IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

MICHAEL HEIDBREDER Plaintiff, vs EPIC GAMES, INC., Defendant.	)))))))))	Case No.: **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

TABLE OF CONTENTS

For his Class Action Complaint, Plaintiff Michael Heidbreder ("Plaintiff"), on behalf of himself and all others similarly situated, alleges the following against Defendant Epic Games, Inc. ("Defendant" or "Epic Games"), based on personal knowledge as to Plaintiff and Plaintiff's own acts, and on information and belief as to all other matters based upon, *inter alia*, the investigation conducted by and through Plaintiff's undersigned counsel:

SUMMARY OF CASE

1. This case involves a data breach Epic Games announced on January 16, 2019, wherein the personal information of 200 million Fortnite users was exposed due to a flaw in Fortnite's code that allowed hackers and other nefarious users to take over player accounts and exploit their personal information for unsavory and illegal purposes ("Data Breach").

2. Epic Games developed and operates Fortnite, a popular battle-royale style video game played by approximately 80 million people per month and with approximately 200 million registered users across computer, console, and mobile platforms.

3. As part of the sign-up process and as a consequence of playing Fortnite, users create, maintain, and update accounts containing personal information, including their names, email addresses, and credit or debit card information, referred to herein as "PII" (personally identifiable information).

4. On January 16, 2019, Epic Games publicly acknowledged that Fortnite users' PII was subject to a security breach, but did not disclose a timeframe for the Data Breach or how many accounts were impacted. Epic Games has not yet directly informed or notified individual Fortnite users that their PII may be compromised as a result of the breach. Epic Games' acknowledgement only came after Check Point Software Technologies Ltd. ("Check Point"), a cybersecurity firm, discovered vulnerabilities in Fortnite's web infrastructure and disclosed their findings to Epic Games in November of 2018.

5. Fortnite's vulnerabilities stemmed from its single sign-on ("SSO") setup, a mechanism that allows users to log into multiple services with the same third-party account such

as Epic Games, Xbox, or Google. Once logged into a third-party account, users could log in and access their Fortnite account by requesting the third-party account send an access token[1] to Fortnite.

6. Hackers exploited the SSO by distributing phishing links over social media messages or forum posts claiming, *inter alia*, to be about a Fortnite promotion. When users opened the link, they were asked to log in to their Fortnite account via the SSO. But instead of having the third-party account send the security token to the legitimate login, hackers redirected those users to an old, unsecured URL maintained by Epic Games. Check Point's research revealed that hackers could embed that URL with malicious JavaScript allowing them to steal Fortnite access tokens which they could then use to take over users' accounts.

7. As a result of Defendant's failure to maintain adequate security measures and notify users of the security breach in a timely manner, Plaintiff and certain Fortnite users' PII was compromised. They have suffered an ascertainable loss in that the credit or debit card information linked to their Fortnite accounts was stolen as a result of Defendant's failures. Hackers used this information to purchase in-game Fortnite currency without the permission of the account holders, including Plaintiff. Hackers also used this information to steal player accounts. Some of these stolen accounts, once loaded up with in-game currency purchased fraudulently, were sold on third-party websites. The sale of Fortnite accounts on the dark web has increased recently,[2] with accounts selling for an average of approximately $11.29.[3] Furthermore, Plaintiff and the other impacted Fortnite users must undertake additional security measures, some at their own expense, to minimize the risk of

---

[1] Access tokens are the equivalent of digital keys that allow users logged into third-party accounts to use those accounts as a verification to log in to their Fortnite accounts.

[2] Antony Cuthbertson, Fortnite, Netflix and Uber Accounts Being Sold For Just £8 on the Dark Web (Feb. 19, 2019), *available at* https://www.independent.co.uk/life-style/gadgets-and-tech/news/fortnite-account-sale-dark-web-price-index-netflix-uber-cyber-crime-a8786686.html (last visited August 8, 2019).

[3] Simon Migliano, Dark Web Market Price Index (February 2019 - UK Edition), *available at* https://www.top10vpn.com/privacy-central/privacy/dark-web-market-price-index-2019-uk-edition/#indextop (last visited August 8, 2019).

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.