HUDSON COOK

Mo Data, Mo Problems: Data Protection and Privacy Concerns for the Gaming Industry

July 10, 2024 | Julia K. Whitelock, Justin B. Hosie and Jason Esteves

The Consumer Financial Protection Bureau's (CFPB) eyes are on the gaming industry and the potential harm consumers may suffer from data security and privacy concerns. In our prior articles, we provided an overview of regulatory risk for the gaming industry and discussed the CFPB's concerns about payment transmission issues and advertising and exploitation. Gaming companies collect significant amounts of financial and personal data from the consumers playing their games. Applications and devices may collect users' banking information and track users' location, interaction with games, devices, and other applications (e.g., integrated social media), and biometric data (e.g., eye posture, voice, heart rate). Third-party systems that assist with payment processing in-app purchases may also collect users' banking information and personally identifiable information. In this article we focus on the CFPB's data protection and privacy concerns.

Data Protection

The CFPB highlighted data protection because it claims that "operators of gaming and virtual worlds do not appear to provide the kinds of customer protections that apply to traditional banking and payment systems." This is likely true where gaming companies have not thought of themselves or been treated as financial institutions.

The CFPB previously issued guidance that an entity's insufficient data protection or information security violates the Consumer Financial Protection Act's prohibition on unfair acts or practices. Other federal laws (e.g., FTC's Safeguards Rule) and state laws (e.g., NY SHIELD Act) may impose additional data protection and reporting requirements on gaming companies. Information security weaknesses or failures can result in data breaches, account theft, scams, and unauthorized transactions that may harm millions of consumers. Insufficient protections that may rise to the level of unfair acts or practices include failing to promptly patch a known software vulnerability or lacking procedures to prohibit a person from paying for services using a credit card account that is not her own. In addition to federal and state enforcement actions, there have been many class action lawsuits brought by consumers affected by data breaches.

Companies may strengthen their data protection through:

- data encryption,

- routine and timely software updates,
- multi-factor authentication, and
- adequate password management policies.

The CFPB likely expects operators of gaming and virtual worlds to implement compliance management systems that comply with consumer protection laws, including those applicable to data protection.

Privacy

While Congress is discussing a draft U.S. comprehensive privacy bill, companies must currently navigate a fragmented patchwork of sectoral-based and state-specific privacy laws. The CFPB questioned whether gaming companies were adhering to proper privacy regulations and whether consumers were fully aware of what information was being collected and how it was being used. The CFPB estimated that approximately 58% of online game users are under the age of 16, which makes them more vulnerable to certain tactics. As a result, privacy policy disclosures may not be effective.

Federal and state regulators have taken action against gaming companies for privacy violations. In 2022, the Federal Trade Commission and Epic Games entered into a consent order to resolve claimed violations of the Children's Online Privacy Protection Act (COPPA). Epic agreed to a $275 million civil penalty and injunctions related to default privacy settings for children and teens and a mandatory privacy program to address allegations that Epic failed to notify or obtain consent from parents regarding Epic's collection and use of such information and failed to delete such information at the request of parents. Last month, California announced a settlement with the makers of the SpongeBob game app for alleged violations of the California Consumer Privacy Act and COPPA. The company agreed to a $500,000 civil penalty and injunctive terms related to the collection, sale, and sharing of personal information of consumers less than 13 years old without parental consent and properly implementing and maintaining third-party software development kits for the same. Consumer users have also sued gaming companies based on similar theories of liability but characterized as violations of state consumer protection statutes. And some states' privacy laws provide for a private right of action.

Companies may reduce the risk of regulatory enforcement and private litigation arising related to data collection and use by:

- reviewing and updating online privacy notices,
- ensuring privacy notices are conspicuous and the user has given unambiguous assent,
- investing in inventory and audit tracking technologies,
- implementing appropriate privacy controls to benefit end users, and

- routinely assessing privacy risk.

As with data protection, the CFPB likely expects operators of gaming and virtual worlds to implement compliance management systems that comply with privacy laws.

So now you know a little more about what the CFPB (and other regulators and consumers) want from the gaming industry. But it's true—the more data you come across, the more problems you see.

The crystal ball is hazy.

It's hard to predict what exactly will come out of the CFPB's report. But suffice it to say that it foreshadows future CFPB activity and heightens the attention of regulators and plaintiffs' lawyers to these issues. This page will be updated with links as the subsequent articles in this series are published.

- "OVER THE LINE!" Where Banking and Gaming Intersect, the CFPB Has Something to Say
- Feeding the Loot Box Monster: The CFPB's Concerns with Payment Transmission in Gaming
- "That's Unfair!" Navigating CFPB Scrutiny and Consumer Protection Challenges in the Gaming Industry

HUDSON
COOK

Hudson Cook, LLP is a national law firm representing the financial services industry in compliance, privacy, litigation, regulatory and enforcement matters.

7037 Ridge Road, Suite 300, Hanover, Maryland 21076
410.684.3200

hudsoncook.com