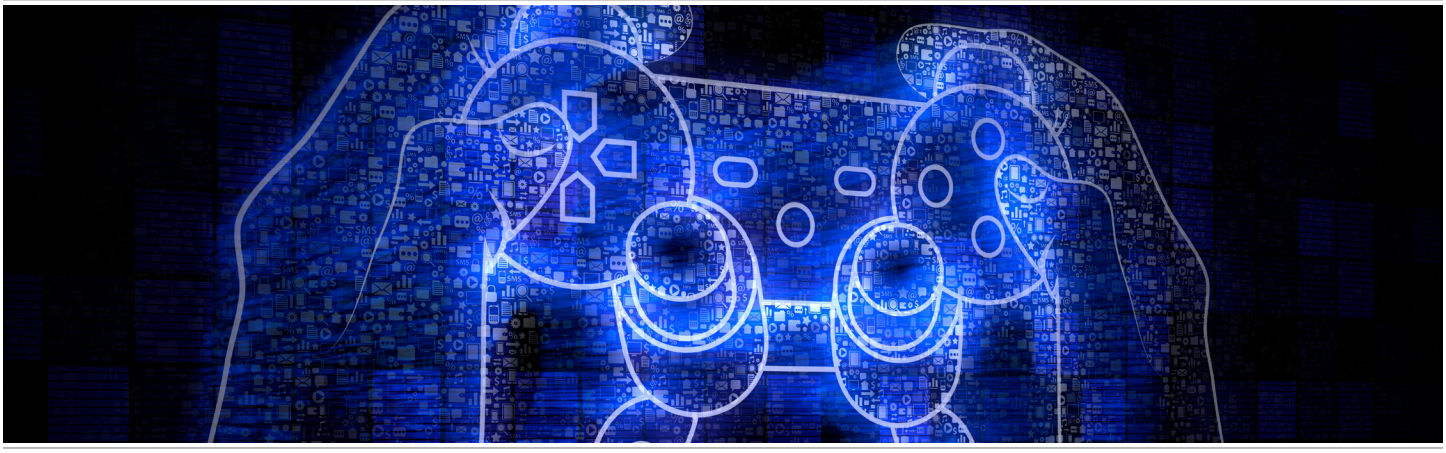
SheppardMullin



CFPB Report Targets Games and Virtual Worlds - What Blockchain Game and Metaverse Companies Need to Know[1]

By: James Gatto, Yasamin Parsarar & Maxwell Earp-Thomas

The Consumer Financial Protection Bureau ("CFPB") published a report on *Banking in Video Games and Virtual Worlds* ("Report") that warns of greater scrutiny of and enforcements against the financial services offered in games and virtual worlds that increasingly resemble traditional financial products and services offered by regulated banking and payment systems. The Report is applicable to all types of games and virtual worlds, but creators and publishers of blockchain games and metaverses, in particular, should take note of this report.

As detailed below, portions of the Report specifically address crypto-assets, convertible virtual currencies, non-fungible tokens ("NFTs"), crypto-asset trading platforms, and lending associated with crypto-assets, including metaverse land. The Report highlights concerns with the "porous" nature of these crypto-assets and the ease with which they can be traded person-to-person ("P2P") and converted to cash, in contrast with traditional "closed-loop" game economies. Additionally, some business models prevalent in blockchain games are likely within the crosshairs of the CFPB's scrutiny. As addressed below, this may include certain models relating to play to earn, "lending" of game-related assets, staking, game guilds and more.

The Report stems from the growing number of consumer (gamer) complaints of reportedly being harmed by scams, theft and other losses, yet not receiving the recourse or protections they would expect under federal consumer protection laws. The Report advises that the CFPB will be monitoring video games/blockchain games and virtual worlds/metaverses where financial products and services are offered to ensure compliance with federal consumer financial protection laws. The Report also focuses on risks associated with the alleged targeting of children and risks of addiction,[2] and highlights the increasing types and amount of "surveillance" data game companies are collecting and allegedly using to exploit some players' addictive proclivities to spend or selling to other companies for purposes outside of game play.

[1] This article is based on a prior publication entitled *Report Signals CFPB Taking Aim at Video Game and Virtual Worlds Industries*, by Moorari Shah, James G. Gatto, A.J. S. Dhaliwal, Mehul N. Madia of Sheppard, Mullin, Richter & Hampton LLP.

[2] A growing number of lawsuits have been filed in the U.S. against game companies alleging that some data collection and game monetization mechanics lead to addiction by gamers, particularly minors. Similar lawsuits have been filed against social media companies.

As detailed below, some examples of financial services on which the CFPB is focused include:

- platform-supported secondary markets that store and transfer valuable assets such as proprietary payment processing systems and money transmitter services;
- payment systems associated with play to earn or user generated content models;
- gaming platforms that facilitate P2P transfer of game assets;
- wallets that can serve as a central hub for anything related to a player: gaming credentials, in-game currency balances and transactions and spending history; and
- lending of and borrowing against game assets by "staking" or holding assets in escrow and providing players with loans.

Key takeaway: Game companies should: i) develop an understanding of the scope of relevant legal issues on which the CFPB and other consumer protection regulators are focused; and ii) undergo an assessment of their business practices, terms of service, data collection and usage, privacy policies and player relations policies to minimize the likelihood or impact of becoming a target of the CFPB and other regulators that are stepping up efforts to police the growing consumer-focused issues around the business models discussed herein.

Report's Key Findings

- Games and game marketplaces and their associated infrastructure increasingly resemble traditional financial products and services. According to the Report, companies leverage players' game assets, which include in-game currencies and virtual items, such as skins or cosmetic items, and crypto-assets, which can be transacted via in-game and external marketplaces, through P2P transfers or buying and selling in-game goods and services, by providing services in the form of payment processing, money transmission, and even loans. Some games also allow consumers to convert game assets back to fiat currency.
- As game assets represent greater amounts of value and their use becomes increasingly similar to that of money, there have also been increased reports of users losing access to game assets through hacking attempts, account theft, scams, and unauthorized transactions. Yet, some operators of game and virtual worlds do not appear to provide the kinds of consumer protections and data security protections that apply to traditional banking and payment systems.
- Game companies are collecting large amounts of data on players, and tracking purchasing history, spending thresholds, and location data. Game companies have also become adept at monetizing behavioral, personal and biometric data. According to the CFPB, there is a risk that gamers may be harmed when their data is sold, bought, and traded between companies, including for purposes outside of game play.

The Market Participants

Market participants at the center of this Report include the companies that publish games (including both traditional video games and blockchain games), virtual world/metaverse platforms and marketplaces which permit buying and selling of currencies and game assets.

How Evolutions in the Business Models of Games Has Led to CFPB Scrutiny

The business models of games have evolved significantly in recent times. Traditionally, game publishers operated a closed-loop economy, where gamers could spend fiat currency to purchase virtual currency which could be used to buy virtual items for in-game use only, with no way to cash out any of those items via the game publisher. Under this model, game companies typically operate an inventory management system to manage the players' inventory of game assets and license those assets only for use in the game for entertainment value, not player profit. Most video games still do not permit any cash out. However, a number of unauthorized marketplaces have arisen, where players can buy, sell and trade virtual currencies, virtual items, and even entire game accounts. Additionally, traditional video game models have evolved to include so-called creator economies, where players can create and sell game assets. Some of these creator economies enable users to earn real money from these creations.

As the Report suggests, from a financial regulatory perspective, these innovations implicate the potential application of money transmission and electronic funds transfer laws. Separately, any perceived weaknesses in a platform's ability to address customer complaints fairly and timely inevitably raise the specter of regulatory claims alleging unfair, deceptive, and abusive acts and practices ("UDAAPs").

A more significant evolution of business models has resulted from blockchain games and metaverses. Blockchain games and metaverses are often premised on play-to-earn business models. With blockchain games, the game assets are typically tokenized and represented as cryptocurrencies or NFTs. With blockchain games, the game economy is typically decentralized, crypto assets are owned and controlled by the players and can be freely bought, sold and traded via P2P wallet transfers or via crypto marketplaces. And the terms of service typically do not prohibit these activities. Additionally, blockchain games' play to earn business model has led to other types of "financial" transactions, including staking, mining, and lending of the game-based crypto assets. For example, players can earn passive income by lending their in-game items to other players for a fee. In some games, players form guilds to collaborate on game play, where players can earn a profit by using the guild's game assets to play the game.

Metaverses are a web3 version of virtual worlds. With metaverses, game assets are also typically tokenized, and the business model includes a creator economy. In metaverses, players buy tokens representing ownership of virtual land and build things or provide services on land to earn money. Some players invest significant upfront capital to do this. Some obtain loans to purchase or build on the land.

This evolution of business models employed in games and virtual worlds has led the CFPB to view elements of these models as being akin to traditional banking and payment services, including lending. To the extent that such purchases of virtual land or other assets are financed, consumer lending protections may apply. Such laws could subject the lender to disclosure requirements under the Truth in Lending Act ("TILA")[3] With respect to players lending out in-game items to earn passive income, the Bureau and other regulators may view these transactions as extensions of credit, which could subject the "lender" or blockchain game companies to disclosure requirements and liability from consumer lending laws.

[3] TILA, and its implementing regulation, Regulation Z, set forth disclosure, advertising, and other requirements and limitations applicable to creditors engaging in various consumer credit transactions.

Furthermore, blockchain game companies may be exposed to liability in connection with state and federal agencies' expansive authority to enforce against UDAAPs.[4] The CFPB in particular construes its UDAAP authority broadly and has shown a willingness to enforce aggressively wherever it recognizes unfairness, deception or abuse toward consumers, including in industries not traditionally governed by consumer protection laws.

Moreover, according to the CFPB and banking regulators, supervised companies have an obligation to oversee any third-party "service providers" to mitigate the potential for consumer harm in connection with the services provided.[5] Certain staking validators, game guilds/members, lenders of in-game assets among other parties participating in blockchain ecosystems, may be deemed "service providers." If so, the relevant entities may be responsible for oversight. This may entail the implementation of due diligence protocols and systems to monitor the conduct of these actors to mitigate consumer harm.

In accordance with gaming companies' obligation to oversee third party service providers, blockchain game companies would be wise to examine how players affiliation with a game guild could lead to consumer injury. After guild members complete in-game objectives to earn rewards, many game guilds distribute the winnings per predetermined distribution ratios. For example, 25% of winnings is distributed to guild members for their efforts and 75% is reinvested in the guild for in-game upgrades to increase the odds of success in future missions. To the extent this model leaves guild members vulnerable to financial exploitation, companies could face liability for a lack of proper service provider oversight or failure to adequately advise consumers of the risks inherent to game guild participation.

One of the things the Report does not squarely address is that blockchain technology is designed to be decentralized, secure and immutable. These characteristics may present complications should there be a court judgment against assets held in a player's digital wallet and secured by the blockchain. Unlike traditional games, in-game transactions in blockchain games are confirmed by a network of validators rather than a centralized server controlled by a game publisher. This means that, should a court order seizure of any on-chain assets, blockchain game companies may be unable to help effect compliance with the judgment. In such scenarios, a blockchain game company's role and potential for liability remain unclear.

Additionally, if a player loses the keys to their crypto wallet and thus access to their NFTs or other games assets, there may be no recourse. But that may not be the game companies' fault. The Report does not really address the differences between player-controlled wallets that result in loss versus loss related to an issue with an in-game inventory management system under a publisher's control.

What Happens Next?

Through this Report, the CFPB continues to signal its commitment to monitoring non-traditional markets and identifying where financial products and services may be offered (regardless of infrastructure), to ensure compliance with federal consumer financial protection laws. The CFPB has not set a timetable for its next moves, or specified

[4] The Dodd-Frank Act authorizes the CFPB to prescribe and enforce rules to prevent covered persons (defined to include persons extending and servicing consumer credit) and service providers from committing or engaging in UDAAPs, in connection with any transaction for a consumer financial product or service. States also enforce UDAAP prohibitions some of which provide private rights of action, granting individual consumers standing to sue.

[5] Agency guidance on service provider relationships may be found at the following: CFPB Compliance Bulletin and Policy Guidance; 2016-02, Service Providers (October 31, 2016), *available at* Compliance Bulletin and Policy Guidance; 2016-02, Service Providers; Interagency Guidance on Third-Party Relationships: Risk Management, 88 FR 37920-01 (2023), *available at* Federal Register: Interagency Guidance on Third-Party Relationships: Risk Management.

what those moves will be. Based on prior CPFB activity, the agency may issue market monitoring orders to certain market participants as they did previously to large technology companies, "buy now, pay later" or BNPL providers, and large auto lenders (see our previous blogs posts on these orders here, here and here). In addition, the Bureau has not been shy about using its risk-based supervision authority to take a closer look at non-bank institutions that offer products that may pose a "risk to consumers" (see our previous blog post regarding the CFPB's first public decision designating a non-bank lender for supervision based on the institution's potential risk to consumers here).

What Blockchain Game/Metaverse Companies Should Do Now

Blockchain game/metaverse companies should carefully review the Report and analyze their current practices to identify any actions that they can take now to minimize the risk that they run afoul of any issues on which the Report focuses. This may include:

- Assessing the potential for harm to gamers, including financial losses due to theft and scams as a result of buying, selling, and trading of game assets, including analyzing trends in federal and state UDAAP enforcement and assessing their applicability;
- Reviewing what you can do to mitigate these harms (to the extent within your control) and assessing your policy for navigating these issues if such harms occur;
- Disclosing risks that may be under control of the players, indicating players' responsibilities related to such risks, and potentially providing information on best practices to avoid such risks;
- Reviewing your data collection and use policies and privacy policies and disclosures, with particular attention to the handling of data procured from minors;
- Consulting an attorney to assess whether your products and services are subject to various consumer financial services laws such as the Electronic Funds Transfer Act, the Bank Secrecy Act and anti-money laundering restrictions, state money transmission requirements, bit licenses, and TILA,[6] and taking steps to ensure compliance with any applicable laws, which may include reviewing and revising your Terms of Service;
- Establishing systems for effectively recording, monitoring, and responding to gamer complaints; and
- Examining the possibility that participants in blockchain game ecosystems are "service providers," and exploring supervision mechanisms based on agency guidance.[7]

The CFPB Report indicates that blockchain and other games will likely face a heightened level of regulatory scrutiny. Now is the time for companies to review their operations and consider strategies to minimize the likelihood and impact of any potential regulatory enforcement.

Sheppard Mullin is uniquely positioned to help on these issues. We have a well recognized Blockchain and Fintech team and a Games team which help clients develop innovative and comprehensive legal strategies to navigate the evolving blockchain and fintech regulatory landscape. Our team is comprised of attorneys with diverse legal backgrounds who collectively understand the wide array of legal issues surrounding blockchain and fintech, and who possess extensive experience advising clients on matters involving blockchain games and digital assets.

---

[6] For example, in connection with "lending" of in-game items or other in-game transactions might trigger disclosure requirements under consumer lending laws such as TILA.

[7] Liability may not be limited to consumer protection laws. In addition to analyzing their practices under consumer protection laws, blockchain game companies should assess the applicability of securities laws as well as tax implications of in-game asset and transactions.

For more information, please contact:

James Gatto
Artificial Intelligence Team Co-Leader
Blockchain and Fintech Team Co-Leader
+1 (202) 747-1945
jgatto@sheppardmullin.com

Jim Gatto is a partner in the Intellectual Property Practice Group in the firm's Washington, D.C. office. He is Co-Leader of the Artificial Intelligence Team, the Blockchain & Fintech Team, and Leader of the Open Source Team.

Yasamin Parsafar
Blockchain and Fintech Team Co-Leader
+1 (415) 774.2927
yparsafar@sheppardmullin.com

Yasamin Parsafar is a partner in the Intellectual Property Practice Group in the firm's San Francisco office and is Co-Leader of the firm's Blockchain & Fintech team.

Maxwell Earp-Thomas
Associate
+1 (714) 424-2880
mearp-thomas@sheppardmullin.com

Maxwell Earp-Thomas is an associate in the Finance & Bankruptcy Practice Group in the firm's Orange County office.

This alert is provided for information purposes only and does not constitute legal advice and is not intended to form an attorney client relationship. Please contact your Sheppard Mullin attorney contact for additional information.