Online Video Games: Cyberlaundering Vulnerabilities and Controls

James Higgs and Stephen Flowerday
The University of Tulsa
jah0701@utulsa.edu

Abstract

The online video game market is predicted to be valued at $321.6 billion by 2027. Today, younger generations increasingly prefer spending time playing video games compared to consuming content on popular streaming platforms. Beyond providing a leisurely — and competitive — activity to the bulk of its user base, online video games have provided cybercriminals with an environment free from the reigns of legal enforcement. More specifically, with the rising popularity of the microtransaction business model, money launderers are provided with novel channels to move their illicitly gained funds. A growing body of evidence highlights that money laundering is taking place through online video games. Foremost, criminals are attracted to the anonymity and global reach offered by online video games. Few to no controls are currently in place to disrupt the laundering process in online video games. Furthermore, regulation continues to play catch up with cybercriminals' latest laundering strategies. This study explores and discusses money laundering in the context of online video games. Vulnerabilities that enable money laundering in online video games are identified. Potential controls to reduce the scale of laundering are proposed.

1. Introduction

Money laundering is not a new phenomenon. Rather, it has taken on a variety of forms throughout history as enabled by the societal and technological innovations present at the time. For example, three thousand years ago Chinese merchants were hiding their wealth for fear of having their hard-earned money plundered by the dynasty (Morris-Cotterill, 2001). Researchers and legal scholars have offered varying definitions of money laundering. Definitions are premised upon whether an economic, societal, political or legal perspective is adopted (Irwin et al., 2012). FinCEN (2023) defines money laundering as:

> *"… disguising financial assets so they can be used without detection of the illegal activity that produced them."*

Traditionally, money laundering operations were strictly contained within the physical world. For example, cash smuggling and wagering are typical activities that would unfold within the physical world of money laundering (Leslie, 2014, p. 18 - 24). Once tighter controls were implemented around the physical world of money laundering, there was a noticeable shift towards wire transfers away from cash intensive laundering operations (Bortner, 1996). Bortner, somewhat scarily, prophesied that tighter controls would continue to emerge, forcing criminals to move their illicit activities elsewhere (Bortner, 1996). The migration of criminals to less tightly regulated environments has become known as the displacement effect (Akartuna et al., 2022b). True to Bortner's word, in the wake of 9/11, the enforcement of know-your-customer (KYC) policies reached an all-time high in the United States (Stevens, 2015). Spearheaded by President George Bush and the U.S. Congress, the USA PATRIOT Act was passed to alleviate the threat of further terrorism, and in addition, address money laundering concerns. Rather abruptly, financial institutions were compelled by legislation to identify their customers during customer onboarding processes, to report suspicious activities, and implement internal controls in the fight against money laundering (FinCEN, 2023a).

Placing the efficacy of such controls to the side, today, clear indicators of a further displacement — by a subset of criminals — to the safe havens of the internet away from a tightly regulated financial sector have

surfaced. The internet, with its promise of anonymity and global reach has provided a fertile playground for cybercriminals to conduct their illegal activities with little fear of repercussion (Filipkowski, 2008; Leslie, 2014, p.59). One such avenue is money laundering through online video games (Akartuna et al., 2022a; Irwin et al., 2014; Moiseienko & Izenman, 2019; Sixgill, 2019)

Currently, there are 5.16 billion active internet users, constituting 64.4% of the global population (Statista, 2023). In Deloitte's most recent survey of U.S. consumers, it was found that the majority of Generation Z, millennials, and Gen X play video games regularly, averaging 11 hours weekly per person (Arkenberg & Westcott, 2022). Half of the respondents for the U.S. market noted that gaming *takes preference over* consuming content on video streaming platforms (Westcott et al., 2022). This preference is even stronger in younger generations (Westcott et al., 2022). Similarly, PwC concluded that video games are the most popular past time for younger generations (PwC, 2022). The video game market was valued at $214.2 billion in 2021, and projections indicate that it will reach $321.6 billion by 2026 (PwC, 2022). This market valuation excludes e-sports, the competitive arm of online video gaming, a market valued at $1.38 billion in 2022 (Statista, 2023). It is no longer possible to view video games as a 'niche,' instead, it has entered mainstream culture and continues to see increased uptake (Stuart, 2023).

As mentioned, money laundering takes place through a variety of internet-driven mediums (e.g., sharing economy, e-commerce, online video games). However, this study focuses specifically on money laundering through online video games. Further, this study seeks to answer the following research question:

> *What controls can be implemented in online video games to introduce friction into the laundering process?*

This study readily acknowledges that it is not possible to 'solve' the problem of money laundering. Instead, this study advocates for an approach that seeks to make the laundering process more difficult for cybercriminals. By introducing the appropriate controls, money laundering becomes more difficult through *increased friction*, and as a result, the scale of laundering is reduced.

This study is structured as follows. Section 2 introduces cyberlaundering and credit card fraud. Section 3 explores online video gaming and its relation to cyberlaundering. Section 4 contributes to the literature base by identifying vulnerabilities and providing controls that can be implemented to introduce added friction into the money laundering process that is taking place in online video games. Vulnerabilities and controls were identified by means of an exploratory narrative literature review — a technique used to collate and present multiple pieces of disperse information about a given topic.

2. Cyberlaundering

To some, defining cyberlaundering may be just as elusive as the phenomenon itself. Leslie (2014, p.55) argues that any definition of cyberlaundering must necessarily entail both dimensions of cybercrime and money laundering. It is not adequate to simply view cyberlaundering as a money laundering technique, but rather to view it as a more advanced and technologically-driven iteration of money laundering in and of itself (Leslie, 2014, p.62). The definitions that Leslie warns against abound in the literature, including the popular press. Leslie (2004 p.60) defines cyberlaundering as:

> "… the use of a computer to form a transaction or a relationship involving property or benefit, whether tangible or intangible, which is derived from criminal activity."

The goal, as with traditional money laundering, would be to obfuscate the audit trail of the illicitly gained funds for reintegration back into the financial economy (Akartuna et al., 2022b). This study contends that Leslie is fundamentally correct as to the appropriate way in which to frame and define cyberlaundering. If cyberlaundering is only to be viewed as a technique, rather than as a more advanced iteration of money laundering, it has potentially harmful ramifications for not only the seriousness, but also urgency with which the problem is treated.

Cyberlaundering and card fraud

Cyberlaundering and predicate crimes share an inextricable link. A predicate crime is an offence that precedes the crime of money laundering and is the source of the illegally acquired funds (Leslie, 2014, p. 3). For example, cybertheft and cyberfraud are predicate crimes which often precede cyberlaundering. More specifically, in the case of cyberlaundering through online platforms, credit card fraud is the most commonly reported — and perhaps most frequently occurring — predicate offense (Cox, 2017; King et al., 2021; Sixgill, 2019; Teicher, 2018). Cybercriminals have found unique ways in which to extract value from stolen credit cards, and in turn, launder funds to hide the illicit origin of the funds. This pattern of credit card fraud preceding cyberlaundering can be found on a variety of online platforms, including ridesharing (Busby, 2018; King et al., 2021; Teicher, 2018), short-term rentals (Cox, 2017; Fazzini, 2019) and streaming platforms (Grayson, 2022; Stanton, 2022). With direct relevance to this study, the same pattern is to be found in cyberlaundering through online video games (Moiseienko & Izenman, 2019; Sixgill, 2019). It is trivially easy to obtain stolen credit card details which can be used for illicit purposes. As of 2022, U.S. issued credit card details accompanied by a CVV costs $17.00 on the dark web (Ruffio, 2022). Similarly, a stolen PayPal account with a minimum balance of $1000.00 would cost a cybercriminal $20.00 to obtain off of the dark web (Ruffio, 2022). In some instances, PayPal shares direct integration with online video games as an accepted payment mechanism (Irwin et al., 2012).

It has been remarked that it is creativity, not avarice, that lies at the center of the launderer's ability to perpetually evade law enforcement (Bortner, 1996; Gilmour, 2023; Leslie, 2014, p.86). One would be hard pressed to find a more apt example of a launderer's creativity than laundering illicitly gained funds from stolen credit card details through online video games. The remainder of this paper explores cyberlaundering within the context of online video games.

3. Cyberlaundering and online video games

Keene, commenting a decade ago, noted that at the time cybercrime in *virtual worlds* remained an understudied domain (Keene, 2011). A virtual world is an environment hosted on a server — or more likely servers — that enable people to interact and accomplish goals through online avatars (Castronova, 2005, p.4 - p.6). In the virtual world, interactions and gameplay decisions are not defined by lawlessness. Instead, game developers put constraints in place that define the boundary of acceptable interaction amongst players, including the rules of gameplay (Castronova, 2005, p.153). Put more simply, a virtual world is *that environment* within which the gamer finds himself and engages with when playing the game. Fast forward to today, of the extant studies available, the majority are characterized by superficial analyses and over simplistic models of cyberlaundering in virtual worlds (Irwin et al., 2012; Matteo, 2022). Few studies explore cybercrime in virtual worlds, including cyberlaundering (Matteo, 2022). Matteo (2022) comments:

> "Since the first virtual world release, *nothing* has been done to develop knowledge and regulations further. As a result, today, these platforms remain *under-regulated, understudied and unmonitored*."

Naturally, this raises the question: why? It may be that the research community has erroneously interpreted the nature of video games; a virtual world to unwind in, free from the stresses of daily life (Keene, 2011). However, the evidence of cyberlaundering in virtual environments illuminates that online video games have interaction effects with the real world, and as such, it is not enough to place an artificial barrier around online video games and suggest that they are merely a virtual affair (Castronova, 2005, p.147; Chambers-Jones, 2018; Keene, 2011; Stevens, 2015). If nation states and the intelligence community view online video games as an *ongoing* threat to national safety (e.g., terrorism and money laundering opportunities) there is no reason why the academic community should not adopt a similar stance (Stevens, 2015). Arguably, it is the most problematic form of cyberlaundering currently available to the cybercriminal (Leslie, 2014, p.86).

3.1 What is virtual currency?

Virtual worlds are accompanied by their own currencies, politics and social dynamics (Chambers-Jones, 2018; Leslie, 2014, p.87). Economies in online video games closely resemble that of everyday economies. Supply, demand and inflation are not concepts foreign to virtual world economies (Holm & Mäkinen, 2018). More specifically, virtual world economies are to be considered every bit as *real* as an ordinary economy (Castronova, 2005, p.174). An integral part of a virtual economy is naturally, virtual currency. Virtual currency is a digital encapsulation of value that can be digitally traded (FATF, 2014). It shares the standard three characteristics of fiat currency — medium of exchange, unit of account and store of value — with the caveat that it does not have legal tender (FATF, 2014). Instead, a virtual currency has purchasing power because the community within the virtual world recognizes that the currency allows access to the attainment of unique items (i.e., items of *value*). Exemplary items of value include a virtual sword, a virtual clothing item, or, even purchasing a monthly subscription to the game (Castronova, 2005, p.148). Currencies are either convertible, or non-convertible. Convertible currency can be exchanged back and forth into fiat currency through official channels. Conversely, non-convertible currency, in principle (but not practice), remains ensconced within the virtual environment that it was created in (FATF, 2014).

3.2 Cyberlaundering in virtual environments explained

The core enabler of cyberlaundering in virtual worlds is the presence of secondary markets for the exchange of *non-convertible* virtual currencies (Moiseienko & Izenman, 2019). Buyers and sellers come together and exchange virtual currencies and digital artefacts according to a set of prearranged rules for trading (Acemoglu et al., 2019, p.93). It is because the cybercriminal has the ability to convert virtual currency back into fiat currency that it is possible to launder money through virtual worlds (Moiseienko & Izenman, 2019). Although secondary exchanges violate the terms of service of games, non-convertible currencies and digital artefacts are often still exchanged on secondary exchanges accompanied by a variable exchange rate to the U.S. dollar (FATF, 2014; Moiseienko & Izenman, 2019). There are no legal repercussions associated with purchasing virtual currency or artefacts from secondary exchanges as it is not a crime in itself (Norton, 2020). Thus, game companies are responsible for setting the appropriate controls in place to detect when a player has purchased virtual currency from a third-party exchange in violation of the company's terms and conditions (Norton, 2020). At worst, the account associated with purchasing or trading currency through a third-party exchange would be banned.

To provide a scale of the quantity of virtual currency in circulation, in 2021, a Blizzard senior security engineer reported that 21 *billion* gold moves through World of Warcraft daily (Icy Veins, 2021). Today, one million gold costs approximately $50 on secondary exchanges. In other words, ~ $1 050 000 million worth of WoW gold is moving through the game daily. That is for one game, in a market of hundreds. Moiseienko & Izenman (2019) list 12 currencies in their study that are easily convertible to fiat currency on secondary exchanges. Continuing with the example of WoW gold, Figure 1 illustrates a typical cyberlaundering process in World of Warcraft.

World of Warcraft has been chosen as the illustrative example for the following reasons. First, there is evidence that WoW laundering strategies have been *discussed and used* in dark web forums (Richet, 2013). Second, the risk of cyberlaundering through WoW, or a similar massively multiplayer online (MMO) game has been widely acknowledged and discussed (Alexandra, 2020; Belding, 2021; Castronova, 2005, p.234; Chambers-Jones, 2018; DaCosta & Seok, 2020; FATF, 2014; Irwin et al., 2014; Moiseienko & Izenman, 2019; Richet, 2013). Third, many of the other virtual worlds found in MMOs are to a large degree influenced by the design principles of World of Warcraft (Stevens, 2015; Thursten, 2014). In other words, although this paper uses the specificities of World of Warcraft for illustrative purposes, view the discussion as a prototypical example of cyberlaundering through MMOs more broadly.

Presupposing that the cyberlaunder already has an account on World of Warcraft, the cybercriminal uses stolen credit card details to purchase WoW gold from a secondary exchange. World of Warcraft has a once off purchase fee, and a monthly recurring subscription fee to play the game. Thus, launderers may prefer free-to-play games to avoid the initial overhead of purchasing a game and paying a monthly subscription. However, this study posits that if laundering operations are profitable enough, purchasing a game and

subscription for ~ $70 can easily be offset by the gains made from laundering. Purchasing WoW gold can be repeated across multiple credit cards to increase the amount of gold owned in the aggregate (Keene, 2011). Next, the gold is delivered in the virtual world by the broker through a virtual avatar. At this point, the cybercriminal owns WoW gold that is a digital representation of the underlying dollar value that can be obtained on the secondary exchange, or from an on-demand purchaser. Crucially, at this stage, the cybercriminal is free from the risk of being caught in the laundering process as the virtual world is completely outside the jurisdiction and surveillance of anti-money laundering agencies and controls.

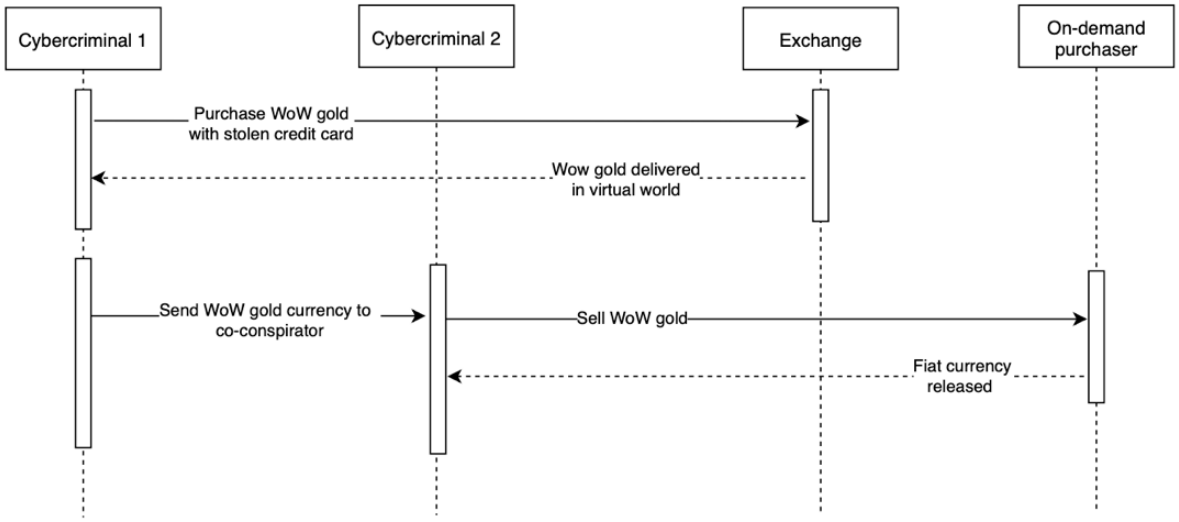

Figure 1: Cyberlaundering in virtual worlds

At worst, the launderer is found to break terms of service for receiving gold from a suspicious source, and the account is temporarily suspended or permanently banned (Norton, 2020). Next, the launderer sends the gold to a co-conspirator inside the virtual world. Two avatars in the game may exchange gold but be physically located in different countries. Finally, the co-conspirator sells the gold to an on-demand purchaser and is paid in fiat currency. Payment can be received in cryptocurrency or fiat, as to the co-conspirator's preference. For example, a 2023 forum post from an on-demand purchaser notes that the purchaser can pay for WoW gold in cryptocurrency, PayPal, as well as a host of gift card options (Sythe, 2023). Interestingly, majority of the payment methods selected have either weak or no know-your-customer policies and controls in place. As far as the audit trail of the financial transactions is concerned, all that it shows is that the co-conspirator received money for selling WoW gold on a secondary exchange — a completely legal action — with no easily identifiable connection to the ultimate source of the WoW gold. In sum, the fundamental idea behind the laundering process is that fiat money passes into the virtual world and virtual currency and is converted back into fiat currency once laundered (Chambers-Jones, 2018).

In arguably the most comprehensive study conducted on cyberlaundering in virtual worlds, Irwin et al. (2014) conducted a feasibility study to see to what extent it was technically possible to launder money through a MMO (e.g., World of Warcraft). The researchers concluded that it is technically feasible for laundering to occur in virtual worlds, with virtual worlds offering a low-risk environment, high levels of anonymity and low detection rates (Irwin et al., 2014). The authors do note that it becomes exponentially more difficult to launder large sums of money (more than ~ $200 000 at the time of publication) (Irwin et al., 2014). However, it is not so much about the scale of a once off laundering process (e.g., for purposes of tax evasion) as it is about the gains made in the aggregate across multiple ongoing iterations of the cyberlaundering process (Cloward & Abarbanel, 2020; Keene, 2011).

4. Challenges and controls

Table 1 presents the core vulnerabilities present in online video games. The vulnerabilities presented are prone to exploitation, and as a corollary, enable cyberlaundering in online video games.

Table 1: Cyberlaundering vulnerabilities present in online video games

No	Vulnerability	Description	References
VUL01	Identity management	Online video games lack robust know-your-customer policies and processes. Poor KYC controls provide a cybercriminal with easy access to anonymous online identities, enabling the launderer to move illicitly gained finances around risk free. Furthermore, by having no KYC controls in place, it is a futile exercise for game developers to implement anomaly detection or behavioral monitoring systems in virtual worlds. Detected anomalies would not be traceable back to the *real-world* identity masquerading behind the virtual avatar.	(Chambers-Jones, 2018; Irwin et al., 2014; Irwin et al., 2012; Keene, 2011; Leslie, 2014, p.90; Richet, 2013)
VUL02	Payment methods	Certain video game companies accept payment methods that either do not require KYC verification procedures or are easily circumvented by cybercriminals. For example, one popular video game company accepts pre-paid cards loaded with the game's virtual currency.	(Akartuna et al., 2022a; Chambers-Jones, 2018)
VUL03	Secondary exchanges	Secondary exchanges enable non-convertible virtual currencies to be converted back into fiat currency. Secondary exchanges are legal, and only violate a virtual world's terms of services. Inadvertently, secondary exchanges are a major enabler for cyberlaundering in virtual worlds.	(Cloward & Abarbanel, 2020; Irwin et al., 2014; Moiseienko & Izenman, 2019; Sixgill, 2019)
VUL04	Data silos	Online video game companies possess intelligence, or data that can be mined for insights into player behavior. Currently, this information is siloed with the gaming companies unavailable to law enforcement agencies.	(Akartuna et al., 2022a; Moiseienko & Izenman, 2019)
VUL05	Regulatory loopholes	Current regulation does not account for the severity of the risk posed by *non-convertible* currencies. For example, the Financial Action Task Force (FATF) explicitly state that only convertible financial currencies pose a money laundering risk.	(Chambers-Jones, 2018; FATF, 2014; Keene, 2011; Norton, 2020).

This study contends that identity management (i.e., VUL01) should be prioritized, and addressed first, if any success is to be obtained in addressing money laundering vulnerabilities present in online video games. As Irwin et al. (2012) explains:

> *"Correctly identifying and verifying a customer from the outset is vital as failure to do so results in subsequent ongoing customer due diligence activity being of little or no value."*

Managing player identities presents a particularly challenging area for online video game vendors and internet services more broadly. Specifically, the lack of effective identity management processes plaguing internet services today is one of the primary sources of cybercrime (Preukschat & Reed, 2021, p.20). There are three reasons why identity management in the context of online video games pose a particular challenge. First, it is not a linear process of simply applying technological solutions that have been implemented successfully in more mature sectors (e.g., banking and financial services) to a new and still developing context (Akartuna et al., 2022a).

Second, a significant driver behind the implementation of identity management and KYC processes in the banking and financial services sector is the presence of regulation and the threat of financial sanctions. Regulation is absent from the online video gaming domain.
Third, majority of video game vendors are dealing with a user base that are habituated to *zero* KYC and customer due diligence processes. This provides a unique challenge as to how to introduce increased control over players' identities without disrupting the seamless user and privacy experience (i.e., only requiring an e-mail account to sign up for most games) that players have grown accustomed to.

Table 2 presents recommended controls for each of the vulnerabilities identified in Table 1. Certain controls are geared towards addressing one vulnerability, whereas other controls may address more than one specific vulnerability. It is not suggested that the controls are exhaustive in addressing, or solving, each of the vulnerabilities enumerated above. Rather, this study posits that the controls suggested will add increased *friction* to the cyberlaundering process, which in turn, reduces the scale of cyberlaundering taking place.

Table 2: Controls to introduce friction into online video game laundering

No	Recommended control	Explanation of control	Vulnerabilities addressed
Control 1	Implement robust identity management processes	Identity management is a central concern in addressing cyberlaundering in virtual worlds. Robust KYC policies must be implemented where in-game purchases are made. If online video game companies do not want to burden the entire player base with KYC checks, at minimum players engaged in financial transactions must go through stringent KYC verification checks. This will allow video game companies to identify the person behind the avatar in the event of suspected or confirmed cyberlaundering.	VUL01, 02, 03
Control 2	Procure payment processors	Online video game companies must pay careful attention to which payment processors are utilized for in-game purchases. Payment processors with weaker KYC controls and processes should be avoided.	VUL02, VUL03
Control 3	Implement tighter controls around where virtual currency enters and exits the virtual world	Tighter controls should be implemented where currency enters and exits the virtual world. This is a challenging task, particularly for video games that do not have official channels for exchanging virtual currency for fiat currency. This study posits that robust KYC policies, operating in tandem with anomaly detection and behavioral monitoring systems will be able to address this vulnerability.	VUL03
Control 4	Design and implement anomaly detection systems for the monitoring of suspicious transaction patterns	Research and development must go into the design and implementation of appropriate anomaly detection systems tailored specific to each virtual world. Parameters that need to be monitored need to be accurately defined. For example, anomaly detection systems could monitor the total quantity of virtual currency in circulation, irregular spikes in the quantity of currency owned by an individual gamer, and the time an account has been opened vs total currency amassed.	VUL04
Control 5	Regulation needs to be discussed and updated in	Regulation needs to take the risk of secondary exchanges seriously. If video game companies do not have incentive to implement the controls discussed above, it may be that the appropriate	VUL05

	cooperation with private industry.	legislation and regulatory requirements may need to be set in place. KYC controls have been enforced in cryptocurrency exchanges. Virtual currencies in virtual worlds share many of the same characteristics as cryptocurrencies and may need to be governed in similar fashion.	

5. Conclusion

The gaming industry is rapidly growing, gaining increasing traction amongst younger generations. Premised on the microtransaction business model, video game companies are increasingly providing its player base with digital artefacts and virtual currencies for purchase. Naturally, secondary exchanges have emerged where gamers are able to exchange and trade digital currencies and artefacts in exchange for fiat currency. This avenue is being exploited by cyberlaunderers. Cyberlaundering in virtual worlds is the latest in a host of challenges faced by anti-money laundering agencies, legal enforcement bodies and now, the gaming industry. Cyberlaundering is not a problem that can be 'solved' in totality. Rather, with the appropriate controls put in place *friction* can be introduced into the cyberlaundering process. Critically, game development companies need to focus on user identity management processes as a starting point, by exploring how cyberlaunderers can be appropriately identified without burdening the entire player base with cumbersome KYC processes. There is a balance to be reached between a positive user experience and putting the appropriate number of controls in place. If controls are burdensome, friction is incorrectly transferred onto the innocent player base rather than the money launderer. Instead, controls need to be designed to shift the friction onto the cyberlaunder. If the cyberlaunderer experiences increased friction, laundering activities become more difficult, reducing the frequency with which cyberlaundering through virtual worlds occur.

References

Acemoglu, D., Laibson, D., & List, J. (2019). *Microeconomics, Global Edition* (2nd ed.). Pearson.

Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022a). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. *Technological Forecasting and Social Change*, *179*, 121632. https://doi.org/10.1016/j.techfore.2022.121632

Akartuna, E. A., Johnson, S. D., & Thornton, A. E. (2022b). The money laundering and terrorist financing risks of new and disruptive technologies: A futures-oriented scoping review. *Security Journal*. https://doi.org/10.1057/s41284-022-00356-z

Arkenberg, C., & Westcott, K. (2022). *Let's make a deal—In gaming! Gaming M&A is growing on the back of consolidation, portfolio plays, and game tech*. Deloitte Insights. https://www2.deloitte.com/xe/en/insights/industry/technology/technology-media-and-telecom-predictions/2023/video-game-deals-gaming-industry-mergers-and-acquisitions.html

Belding, G. (2021). *In-game currency & money laundering schemes: Fortnite, World of Warcraft & more* [Bel]. Infosec Resources. https://resources.infosecinstitute.com/topic/in-game-currency-money-laundering-schemes-fortnite-world-of-warcraft-more/

Bortner, R. M. (1996). *Cyberlaundering: Anonymous Digital Cash and Money Laundering*. http://osaka.law.miami.edu/~froomkin/seminar/papers/bortner.htm

Busby, M. (2018). Cyberlaundering: From ghost Uber rides to gibberish on Amazon. *The Guardian*. https://www.theguardian.com/technology/2018/may/17/cyberlaundering-funds-terror-internet-fake-transactions-cashless-society

Castronova, E. (2005). *Synthetic worlds: The business and culture of online games*. University of Chicago Press.

Chambers-Jones, C. (2018). Money Laundering in a Virtual World. In C. King, C. Walker, & J. Gurulé (Eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law* (pp. 165–182). Springer International Publishing. https://doi.org/10.1007/978-3-319-64498-1_8

Cloward, J. G., & Abarbanel, B. L. (2020). In-Game Currencies, Skin Gambling, and the Persistent Threat of Money Laundering in Video Games. *UNLV Gaming Law Journal*, *10*(1). https://scholars.law.unlv.edu/glj/vol10/iss1/6

Cox, J. (2017). Inside Airbnb's Russian Money-Laundering Problem. *The Daily Beast*. https://www.thedailybeast.com/inside-airbnbs-russian-money-laundering-problem

DaCosta, B., & Seok, S. (2020). Cybercrime in Online Gaming: In M. Khosrow-Pour D.B.A. (Ed.), *Encyclopedia of Criminal Activities and the Deep Web* (pp. 881–892). IGI Global. https://doi.org/10.4018/978-1-5225-9715-5.ch059

FATF. (2014). *Virtual currencies – Key Definitions and Potential AML/CFT Risks*.

Fazzini, K. (2019). *How criminals use Uber and Airbnb to launder money stolen from your credit card*. CNBC. https://www.cnbc.com/2019/02/07/how-criminals-use-airbnb-uber-launder-stolen-credit-card-money.html

Filipkowski, W. (2008). *Cyber Laundering: An Analysis of Typology and Techniques*. *3*(1).

FinCEN. (2023a). *USA PATRIOT Act*. https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

FinCEN. (2023b). *What is money laundering?* https://www.fincen.gov/what-money-laundering

Gilmour, P. M. (2023). Reexamining the anti-money-laundering framework: A legal critique and new approach to combating money laundering. *Journal of Financial Crime*, *30*(1), 35–47. https://doi.org/10.1108/JFC-02-2022-0041

Grayson, N. (2022). Turkish police detain 40 people over Twitch streamer money laundering scheme. *Washington Post*. https://www.washingtonpost.com/video-games/2022/01/11/twitch-bit-money-laundering-turkey-police/

Holm, J., & Mäkinen, E. (2018). The Value of Currency in World of Warcraft. *Journal of Internet Social Networking and Virtual Communities*, *2018*, 1–13. https://doi.org/10.5171/2018.672253

Icy Veins. (2021). *21 Billion Gold Moves Through WoW Each Day*. Icy Veins. https://www.icy-veins.com/forums/topic/56045-21-billion-gold-moves-through-wow-each-day/

Irwin, A. S. M., Slay, J., Raymond Choo, K., & Liu, L. (2012). Are the financial transactions conducted inside virtual environments truly anonymous?: An experimental research from an Australian perspective. *Journal of Money Laundering Control*, *16*(1), 6–40. https://doi.org/10.1108/13685201311286832

Irwin, A., Slay, J., Raymond Choo, K.-K., & Lui, L. (2014). Money laundering and terrorism financing in virtual environments: A feasibility study. *Journal of Money Laundering Control*, *17*(1), 50–75. https://doi.org/10.1108/JMLC-06-2013-0019

Keene, S. D. (2011). Emerging threats: Financial crime in the virtual world. *Journal of Money Laundering Control*, *15*(1), 25–37. https://doi.org/10.1108/13685201211194718

King, S. T., Scaife, N., Traynor, P., Abi Din, Z., Peeters, C., & Venugopala, H. (2021). Credit Card Fraud Is a Computer Security Problem. *IEEE Security & Privacy*, *19*(2), 65–69. https://doi.org/10.1109/MSEC.2021.3050247

Leslie, D. A. (2014). *Legal Principles for Combatting Cyberlaundering* (Vol. 19). Springer International Publishing. https://doi.org/10.1007/978-3-319-06416-1

Matteo, C. (2022). Cybercrimes and Virtual Worlds: A Systematic Literature Review. *Journal of Information Security and Cybercrimes Research*, *5*(2), 124–134. https://doi.org/10.26735/CBBQ4731

Moiseienko, A., & Izenman, K. (2019). *Gaming the System: Money Laundering Through Online Games*. *39*(9).

Morris-Cotterill, N. (2001). Money Laundering. *Foreign Policy*, *124*, 16. https://doi.org/10.2307/3183186

Norton, A. (2020). *Gaming the System: Money Laundering through Microtransactions and In-Game Currencies*. https://sites.psu.edu/jlia/gaming-the-system-money-laundering-through-microtransactions-and-in-game-currencies/

Preukschat, A., & Reed, D. (2021). *Self-Sovereign Identity*. Manning Publications Co.

PwC. (2022). *Global Entertainment & Media Outlook 2022–2026 Perspectives Report*. PwC. https://www.pwc.com/gx/en/industries/tmt/media/outlook/outlook-perspectives.html

Richet, J.-L. (2013). *Laundering Money Online: A review of cybercriminals methods* (arXiv:1310.2368). arXiv. http://arxiv.org/abs/1310.2368

Ruffio, P. (2022,). *Dark Web Price Index 2022—Dark Web Prices of Personal Data*. https://www.privacyaffairs.com/dark-web-price-index-2022/

Sixgill. (2019). *Carding and the Digital Gaming Industry*.

Solon, O. (2013). Cybercriminals launder money using in-game currencies. *Wired UK*. https://www.wired.co.uk/article/money-laundering-online

Stanton, R. (2022). *Turkish police arrest 40 in Twitch money laundering scandal*. https://www.pcgamer.com/turkish-police-arrest-40-in-twitch-money-laundering-scandal/

Statista. (2023). *Gaming monetization*. Statista. https://www.statista.com/topics/3436/gaming-monetization/

Stevens, T. (2015). Security and Surveillance in Virtual Worlds: Who Is Watching the Warlocks and Why? *International Political Sociology*, *9*(3), 230–247. https://doi.org/10.1111/ips.12094

Stuart, K. (2023, March 1). Hot buttons: Why fashion houses are getting into video games. *The Guardian*. https://www.theguardian.com/games/2023/mar/01/why-fashion-houses-are-getting-into-video-games

Sythe. (2023). *Buying WoW Classic GOLD All Servers*. Sythe. https://www.sythe.org/threads/buying-wow-classic-gold-all-servers-instantpayment-paypal-skrill-wmz-more.3791157/

Teicher, R. (2018, March 18). *How Uber ghost rides are linked to online money laundering*. TNW | Contributors. https://thenextweb.com/news/uber-ghost-rides-linked-online-money-laundering

Thursten, C. (2014). Five ways World of Warcraft changed MMOs forever. *PC Gamer*. https://www.pcgamer.com/five-ways-world-of-warcraft-changed-mmos-forever/

Westcott, K., Arbanas, J., Arkenberg, C., Auxier, B., Loucks, J., & Downs, K. (2022). *2022 Digital media trends, 16th edition: Toward the metaverse*. Deloitte Insights. https://www2.deloitte.com/us/en/insights/industry/technology/digital-media-trends-consumption-habits-survey/summary.html