DOI: https://doi.org/10.17816/RJLS641997

Revisiting the use of game assets in criminal activity

A.A. Dyachenko, S.V. Plokhov

The Prosecutor General's Office of the Russian Federation, Moscow, Russia

ABSTRACT

The article discusses the problem of using game assets in criminal activity. The study presents the main types of these assets, provides the procedure for determining their value, and also examines existing examples and possible risks of using game assets and in-game trading for criminal purposes.

The work contains a detailed analysis of the legislation of the Russian Federation and foreign states in the designated field. Particular emphasis is placed on the study of various legal approaches to loot boxes, including in terms of their regulation for the purposes of gambling legislation.

The study examines a number of examples from Russian and international judicial practice in civil and criminal cases in this field.

Based on the study conducted, the author's approach to solving problems arising in connection with the use of game assets has been developed, including specific proposals for amending Russian legislation in order to protect the rights of citizens and minimize the risks of criminal use of computer games.

Keywords: virtual assets; game assets; computer games; in-game trading; loot boxes; money laundering; cybercrime.

To cite this article

Dyachenko AA., Plokhov SV. Revisiting the use of game assets in criminal activity. *Russian journal of legal studies*. 2024;11(4):121–131. DOI: https://doi.org/10.17816/RJLS641997

Received: 18.10.2024 **Accepted:** 18.11.2024 **Published online:** 28.12.2024

УДК 343

DOI: https://doi.org/10.17816/RJLS641997

К вопросу об использовании игровых активов в преступной деятельности

А.А. Дьяченко, С.В. Плохов

Генеральная прокуратура Российской Федерации, Москва, Россия

АННОТАЦИЯ

В статье рассматривается проблематика использования игровых активов в преступной деятельности. В исследовании представлены основные виды названных активов, приведен порядок определения их стоимости, а также рассмотрены имеющиеся примеры и возможные риски использования игровых активов и внутриигровой торговли в преступных целях. Работа содержит детальный анализ законодательства Российской Федерации и иностранных государств в обозначенной сфере. Отдельный акцент сделан на изучении различных правовых подходов к лут-боксам, в том числе в части их регулирования в целях законодательства об азартных играх.

В исследовании рассмотрен ряд примеров из российской и зарубежной судебной практики по гражданским и уголовным делам в данной области.

На основании проведенного изучения выработан авторский подход к решению проблем, возникающих в связи с использованием игровых активов, в том числе конкретные предложения по внесению изменений в российское законодательство в целях защиты прав граждан и минимизации рисков криминального использования компьютерных игр.

Ключевые слова: виртуальные активы; игровые активы; компьютерные игры; внутриигровая торговля; лут-боксы; отмывание денег; киберпреступность.

Как цитировать

Дьяченко А.А., Плохов С.В. К вопросу об использовании игровых активов в преступной деятельности // Российский журнал правовых исследований. 2024. Т. 11. № 4. С. 121–131. DOI: https://doi.org/10.17816/RJLS641997

Рукопись получена: 18.10.2024 **Рукопись одобрена:** 18.11.2024 **Опубликована online:** 28.12.2024

Revisiting the use of game assets in criminal activity

Over the past few years, one of the main global trends has been the growing interest in virtual asset turnover. Open sources report that at least 560 million people worldwide will own cryptocurrency in 2024.[1] in July 2024, cryptocurrency market capitalization was more than $2.4 trillion.[2]

However, rapid technology development creates new opportunities for the use of virtual currencies to commit global crimes, primarily related to money laundering, terrorist financing, corruption, and drug trafficking.

Some expert studies stated that the amount of illegal cryptocurrency transactions would exceed $24 billion in 2023.[3]

Increased criminal use of virtual assets is also observed in the Russian Federation. In particular, in late 2023, Yuriy A. Chikhanchin, Director of the Federal Service for Financial Monitoring (Rosfinmonitoring), stated that the number of illegal cryptocurrency transactions had doubled in Russia.[4]

Despite the fact that legal regulation of virtual assets is on the national agenda in all countries, it is now too early to suggest that this sector is effectively regulated. This is also evidenced by the difficulties faced by many national law enforcement agencies in investigating crimes committed using information technologies.[5]

It should be noted, however, that, when studying legal regulation issues related to virtual assets, most researchers and practitioners only focus on cryptocurrencies and digital currencies (i.e. a digital alternative to national fiat currencies), whereas the relations developing in the gaming industry around the use of so-called "game assets" are still barely covered.

Most online games have in-game currency that can be purchased with fiat money and in-game items allowing to improve your characters' in-game features or stand out from other players. The price of such items can be as much as several million RUB, and it is suggested that there is a method used to determine their value.

For example, in Counter-Strike: GO gaming community, the price of skins (a game asset used to customize individual game elements rather than provide a game advantage) for weapons is determined based on 7 skin rarity types and 5 quality types.[6]

In addition, if an in-game item is included in the collection that is of particular interest to players, it greatly affects the final cost of a game asset.

Based on such classification, the cost of an iconic AWP gaming rifle in numerous online game asset marketplaces may vary from 5,000 RUB (a skin of average quality and low rarity from a regular collection) to 1.3 million RUB (a rifle of the highest rarity and quality from a most sought-after collection, Dragon Lore).[7]

Such type of game assets as loot boxes is worth mentioning as a separate point. This asset is a virtual case (box, chest) allowing to obtain random in-game items of various value after opening it. Loot boxes are often purchased with fiat money or require purchasing additional game keys to open them.

The society acknowledges the value of game assets determined by obvious factors: success in the game is possible either by spending much time in it or by investing large amounts of money in in-game items and in-game currency.

According to experts, Russian nationals spent approximately 135 billion RUB on games and in-game purchases over 9 months of 2023,[8] while in December 2023, President of the Russian Federation Vladimir Putin stated that the Russian gaming audience was approximately 60% of the population (88 million residents) of the Russian Federation.[9]

Today, in-game items are, unfortunately, used not only for their intended purpose, but may also be easily used for money laundering. Such practices are reported, *inter alia*, by gaming companies. For example, in 2019, Valve made a statement that the ultimate goal of almost all in-game purchases of CS:GO game keys to open loot boxes was money laundering.[10]

There are examples of criminal arrangements used by criminals to launder money with game currency via

---

1 The state of global cryptocurrency ownership. URL: https://www.triple-a.io/cryptocurrency-ownership-data (accessed on October 25, 2024).

2 Cryptocurrency market capitalization. URL: https://ru.investing.com/crypto/charts (accessed on October 25, 2024).

3 The Chainalysis 2024 Crypto Crime Repor. URL: https://go.chainalysis.com/crypto-crime-2024.html (accessed on October 25, 2024).

4 President of the Russian Federation V.V. Putin Meets with Director of Rosfinmonitoring. URL: http://www.kremlin.ru/events/president/news/72874 (accessed on October 25, 2024).

5 For more information see Global Compliance Institute: Cryptocurrencies—the challenges for criminals and investigators. URL: https://www.gci-ccm.org/insight/2022/01/cryptocurrencies-challenges-criminals-and-investigators (accessed on October 25, 2024).

6 See, e.g., CS 2 skin qualities by priority. All in-game skin rarities. URL: https://cyber.sports.ru/tribuna/blogs/cyberkotlets/3191977.html (accessed on October 25, 2024).

7 See, e.g., CS. Money. AWP. URL: https://wiki.cs.money/ru/weapons/awp (accessed on October 25, 2024).

8 See 135 Billion RUB Have Been Spent On Games And In-Game Purchases // Vedomosti, September 20, 2023. URL: vedomosti.ru/technology/articles/2023/09/20/995994-na-igri-i-vnutriigrovie-tovari-s-nachala-goda-potratili-135-mlrd-rublei?from=newsline (accessed on October 25, 2024).

9 See "Vladimir Putin Meets With Winners And Mentors of The All-Russian Professionals Skills Championship". URL: http://kremlin.ru/events/president/news/73019 (accessed on October 25, 2024).

10 See Valve Restricts CS:GO Key Trade As They Are Used for Money Laundering // Hacker. URL: https://xakep.ru/2019/10/30/csgo-keys/ (accessed on October 25, 2024).

mobile applications. The crime involves creating multiple email addresses using fake credentials to register mobile device accounts (such as Apple ID). Criminals link stolen bank cards to in-game accounts to transfer money. When an ID is created, the intruders download mobile applications to purchase in-game currency for money on bank cards. The ID is then sold together with all game assets making it very difficult to track the money.[11]

Most online games have separate in-game item marketplaces used to purchase and sale game assets for fiat currency and are not subject to any regulation.

In addition, a number of websites acting as marketplaces for in-game items used in online games with the largest audience (Dota2, CS:GO, etc.) were found on the Internet. Registration for trading on such platforms is often limited to linking the player's account in Steam, an online digital game distribution service. Withdrawal of proceeds from transactions on such platforms does not require to link any bank cards as the websites allow to make transfers via electronic payment systems such as PayPal and crypto wallets. You can receive the money as soon as possible, in a matter of minutes.

The lack of legal regulation of such trading practices, the availability of online platforms to general public, the ability to ensure enhanced anonymity of transfers, and rapid withdrawal of money—all these factors create perfect conditions for money laundering.

For example, Japanese media outlets report that national law enforcement agencies are concerned about the lack of regulation of in-game asset trading on online platforms, which leads to numerous cases of money laundering.

In particular, in July 2024, police in Kanagawa prefecture (Japan) uncovered a criminal arrangement involving purchases of in-game currency in a popular computer game, namely Lineage M. Using third-party bank card details, the hackers purchased large amounts of in-game currency and then sold it at a reduced price on an online platform they created. As a result, the criminals managed to earn approximately $18 million in 2014–2023.[12]

Another issue is the use of computer technologies by criminals that allow them to create game assets not designed by game developers. Using hacking programs, hackers create unlimited amounts of in-game currency and later convert it to fiat money, which may be used to commit crimes.[13]

The above facts prove the high relevance of game asset turnover regulation. However, in most countries, the risks associated with the use of computer games to commit crimes are not studied.

The exception is the European Union (EU). In 2023, the European Parliament issued Resolution No. 2023/C 214/03, which essentially is the first document capturing the EU's approach to game asset regulation.

The document mentions that provisions of Directive No. 2005/29/EC of the European Parliament and of the Council of May 11, 2005, concerning unfair business-to-consumer commercial practices, and Directive (EU) No. 2019/770 of the European Parliament and of the Council of May 20, 2019, on certain aspects concerning contracts for the supply of digital content and digital services, are extended to in-game trading systems.

The Resolution focuses on the lack of uniform legal regulation of loot boxes in the EU; thus, the European Parliament calls on the European Commission to review their purchase practices and take appropriate steps to develop a pan-European approach to the relevant regulation.

The same document indicates the increased money laundering risk as it is possible to exchange and sell in-game items on websites for fiat money. In addition, the European Parliament stated that Regulation (EU) No. 2022/2065 of the European Parliament and of the Council (the "Digital Services Act") "may help in solving this problem."[14]

This Regulation, in turn, contains some provisions aimed at improving regulation in the digital services industry. These require service providers to timely provide data of service recipients as requested by competent authorities; create systems allowing any individual or company to notify the provider of unlawful content in their system, if such persons believe that it is illegal; perform initial identification of traders on online platforms and require platform owners to assess the risks of unlawful use of the online platform and create dedicated teams to monitor compliance with the above Regulation.

Analysis of the provisions under consideration shows that in-game trading falls under the applicable legal definition of "Information Society Services," which implies that the Digital Services Act applies to such activities.

Directive No. 2019/770, which will apply to online games from January 2022,[15] is of further interest. In particular,

[11] See, e.g., 6 Major Data Breaches We Found and Reported in 2018 // MacKeeper. URL: https://mackeeper.com/blog/data-breach-reports-2018/ (accessed on October 25, 2024).

[12] See Japan police on alert as online game "real money trading" becomes crime hotbed. URL: https://mainichi.jp/english/articles/20240910/p2a/00m/0na/014000c (accessed on October 25, 2024).

[13] See Can you make a fortune by hacking a video game? URL: https://www.euronews.com/next/2022/08/20/can-you-make-a-fortune-by-hacking-a-video-game (accessed on October 25, 2024).

[14] See European Parliament resolution of January 18, 2023, on consumer protection in online video games: a European single market approach. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2023.214.01.0015.01.ENG&toc=OJ%3AC%3A2023%3A214%3AFULL (accessed on October 25, 2024).

[15] Directive (EU) No. 2019/770 of the European Parliament and of the Council of May 20, 2019, on certain aspects concerning contracts for the supply of digital content and digital services. URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32019L0770 (accessed on October 25, 2024).

Clause 1, Article 3 of the Directive mentions that its provisions also apply to any agreement where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price.

Special legal regulation of this sector exists in the People's Republic of China.

In 2010, the Ministry of Culture of the People's Republic of China issued an order approving the Interim Measures for the Administration of Online Games.[16] It provides for protecting the rights of minors, issuing permits to conduct business in cyber domain for companies, etc.

In 2023, it was reported that the Government considers a new expanded package of online game administration policies. The draft was posted on the website of the National Press and Publication Administration of China for public debate, but was subsequently removed. As of late 2024, there is no public information on whether they still work on the draft.

Some countries specifically consider the legal regulation of game assets such as loot boxes. However, there are different approaches to determining their legal nature. For example, in some jurisdictions, the opening of such cases is treated as gambling, which leads to restrictions or a ban on their purchase.

For example, in 2018, the Belgian Gambling Commission banned all uses of such assets.[17]

There is also a lot of discussion of this issue in the United States as the Federal Trade Commission (FTC) studies the effect of loot boxes on children. Legal amendments have been proposed to restrict the use of loot boxes in games for minors.[18]

In October 2023, Austrian gambling lawyer K. Rapani presented an overview of the most significant decisions of Austrian courts in this sector. Based on his generalization, we can conclude that, in some cases, Austrian courts state that the use of loot boxes is gambling, but there is no uniform approach to determining their legal nature.[19]

However, the UK decided not to regulate loot boxes as gambling in 2017.[20] Later, in 2022, Nadine Dorries, Secretary of State for Culture, Media, and Sport, stated that she was of the opinion that it was necessary to require that minors purchase loot boxes only with parental consent and explained that the issue of amending the UK Gambling Act related to loot box regulation was not discussed by the Government.[21] As of late 2024, no changes to this position have been announced.

The UK Gambling Commission's rationale for its refusal to regulate loot boxes is that, unlike casinos, loot boxes offer in-game items, which are confined for use within the game and cannot be converted to fiat money, rather than cash prizes.[22]

Canadian courts eventually had a similar position.[23]

However, its advocates believe that the argument related to the ability to gain profit from selling such items on third-party websites is meritless as it is almost always prohibited by user agreements of online games. In particular, this statement is often used by American courts as a reason to refuse to acknowledge the financial value of loot boxes.[24]

The above examples show that approaches to legal regulation of in-game currency in different countries vary from a complete ban or strict regulation to no regulation at all.

As for our country's experience, in the Russian Federation, the use of digital financial assets and digital currency is governed by Federal Law No. 259-FZ *On Digital Financial Assets, Digital Currency and Amendments to Individual Laws*, dated July 31, 2020.

However, this Federal Law only applies to assets and currencies defined in it.

In Russia, as in foreign countries, the issue applying this Federal Law to in-game currency used in computer games is still unresolved due to different opinions on whether in-game currency has any attributes of a digital financial asset (digital currency) or it is confined for use within a game.

The concept of "magic circle" first introduced by the Dutch philosopher J. Huizinga in his book *Homo Ludens: A Study of the Play-Element in Culture*, suggested that the game and

---

16 Interim Measures for the Administration of Online Games. URL: http://www.lawinfochina.com/display.aspx?lib=law&id=8179&CGid= (accessed on October 25, 2024).

17 Loot boxes in three video games violate gaming laws. URL: https://www.koengeens.be/fr/news/2018/04/25/loot-boxen-in-drie-videogames-in-strijd-met-kansspelwetgeving (accessed on October 25, 2024).

18 In-Game Currency Triggers State Gambling Laws, Rendering Mobile Game "Illegal Gambling". URL: https://www.fenwick.com/insights/publications/in-game-currency-triggers-state-gambling-laws-rendering-mobile-game-illegal-gambling (accessed on October 25, 2024).

19 Landmark decisions of Austrian courts in 2023. URL: https://www.imgl.org/publications/imgl-magazine-volume-3-no-1/landmark-decisions-of-austrian-courts-in-2023/ (accessed on October 25, 2024).

20 Loot boxes within video games. URL: https://www.gamblingcommission.gov.uk/news/article/loot-boxes-within-video-games (accessed on October 25, 2024).

21 Government response to the call for evidence on loot boxes in video games. URL: https://www.gov.uk/government/calls-for-evidence/loot-boxes-in-video-games-call-for-evidence/outcome/government-response-to-the-call-for-evidence-on-loot-boxes-in-video-games (accessed on October 25, 2024).

22 Loot boxes within video games. URL: https://www.gamblingcommission.gov.uk/news/article/loot-boxes-within-video-games (accessed on October 25, 2024).

23 See, e.g., Sutherland v. Electronic Arts Inc., No. 2023 BCSC 372. URL: https://cdn.ca9.uscourts.gov/datastore/opinions/2018/03/28/16-35010.pdf Sutherland v. Electronic Arts Inc., No. 2023 BCSC 372 (accessed on October 25, 2024).

24 See, e.g., United States District Court, Northern District of California, San Jose Division, case No. 20-cv-03901-BLF. URL: https://cases.justia.com/federal/district-courts/california/candce/5:2020cv03901/360878/82/0.pdf?ts=1641929411 (accessed on October 25, 2024).

all relations building in its course are limited by the game space and subject only to its specific game rules [1].

Russian courts have a similar position in civil disputes related to companies terminating access to in-game accounts or suspending certain game capabilities in online games. Analysis of civil proceedings in this sector[25] identifies several main arguments of the court:

- In-game currency is virtual, has no monetary value, and cannot be used for payments;
- Registration in the game and reading the user agreement equals to signing an agreement in the meaning of Articles 435 and 438 of the Civil Code of the Russian Federation (the "Russian Civil Code") and entails the obligation to comply with the rules of the game;
- Article 1062 of the Russian Civil Code (requirements related to game and bet management and participation in them) apply to all in-game processes, including the restrictions introduced by gaming companies for users, which, accordingly, rules out any related remedies.

Thus, some believe that in-game currency is the so-called non-convertible virtual currency, i.e. it is confined for use within the game and cannot be exchanged for fiat money in accordance with rules of the gaming company.

However, as mentioned above, there are black markets for such in-game currencies. The above facts indicate the volatility of such attribute of in-game currency as "non-convertibility," which is confirmed by the Financial Action Task Force (FATF). FATF acknowledges the financial value of such currency and that it can be used to finance crimes.[26]

Members of the Russian school of thought also treat in-game items as assets [2].

This approach appears to be consistent with contemporary legal relations caused by the digital transformation of society and meets the goals of combating the use of computer games to commit crimes.

In this regard, the Award of the Moscow Arbitration Court dated November 23, 2017, in case No. A40-153705/17-122-1361, related to remote gambling, where in-game items, rather than money, were paid as winnings, is significant.

The court rejected the defendant's (gaming company) arguments that the results of the games played on the website do not create potential profit for the players as in-game items do not have a real monetary equivalent and cannot be exchanged for cash. As a reason for its decision, the court stated that, given that there were numerous online marketplaces allowing to sell game assets, items received as winnings could be converted to real money; thus, it may be an alternative to gambling chips used by gambling establishments. Therefore, the court declared that the defendant created an online casino.

However, not every computer game is gambling, and a broad interpretation of Article 1062 of the Russian Civil Code is unacceptable.[27]

In addition, the issue of game asset classification as an asset has a criminal law element.

Some researchers have proposed that the theft of game assets shall be classified by amending Article 272 of the Criminal Code of the Russian Federation (the "Russian Criminal Code") (Illegal Access to Computer Information) and adding provisions on the illegal possession of virtual assets or by introducing a separate Article on the theft of virtual items and accounts [3].

However, given that it is possible to exchange virtual assets for fiat money (which, in turn, suggests that they have financial value, a key attribute of an asset), we believe that the above act has elements of crime under Article 158 of the Russian Criminal Code (Theft).

In this regard, it is worth noting that Russian courts have positive crime classification practice under Article 158 of the Russian Criminal Code in cases related to cryptocurrency, which is also a virtual asset.

For example, on June 24, 2021, the Third Court of Cassation upheld the prosecutor's cassation and overturned the verdict of the Petrogradsky District Court of St. Petersburg dated June 30, 2020, due to violation of the legal rights of the victim.

When considering the case, the District Court classified the theft of 5 million RUB in cash by the defendants as embezzlement and excluded the theft of the victim's cryptocurrency amounting to more than 55 million RUB from the scope of the charges.

The Court of Cassation ruled that cryptocurrency not only had economic and financial value, but was also used for payments, investments and savings, which could not prove that the item did not exist in the meaning of the Note to Article 158 of the Russian Criminal Code.[28]

A similar approach to game assets is used abroad.

A significant example is a criminal case heard by a court in the Netherlands in 2008 [4]. According to the facts of the case, two defendants had forced the victim to transfer in-game items on his in-game account to the account of one

[25] See, e.g., Appellate Ruling of the Civil Division of the Moscow City Court dated May 20, 2019 in case No. 33-21065/2019. URL: https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/0de6b77e-95c8-4707-8921-f762e36dd67d (accessed on October 25, 2024).

[26] Virtual Currencies: Key Definitions and Potential AML/CFT Risks. URL: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html (accessed on October 25, 2024).

[27] S.P. Grishaev, Yu.P. Svit, T.V. Bogacheva. Article-by-article commentary on the Civil Code of the Russian Federation. Part 2, Article 1062. URL: https://legalacts.ru/kodeks/GK-RF-chast-2/razdel-iv/glava-58/statja-1062/ (accessed on October 25, 2024).

[28] Cassation Ruling of the Third Court of Cassation in case No. 77-1411/2021 dated June 24, 2021. URL: https://3kas.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=5943246&delo_id=2450001&new=2450001&text_number=1 (accessed on October 25, 2024).

perpetrator by using violence against the victim. The act was classified under Article 312 of the Dutch Criminal Code (as robbery, i.e. an attack for the purpose of stealing someone else's assets committed with the use of life-threatening violence or with the threat of using such violence). The court ruled that, despite that in-game items are virtual, they were an asset as they had value and could be used and sold. The verdict was appealed by the defense, but the Supreme Court of the Netherlands upheld it.

We believe that Article 272 of the Russian Criminal Code may be reasonably applied to classify unlawful acts aimed at creating in-game currency.

Russian courts are already following this path. For example, in a criminal case heard in 2014, a criminal used a special computer algorithm to create in-game items, which he then sold to other users of the video game for fiat money. The court rendered a guilty verdict and classified the act under Part 2, Article 272 of the Russian Criminal Code.[29]

As for the prospects of separate legal regulation of loot boxes in the Russian Federation, it is worth noting that, according to experts,[30] gambling must meet three criteria:

1) Financial risk for the player, i.e. bets;

2) Uncertain outcome of the game;

3) Possible valuable winnings.

As this game asset meets all criteria and the definition of gambling in Article 4 of Federal Law No. 244-FZ *On State Regulation of Gambling Activities and Amendments to Individual Laws of the Russian Federation*, dated December 29, 2006, we believe that it is reasonable to apply this Federal Law to loot boxes.

The issues of regulation of game assets outlined in this study require prompt solutions to combat crimes involving such assets.

It seems that a ban on game asset trading may not be helpful given the constant growth in the number of players, the demand for gaming products, and the overall development of public relations around computer games. Harsh restrictions could lead to significant financial losses in the IT industry, which is not in line with the relevant Russian policy, including the Digital Economy National Project.

It is required to develop a balanced approach to accommodate the interests of *bona fide* users and gaming companies, as well as the State represented by its law enforcement and tax authorities.

We propose the following solutions based on foreign experience:

1. The Russian Federation shall develop federal laws governing the gaming industry with the following provisions:

1.1. Game assets shall be treated as assets for the purposes of criminal, civil, and tax laws.

We have mentioned that there is an issue of classification of crimes as the status of a game asset as an asset is not provided by law. It covers multiple offenses (e.g. the transfer of an in-game account with expensive game assets for financial gain may not be an offense under Articles 290 [Bribery] and 291 [Bribe-Taking] of the Russian Criminal Code; criminals can freely convert fiat money to game assets to avoid foreclosure of their assets, etc.).

The gap in laws may lead to violation of the rights of victims and the principle of equity provided by Article 6 of the Russian Criminal Code.

Based on the above, we propose to introduce laws governing the status of game assets as assets and classify them as a virtual asset. In this case, it is advisable to consider amending Para. g, Clause 3, Article 158 of the Russian Criminal Code to read as follows: "Theft from a bank account and theft of electronic money and virtual assets."

1.2. Game asset marketplaces shall be licensed and a ban on unfair business practices shall be applied to them.

We believe that, provided that individuals comply with anti–money laundering and terrorist financing regulations, gaming companies shall not restrict the rights of *bona fide* users to sell their assets.

It is worth noting that the content of game asset marketplaces shows their similarity to stock exchanges (the websites include price fluctuation charts for game assets, trade blotters, and other financial indicators[31]).

In addition, as operators of such platforms are not within the law, it creates unlimited opportunities for criminals to unlawfully enrich themselves by manipulating this gaming market.

For example, purchasing cheap skins and inflating artificially their value (by disseminating information in the media through bloggers and other media personalities, deliberately displaying and advertising such game assets during popular streams or eSports tournaments) allow to gain enormous profit, which may be used for unlawful activities (without any elements of crime under Article 185^3 of the Russian Criminal Code for the above reasons).

Considering that it is required to at least monitor suspicious in-game transactions and block in-game accounts to timely and effectively combat unfair trading

[29] Verdict of the Khoroshevsky District Court in case No. 1-260/2014. URL: https://actofact.ru/case-77RS0031-1-260-2014-2014-04-22-2-0/ (accessed on October 25, 2024).

[30] See, e.g., Patrick Sullivan. Video Game Industry Responds to Regulation of Pay-To-Win Microtransactions And Loot Boxes. URL: https://www.mondaq.com/unitedstates/gaming/839790/video-game-industry-responds-to-regulation-of-pay-to-win-microtransactions-and-loot-boxes (accessed on October 25, 2024).

[31] See, e.g., CS. Money: Dragon Lore AWP. URL: https://wiki.cs.money/ru/weapons/awp/dragon-lore (accessed on October 25, 2024).

practices and money laundering in the game asset sector, it is reasonable that gaming companies shall directly manage trading activities (other marketplaces do not have the appropriate authorities as they act only as trading intermediaries).

1.3. Game users involved in in-game trading shall be identified.

It should be noted that gaming companies address the issue of using in-game trading for money laundering purposes.

In particular, Steam prohibits trading and exchanging items for users that have not completed two-factor authentication. Price thresholds for in-game transactions have been set, above which a trade ban is applied to resale of acquired game assets. It is an effective arrangement preventing the theft of in-game accounts (the average ban duration is 1–2 weeks, and the victim can promptly contact the company and block the account before the assets on it are sold). In 2019, the platform officially banned trading and exchanging keys to loot boxes.

However, such efforts are not sufficient to eliminate the risks.

The cornerstone of existing security systems is the two-factor authentication, i.e. the use of both login and password and a unique code sent to the mobile phone specified during authorization to register and enter the game.

Today, existing capabilities enable seamless generation of random phone numbers to register in-game accounts. In addition, criminals may use stolen numbers to commit crimes, which does not provide any ground to consider two-factor authentication as an effective anti–money laundering tool.

It is necessary to address the issue of verifying the information provided by users upon registration.

For example, Second Life requires users to register through a subsidiary, Tilia Inc., which must comply with anti–money laundering (AML/CTF) regulations.[32]

As an appropriate measure to protect in-game trading, it is possible to provide a separate verification procedure, when linking a bank card to an account, by sending requests to banking institutions to verify the identity of its holder.

For each in-game transaction, the bank shall first send requests to the seller and buyer to confirm that they have made the transaction, and in case of a crime investigation, it will allow to reliably identify the perpetrators.

1.4. Game providers shall monitor information on the provision of services for the sale of game assets by unlicensed companies and individuals to impose penalties on the perpetrators.

Such offers are distributed by creating websites, open communities in social media, and in-game chats. Gaming companies shall block the accounts of persons offering such services within games as soon as possible. If relevant online communities or websites are identified, it is advisable to provide information to Roskomnadzor to block them.

1.5. Gaming companies shall create analytical departments to monitor suspicious transactions.

A comprehensive analysis of in-game transactions will allow to timely identify suspicious transactions and prevent risks of criminal use of game assets.

We believe that high-quality monitoring of trading activities shall be based on the following information:

- When the account is created;
- When a bank card is linked to an account; When the first transaction is made;
- How many hours a person spends in the game;
- The person's game performance (game achievements);
- Frequency of transactions made by a person;
- Whether the price set by persons for a game asset matches its average market price.

A set of such indicators will help to identify whether a person is a *bona fide* player using a computer game for entertainment or a person, who is not interested in the game and uses the gaming app as a money laundering channel.

1.6. Gaming companies shall cooperate with law enforcement agencies.

We consider it necessary that the relevant obligations shall, first, include the requirement to provide law enforcement agencies with information on persons engaged in in-game trading and suspicious transaction identified during monitoring.

1.7. There shall be requirements to user agreements between gaming companies and players.

It is related to the need to protect the rights of players. Many gaming companies adopt user agreements with the only purpose of protecting their interests rather than the rights of service recipients; therefore, they often have discriminatory provisions.

For example, in the famous case of *Bragg v. Linden Research, Inc.*, a gaming company blocked a user's account, because the user was in breach of the user agreement. The claimant, whose game assets on the blocked account were worth several thousand US dollars, filed a lawsuit citing that provisions of the user agreement violated the law.

In particular, Linden Research, Inc.'s user agreement provided that the company might block a user's account

[32] See Gaming the System: Money Laundering Through Online Games. URL: https://www.rusi.org/explore-our-research/publications/rusi-newsbrief/gaming-system-money-laundering-through-online-games (accessed on October 25, 2024).

at any time without giving any reason. However, it provided for a "suspicion of violation of the law" as a sufficient basis for the refusal to return funds to users.[33]

The court ultimately declared that the company's rules violated the law and ordered to reinstate the account under the settlement agreement of the parties.

It is possible that a person, who has spent time and financial resources in a gaming system, may lose his or her game assets for reasons contrived by the company and will not have effective remedies, which is unacceptable given the financial value of game assets.

2. Application of FATF standards to game assets.

In accordance with generally accepted anti–money laundering standards provided in FATF recommendations, we believe that it is required to treat game assets as a virtual asset defined as a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes.[34] Given that game assets meet the above definition, it is natural that FATF Recommendation 15 (New Technologies) shall be applied to them.

We believe that the implementation of these proposals will ensure a comprehensive approach to regulating the virtual asset turnover and significantly reduce the risks of criminal use of in-game trading.

If we properly address the above issues, when addressing issues of combating money laundering, and intensify law enforcement efforts in this sector, it will help to eliminate the risk of violating the rights of *bona fide* individuals and criminals will lose yet another way to launder money.

REFERENCES

1. Huizinga J. *Homo Ludens: an attempt to define the game element of culture.* Saint Petersburg: Ivan Limbach Publishing House; 2011. 416 p. EDN: QPUPXF

2. Lisachenko A.V. Law of virtual worlds: new objects of civil rights. *Russian legal journal*. 2014;(2):104–110. EDN: SFPBYV

3. Safronuk AO, Grimalskaya SA. On the issue of criminal liability for the theft of virtual gaming items and accounts in the Russian Federation. *Education and Law.* 2023;(5):378–381. EDN: EMMSCX doi: 10.24412/2076-1503-2023-5-378-381

4. Budylin SL. *The case of the immaterial fish and other stories. Notes of a comparativist.* Moscow: Infotropic-media; 2017. 308 p. (In Russ.)

СПИСОК ЛИТЕРАТУРЫ

1. Хейзинга Й. Человек играющий: опыт определения игрового элемента культуры. Санкт-Петербург: Издательство Ивана Лимбаха, 2011. 416 с. EDN: QPUPXF

2. Лисаченко А.В. Право виртуальных миров: новые объекты гражданских прав // Российский юридический журнал. 2014. № 2(95). С. 104–110. EDN: SFPBYV

3. Сафронюк А.О., Гримальская С.А. К вопросу об уголовной ответственности за кражу игровых виртуальных активов и аккаунтов в Российской Федерации // Образование и право. 2023. № 5. С. 378–381. EDN: EMMSCX doi: 10.24412/2076-1503-2023-5-378-381

4. Будылин С.Л. Дело о нематериальной рыбе и другие истории. Записки компаративиста. Москва: Инфотропик-медиа, 2017. 308 с.

[33] See Para. 88 No. CIV.A.06 4925. Marc BRAGG v. LINDEN RESEARCH, INC. URL: https://scholar.google.co.uk/scholar_case?q=Bragg+v.+Linden&hl=en&as_sdt=2006&case=583434033289222111 (accessed on October 25, 2024).

[34] See International standards on combating money laundering and the financing of terrorism and proliferation updated November 2023, page 137. URL: https://www.fatf-gafi.org/content/dam/fatf gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf (accessed on October 25, 2024).

AUTHOR INFO

***Anton A. Dyachenko,** prosecutor, lawyer of 3rd class;
ORCID: 0009-0001-8890-1692; e-mail: dyachenko.a@genproc.gov.ru

Sergei V. Plokhov, Cand. Sci. (Jurisprudence), state counsellor of justice of 3rd class; ORCID: 0009-0001-6311-0640;
eLibrary SPIN: 1539-9875; e-mail: s4286@mail.ru

ОБ АВТОРАХ

***Антон Андреевич Дьяченко,** прокурор, юрист 3-го класса;
ORCID: 0009-0001-8890-1692; e-mail: mr.anton.rusanov@mail.ru

Сергей Владимирович Плохов, канд. юрид. наук,
государственный советник юстиции 3-го класса;
ORCID: 0009-0001-6311-0640; eLibrary SPIN: 1539-9875;
e-mail: s4286@mail.ru

* Corresponding author / Автор, ответственный за переписку