RUSI
www.rusi.org

Gaming the System: Money Laundering Through Online Games

Anton Moiseienko and Kayla Izenman

In-game artefacts and currencies often have real-life value and can be used to move or invest criminal proceeds. But there are no clear expectations of what game operators can or should do to identify criminal activity.

Online games – especially massive multiplayer online role-playing games – have long been suspected of offering an avenue for moving or otherwise using criminal proceeds, a process known as money laundering. As early as 2013, cybercrime analyst Jean-Loup Richet wrote, based on his investigation of hacker forums, that 'using the virtual currency systems in [online] games, criminals in one country can send virtual money to associates in another country'.

If criminal money has indeed poured into online gaming worlds, one could hardly think of a better demonstration of 'the displacement effect': the notion that as some parts of the economy become ever more tightly regulated, tainted money goes elsewhere, like the air in a squeezed balloon. But how exactly can online games be used for money laundering, what evidence is there of this happening, and what should be done about this?

The State of Play

The key factor that makes money laundering through online games possible is that virtual, in-game items sometimes have a real-life value outside the game. This includes, for instance, artefacts that vest the player's character with additional powers (such as swords, armour, and magic potions) or 'currency' that can be used to purchase them.

Some games officially allow the purchase and sale of in-game items for government-issued fiat currency, such as dollars or pounds. This practice is known as 'microtransactions' and is particularly widespread in games that are free to play but offer paid in-game items. For example, *Second Life* and *Entropia Universe* allow in-game purchases through their official stores. Furthermore, a growing number of games resort to gambling-style microtransactions by selling 'loot boxes', a collection of randomly selected in-game artefacts whose contents are only revealed to the buyer after purchase.

> *Online games are not regulated, which means there are no clear expectations of what game operators can or should do to identify criminal activity*

According to analysis by Juniper Research cited in the Parliament of Australia's 2018 enquiry (p. 5), sales of loot boxes generated 25% of the global gaming industry's revenue of $117 billion. In 2016, Electronic Arts (EA) reported that loot boxes account for $650 million per year, roughly 30% of EA's digital sales revenue.

In other instances, in-game items are traded unofficially on online marketplaces extraneous to the game. This underground trade has historically been closely related to 'gold farming', the practice of playing online games specifically to obtain valuable items and resell them to other gamers. Gold farming had its heyday in the mid-2000s, when economist Edward Castronova estimated (p. 149) that eBay was trading $30 million worth of in-game goods per year, with *World of Warcraft*'s 'gold' trading against the US dollar at a higher exchange rate than that of Japanese yen.

Unofficial sale of in-game items can contravene the game's rules and has given rise to several court disputes in the US (Blacksnow Interactive vs. Mythic Entertainment, Inc.; Hernandez vs. Internet Gaming Entertainment Ltd; and MDY Industries vs. Blizzard Entertainment). For instance, *World of Warcraft* does not allow direct purchases of its 'gold' with fiat currency, but does offer a special token that can be purchased for £17 and auctioned off for gold in-game. In 2007, eBay announced a clampdown on listings of digital products obtained in breach of software use agreements, including in-game items. However, a number of English-language websites, such as PlayerAuctions, g2g.com or iGVault, continue to list in-game items.

Since in-game items can be used to store value, some may be tempted to convert illicit income into them. In January 2019, cyber security firm Sixgill published its findings on money laundering through V-bucks, an in-game currency used in the online computer game *Fortnite*. According to Sixgill, criminals were using stolen bank card details to buy V-bucks from the official *Fortnite* store and then selling them at a discounted rate to other players on the dark web or through social media platforms. Similarly, Kromtech, a software development company, reported that

The in-game items and currencies that run the virtual economies of online games can have real-life value outside of the game. The trade and sale of these through official and unofficial channels poses a new environment of money-laundering risks. *Courtesy of Anastassiya/stock.adobe.com*

a cyber-criminal group had automated the use of stolen card details to create a large number of Apple IDs, bought in-game items in mobile games such as *Clash of Clans* or *Marvel Contest of Champions*, and resold them on third-party websites for fiat currency.

In essence, buying in-game items with stolen card details is no different from the online purchase of any good, tangible or intangible, with stolen card details. The primary responsibility for detecting this criminal activity lies with the payment processing company. That said, the gaming company can possess valuable intelligence about the criminal's in-game activities, such as interactions with other players, which may shed light on their identity or expose criminal networks.

There is evidence of 'lifestyle spending', or people using criminal income to play online games. In 2016, Kevin Lee Co admitted to stealing $4.8 million from his work, of which he spent $1 million on in-app purchases in the mobile game *Game of War*. In 2018, former library director Adam Winger pled guilty to theft and forgery after stealing $89,000 from the library, also to use on in-app purchases in *Game of War*.

Lifestyle spending aside, it is easy to imagine a scheme designed to move criminal income. Suppose a drug trafficker deposits cash with a poorly regulated overseas bank. Instead of making a transfer to their accomplice's UK bank account, they can purchase online game currency and hand it over to the accomplice's in-game character, who can then in turn resell it for fiat money. Alternatively, instead of transferring specific in-game items, she can hand over the log-in details from her entire game account. Although the authors are not aware of confirmed case studies, similar methods were discussed in the cybercrime forum messages cited in Jean-Loup Richet's 2013 report.

Whether a currency or commodity is valuable depends on whether people treat it as such

In contrast, cybercrime involving online games is well-documented, specifically stealing login credentials and then selling the hacked user's in-game possessions. According to TrendMicro, some scam websites offering in-game items for sale require customers to disclose their gaming login details, thus giving hackers access to their account. As early as 2012, the same company reported that computer game hacking is especially widespread in China given its large gaming community. In August 2019, FireEye alleged that APT41, a leading Chinese cyber-criminal group, was systematically targeting the video game industry, and in one case 'in less than three hours the group generated tens of millions of dollars of a popular game's virtual currency [which was then] most likely sold and laundered in underground markets' (p. 19).

Besides their value-transfer functionality, online games can also have some appeal to criminals due to the communication channels they offer, varying from moderated text chats to unfiltered audio chat. For example, in 2018, the FBI presented Sony with a search warrant for a suspect's PlayStation 4 data as part of an active terror investigation. Documents leaked by Edward Snowden show that UK and US signal intelligence agencies (the National Security Agency and GCHQ) both collected information and data

from *World of Warcraft*, *Second Life* and *Xbox Live*, reportedly due to a fear that terrorists might be both communicating and moving funds through these platforms.

Outflanked by Regulation?

If a computer game allows players to transfer in-game items to each other, and these in-game items can be exchanged into fiat currency, the gaming company's position is similar to that of a virtual currency exchange. But unlike gaming companies, virtual currency exchanges should be subject to anti-money laundering/counter-terrorist financing (AML/CTF) regulation as per the October 2018 revision of the Recommendations of the Financial Action Task Force (FATF), the global AML/CTF standard-setter. Under these rules, regulated businesses are required to identify their customers, monitor their activity and report suspicions of criminality to authorities.

In 2016, Electronic Arts (EA) reported that loot boxes account for $650 million per year, roughly 30% of EA's digital sales revenue

On 1 July 2019, Linden Lab, the developer of the online game *Second Life*, announced that all *Second Life* users would henceforth need to register with its fully owned subsidiary Tilia Inc., a money service business (MSB) licensed in 46 US states. As an MSB, Tilia is required to comply with AML/CTF obligations under the Bank Secrecy Act and its implementing regulations, including in relation to customer verification and suspicious transaction reporting.

The 47-page discussion of the announcement on *Second Life's* official forum displays some consternation among the game's users, some of them worried that cashing out from Linden Dollars into fiat currency might become more complicated. The fact that Linden Lab itself had already been a registered MSB for at least several years – its licence was last renewed in December 2017 according to the official MSB register – has attracted relatively little attention, although it suggests that the company had long ago concluded it had to comply with US AML/CTF rules.

Besides their value-transfer functionality, online games can also have some appeal to criminals due to the communication channels they offer

The expanding international and domestic regulation of virtual currencies, also known as virtual assets, may have played its part. In October 2018, the FATF updated its Recommendations so as to require states to regulate and licence or register virtual asset service providers (VASPs). The FATF uses the following definition of virtual assets: 'A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes'.

The FATF also published guidance on virtual assets, which is similar in key respects to the 2013 and 2019 documents issued by the US financial intelligence unit, the Financial Crimes Enforcement Network (FinCEN). Neither the FATF nor FinCEN states whether in-game currencies are covered by AML/CTF regulations, but if one accepts the FATF definition as a starting point, the first question must be whether a given in-game currency constitutes 'a representation of value'.

Both in the physical world and online, whether a currency or commodity is valuable depends on whether people treat it as such. As the prices of Bitcoin and other cryptocurrencies demonstrate, a virtual currency can acquire significant economic value in the eyes of the public. If in-game items can be traded, officially or unofficially, there is a strong argument that they meet the FATF's virtual asset definition.

Even if it is a third-party trading platform that enables such trade, the game developer can face AML/CTF obligations in its capacity as the issuer of virtual currency. Crucially, the FATF's definition encompasses not only decentralised virtual currencies such as Bitcoin or Ether, which are maintained by a dispersed user community without a central administrator, but also those currencies that, like Linden Dollars, are issued by central administering entity.

This analysis applies not only to in-game currencies but also to any other in-game items. There is no obvious reason why their function within the game should make a difference; what matters is whether they are traded for fiat currency, which is evidence of them being a digital representation of value.

Since many games do not intend their items to be traded, it is arguably unfair for the game operator to bear the burdens of AML/CTF regulation solely on account of in-game items being traded through an unauthorised third-party website, on that account. But a virtual item can be used as a substitute for value and thus be exploited for money laundering regardless of whether it is traded officially or unofficially; nor would drawing such a distinction have any basis in the FATF's definition of a virtual asset or VASP.

Since in-game items can be used to store value, some may be tempted to convert illicit income into them

In practice, one might expect that the games with the largest in-game economies, official or unofficial, will be the first to either appear on the authorities' radar or decide to take AML/CTF measures. In *Second Life's* case, for instance, Linden Lab estimated in 2013 that the

Table 1: Examples of In-Game Currencies and Their Value

Game	Currency	Estimated Exchange Rate	Example Exchanges
Clash of Clans	Gems	$1 = 80 gems*	G2G, PlayerAuctions, PlayerUp, MMOCS, EpicNPC
Clash Royale	Gems	$1 = 80 gems*	G2G, PlayerAuctions, PlayerUp, MMOCS, EpicNPC
Counter Strike: Global Offensive	Keys	$1 = 0.4 Case Key†	Official Steam Marketplace, G2G, BitSkins, KeyVendor
Entropia Universe	Project Entropia Dollars (PED)	$1 = 10 PED‡	PlayerUp, MMOCS, EpicNPC
EVE Online	PLEX, ISK	$1 = 227m ISK§	G2G, PlayerAuctions, PlayerUp, MMOCS, EpicNPC
Final Fantasy XIV	Gil	$1 = 881,057 Gil§	G2G, PlayerAuctions, PlayerUp, MMOCS, EpicNPC
Fortnite	V-Bucks	$1 = 120 V-Bucks^	PlayerAuctions, PlayerUp, MMOCS, EpicNPC
League of Legends	Riot Points (RP), Blue Essence	$1 = 130 RP¶	G2G, PlayerUp, MMOCS, EpicNPC
Marvel's Contest of Champions	Units	$1 = 23 units*	G2G, PlayerAuctions, PlayerUp, MMOCS, EpicNPC
RuneScape	Gold	$1 = 7.6m gold§	PlayerAuctions, PlayerUp, MMOCS, EpicNPC
Second Life	Linden Dollars (LD)	$1 = 308 LD**	G2G, PlayerAuctions, PlayerUp, EpicNPC
World of Warcraft	Gold coins, tokens	$1 = 8,751 gold††	G2G, PlayerAuctions, PlayerUp, MMOCS, EpicNPC

**: Varies by item purchased, based on in-app purchase price.*
†: Case Key price on Stream Community Marketplace.
‡: See Etropia Universe, 'Think Future – Invest in your Avatar!', <https://account.entropiauniverse.com/account/deposits/>, accessed 11 October 2019.
§: Based on the average price of a transaction on PlayerAuctions.
^: Based on V-buck bundle on the Microsoft Store.
¶: Based on price of prepaid game cards, see League of Legends, 'League of Legends Prepaid Game Cards', <https://na.leagueoflegends.com/en/community/prepaid-cards >, accessed 11 October 2019 .
***: See CurrencyRate, '1 USD US Dollar to LD Linden Dollar', <https://usd.currencyrate.today/ld>, accessed 11 October 2019.*
††: According to the $20 price for one token on the official Blizzard Shop, and an estimated auction price of one token for 175,018 gold as per WoWTokenPrices.

value of its in-game transactions over the preceding 10 years reached $3.2 billion, a scale that few games have achieved.

A Bit of a Gamble

In many countries, gambling is either prohibited or regulated. If an online game involves microtransaction mechanics with an element of chance, it can potentially fall within the gambling regulatory regime. For instance, in several games, such as *Grand Theft Auto Online* and *Red Dead Online*, a user's character can gamble in an in-game casino.

Given the risk that such activities may amount to unlawful gambling, some game developers take action to avoid legal repercussions. Shortly after the FBI expressed interest in one of the virtual casinos operating within *Second Life* in 2007, Linden Lab instituted a policy whereby only skill-based games, which are not captured by the US definition of gambling, are permitted. In *Red Dead Online*, the availability of poker varies from one US state to the other, depending on the local legislation, even though playing it does not involve virtual items that are convertible into fiat currency.

In Great Britain, the Gambling Commission's view is that to come under gambling regulation, a game must 'look and feel like traditional gambling' and involve bets or payouts in 'money or money's worth' (p. 6). The Commission also suggests that in-game items constitute money or money's worth if they are traded for fiat currency – but, it seems, only if it happens 'on a marketplace within a platform *operated by the game's developer or distributer*' (p. 4, authors' emphasis). The UK Parliament's Digital, Culture, Media and Sport Committee concurs with most of the Gambling Commission's analysis but argues that in-game items can be 'money's worth' due to their subjective value for the player even if they cannot be converted into fiat currency. Even if regulators or law enforcement agencies deem a computer game to involve gambling, it will not necessarily be subject to AML/CTF requirements. For instance, the EU's 4th Money Laundering Directive allows countries to exclude non-casino gambling operators from their AML/CTF regime if a national risk assessment so warrants. In the UK, the position is yet more complex: although only casinos are subject to Money Laundering Regulations 2017, other gambling outlets operating in the UK face similar AML/CTF requirements as a condition for obtaining a licence.

The Gaming Industry's Next Quest

To restate the issue, if traded for fiat currency, whether on a game's official platform or elsewhere, in-game items can be alluring to criminals. They can be stolen through hacking, purchased with stolen card details or simply bought for fun using criminal income. And although primary responsibility for preventing the latter two issues lies with the payment processing company, a wealth of information on the criminal's behaviour, such as transfers of in-game items from one character to another, is only going to be accessible to the company operating the game while having potential law enforcement value.

A growing number of games resort to gambling-style microtransactions by selling 'loot boxes', a collection of randomly selected in-game artefacts whose contents are only revealed to the buyer after purchase

Yet online games are not regulated, which means there are no clear expectations of what game operators can or should do to identify criminal activity. For instance, while they could conceivably monitor changes in gaming patterns or IP use to identify accounts surreptitiously transferred from one user to another, whether doing so would be necessary or proportionate is subject to debate – a debate that is not yet happening.

So far, governments have confined their examination of in-game transactions to consumer protection and/or gambling issues arising from 'loot boxes', including inquiries by the US Federal Trade Commission, the Parliament of Australia and the UK Parliament, as well as papers published by various state authorities in Belgium, France and the Netherlands, among others.

Important as these matters are, possible criminal abuse of online games also deserves attention. Although subjecting online games to AML/CTF regulation absent further evidence would be a step too far, governments should engage with the industry to clarify expectations in relation to the identification of criminal conduct and its reporting. In the absence of an industry regulator, one of the issues governments will need to resolve is who exactly should drive that conversation.

As for the industry itself, there is little doubt that even in the absence of regulation, game developers have the powerful incentive to safeguard their reputation and be good corporate citizens. To do so, they should consider instituting customer verification and voluntary reporting of suspicious activity to law enforcement if their in-game items trade for fiat currency, whether officially within the game or on extraneous platforms.

Anton Moiseienko
Anton is a Research Fellow at RUSI's Centre for Financial Crime & Security Studies.

Kayla Izenman
Kayla is a Research Analyst at RUSI's Centre for Financial Crime & Security Studies.

This article forms part of the Financial Crime 2.0 research programme sponsored by EY and Refinitiv. The authors are grateful to all those who have generously taken their time to discuss this research with them.

The views expressed in this article are the authors' and do not represent those of RUSI or any other institution.