items in online multiplayer computer games: an ontological and moral analysis. - *Ethics and Information Technology*, Vol. 14, Issue 2, 89 – 97. Springer Netherlands.

25. Strikwerda, L. (2014). Should virtual cybercrime be regulated by means of criminal law? A philosophical, legal-economic, pragmatic and constitutional dimension. - *Information & Communications Technology Law*, Vol. 23:1, 31 – 60. Taylor & Francis Group.

26. Uysal, A. (2016). Commitment to multiplayer online games: An investment model approach. - *Computers in Human Behavior*, Vol. 61, 357 – 363. Elsevier Ltd.

27. Wang, Q. – H., Mayer – Schönberger, V., Yang, X. (2013). The determinants of monetary value of virtual goods: An empirical study for a cross-section of MMORPGs. - *Information Systems Frontiers*, Vol. 15, Issue 3, 481 – 495. Springer LLC.

28. Webber, N. (2014). Law, culture and massively multiplayer online games. - *International Review of Law, Computers & Technology*, Vol. 28:1, 45 – 59. Taylor & Francis.

29. Wu, Y., Chen, V. H. H. (2013). A social-cognitive approach to online game cheating. - *Computers in Human Behavior*, Vol. 29, Issue 6, 2557 – 2567. Elsevier Ltd.

30. Xu, X., Yang, X., Lu, J., Lan, J., Peng, T.-Q., Wu, Y., Chen, W. (2017). Examining the effects of network externalities, density, and closure on in-game currency price in online games. - *Internet Research*, Vol. 27 Issue: 4, 924 – 941. Emerald Publishing Limited.

31. Yan, J. J., Choi, H.-J. (2002). Security issues in online games. - *The Electronic Library*, Vol. 20 Issue: 2, 125 – 133. Emerald insight.

7.2. Estonian legislation

32. Rahapesu ja terrorismi rahastamise tõkestamise seadus. RT I, 17.11.2017, 38

33. Karistusseadustik, RT I 2001, 61

34. Võlaõigusseadus, RT I 2001, 81, 487

7.3. European legislation

35. The European Parliament and the Council of the European Union (EU) No 2015/849 of 5 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ L 141/73 20.05.2015.

36. The European Parliament and the Council of the European Union (EU) No 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119/1, 04.04.2016.

7.4. Other sources

37. BLIZZARD END USER LICENSE AGREEMENT. Available at: http://us.blizzard.com/en-us/company/legal/eula Last accessed: 14.03.2018.

38. Gamepal. Available at: http://www.gamepal.com/content.php Last accessed: 11.03.2018.

39. Patterson, N.C., Hobbs, M. (2010) A Multidiscipline Approach to Governing Virtual Property Theft in Virtual Worlds. – *What Kind of Information Society? Governance, Vitality, Surveillance, Sustainability, Resilience,* Vol. 328., 161-171. IFIP Advances in Information and Communication Technology, Springer.

40.Yan, J., Randell, B. (2005). A systematic classification of cheating in online games. - *NetGames'05*, 1 – 9. Hawthorne. ACM.

41. Woo, K., Kwon, H., Kim, H.- C., Kim, C.- K., Kim, H. K. (2011). What Can Free Money Tell Us on the Virtual Black Market? - *ACM SIGCOMM Computer Communication Review,* Vol. 41 Issue 4. 392 – 393. Association for Computing Machinery.

42. Taylor. T. L. (2002). „Whose Game Is This Anyway?": Negotiating Corporate Ownership in a Virtual World. – *Proceedings of Computer Games and Digital Cultures Conference.* 227 – 242. Ed. Frans Mäyrä. Tampere University Press.

43.United Nations Manual. (2014). Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies. [Online:] https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf. Last accessed: 01.05.2018.