Consumer Advisory: Video games are targeting your children to get into your wallet

By Consumer Financial Protection Bureau – AUG 28, 2024

As summer comes to a close, we can assume many children and young adults spent a large part of their break playing video games. It's estimated that 45.7 million children in the U.S. play video games, or more than 80 percent of all children between the ages of 5 and 18, according to recent data (https://www.theesa.com/wp-content/uploads/2024/05/Essential-Facts-2024-FINAL.pdf). Video games and virtual worlds may seem harmless, but recent public reports have underlined the harms incurred through the industry's use of design tricks, technology, and surveillance data to entice players into spending money. As the CFPB highlighted earlier this year, many video games and virtual worlds increasingly resemble traditional banking and payment systems that facilitate the storage and exchange of billions of dollars in assets, including virtual currencies. Gamers—or their parents and guardians—frequently report being harmed by scams or theft on gaming platforms. Players report having little recourse with gaming companies when they suffer losses, and game publishers claim to have no obligation to compensate the players for financial losses, including when service to a game is suspended or a consumer's account is closed.

Over the summer, did you or your child lose money playing a video game? Were you able to dispute those transactions? Were their gaming accounts hacked or assets stolen? Did your family get a straight answer from the company about what happened and how to get help? Gaming companies frequently use underhanded tactics to encourage spending, which can lead to unexpected charges on your debit card, credit card, or mobile payment service. Since the release of our report in April 2024 (cfpb.gov/data-research/research-reports/issue-spotlight-video-games/), the CFPB has continued monitoring developments in these markets, the companies involved, and the risks to players and their families.

In-game currencies hide costs

Many games require a form of payment to be stored on the gaming account to readily convert dollars to in-game currency. Video game companies can use those in-game currencies to conceal the real costs of transactions in game. For example, they use confusing and inconsistent exchange rates (pay $2.95 for 320 coins or pay $9.05 for 1020 coins) that make the mental math from one currency to the other difficult. Players are

typically prompted to purchase game currency outside of game play, separating those purchasing decisions from the players' actual spending decisions during the game which can ultimately drive costs.

Gambling-like design tricks conceal odds and encourage spending

Games are often designed to capture a player's attention and then deliver constant and immediate rewards to encourage a player to keep playing. Collecting virtual items, like "skins" or "loot," is a key aspect of that reward system. These items are often considered rare, immensely valuable, and collecting them is reinforced by other players.

Many games use gambling-like design tricks to hide the odds and encourage compulsive spending. This can include activities like skin betting or token wagering—activities that allow players to bet with valuable gaming assets. Another gambling-like tactic used by gaming companies involves loot boxes, which are surprise packages available for purchase. Loot boxes are marketed as random-chance and can contain extremely rare or valuable items missing from a player's collection, but often, design tricks in the game are used to suggest a player narrowly missed out on the item they are searching for to encourage them to buy more loot boxes.

These design tricks can lead to increased spending, especially when a game is connected to a mobile payment service or credit or debit card. Parents have reported an overwhelming amount of unexpected gaming transactions on their credit or debit card statements in consumer complaints to the Federal Trade Commission and Consumer Financial Protection Bureau.

What you can do

Consider a gift card or other option to block surprise overcharging: Many of these platforms require a debit card, credit card, gift card, or other payment method to be stored on the account to readily convert dollars to gaming currencies. You can refrain from storing your debit or credit card information on your child's gaming account; if a game requires card information to create an account, a gift card, with a finite amount of dollars available for your child to convert to gaming currency, can be an alternative.

Look for parental controls on payments: Some games support parental controls or specialized accounts for children that require a password prior to transactions. Banking alerts can help flag repeated payments to gaming platforms. You can also check to see if your bank will allow you to block payments to certain gaming vendors.

Consider games without in-game purchases: When choosing which games to play, there are options that don't have microtransactions. Consider games that are playable with a one-time purchase, or where add-ons have a clear and consistent value.

Limit data collection and sharing on your child's account: Game publishers typically monitor player behavior, such as purchasing history and spending thresholds. Gaming technology has been found to collect and monitor a child's physical location and social media activity. Virtual or mixed-reality headsets can collect biometric data, such as iris scans, eye movements, pupil response, gestures, voice, and facial expressions as well as scanning the size of the room a player is in and if any other people are in range. Viewed together, such collected data can be used to generate an accurate portrait of a player's offline identity, including their daily routines, home address, who they connect with while playing, and sensitive health conditions. This can be used to change in-game prices of items, ads displayed, playing conditions, and even the odds of winning rare items. Several games allow you to opt-out of third-party sharing and personalized content, including price updates on an individualized level. Consider opting-out of these data sharing and collection policies when possible.

Submit a complaint: You can submit a complaint about a problem with a financial product or service in video gaming at consumerfinance.gov/complaint (cfpb.gov/complaint/) or by calling (855) 411-CFPB (2372). While most complaints receive a response from the company, many complaints about video games do not. We've been working with companies to improve that. Whether a company responds to you or not, your complaint makes an impact by helping us, other agencies, and law enforcement find bad business practices and spot problems and patterns.

The CFPB will continue to monitor gaming markets, their similarities to traditional banking and payment systems, and the risks to players and their families. For more information, read our report *Banking in video games and virtual worlds*. (cfpb.gov/data-research/research-reports/issue-spotlight-video-games/)

PRESS INFORMATION

If you want to republish the article or have questions about the content, please contact the press office.

Go to press resources page (cfpb.gov/about-us/newsroom/press-resources/)

An official website of the United States government