IN THE UNITED STATES DISTRICT COURT
FOR DISTRICT OF MARYLAND
SOUTHERN DIVISION

HADONA DIEP
18013 Foxworth Court
Gaithersburg, MD 20874

Individually, and on behalf of similarly-situated persons, as Plaintiff,

v.

APPLE, INC.,
One Apple Park Way
Cupertino, CA 95014

Defendant.

Case No. 21-2359

CLASS ACTION COMPLAINT

Plaintiff Hadona Diep, by and through undersigned counsel, and on her own behalf and on behalf of those similarly situation, for her Class Action Complaint against Apple, Inc., seeking damages, hereby alleges as follows:

NATURE OF THE CASE

1. This action is a class-action suit for damages under the federal and state laws of the United States, seeking legal remedy for the Defendant's breaches of those same laws, in participating in and or allowing "hacking" and "breach" of financial account information and actual theft of personal financial assets, by authorizing a malicious application in the "App Store" and maintaining the same, despite knowledge of the criminal activity, and the Defendant's further failures to notify Plaintiff and the Class Members that their financial information had been compromised.

PARTIES

2. Plaintiff Hadona Diep is a resident of the State of Maryland.

3. Defendant Apple, Inc. is a corporation of the State of California.

JURISDICTION AND VENUE

4. Jurisdiction is proper in the Court as the Plaintiff brings Federal causes of action pursuant to 18 U.S.C. § 1030(g) and 47 U.S.C. § 230(e)(4). This Court has supplemental jurisdiction over the State law claims pursuant to 28 U.S.C. § 1367.

5. Jurisdiction is further proper under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because, on information and belief, the proposed Class(es) consists of 100 or more members; the amount in controversy exceeds $5,000,000, exclusive of costs and interest; and minimal diversity exists.

6. This Court may exercise personal jurisdiction over the Defendant, who has availed itself of the jurisdiction of this Court through acts and omissions, including but not limited to, advertising its services in this District, selling products and services to consumers in this District, and by otherwise conducting business in this District.

7. Venue is proper in this forum pursuant to 28 U.S.C. § 1391(b), as the Plaintiff resides in this judicial district and/or a substantial part of the acts or omissions giving rise to the claims herein occurred in the same.

GENERAL ALLEGATIONS

8. Plaintiff uses a computer in interstate commerce.

9. Plaintiff makes her living as a full-time cyber-security IT professional.

10. Apple, Inc. ("Apple") is the largest, or at least one of the largest, mobile and tablet application providers in the world, through its universally-known "App Store."

11. Apple itself describes the App Store to consumers as, for over a decade, having

> proved to be a safe and trusted place to discover and download apps. But the App Store is more than just a storefront — it's an innovative destination focused on bringing you amazing experiences. And a big part of those experiences is ensuring that the apps we offer are held to the highest standards for privacy, security, and content. Because we offer nearly two million apps — and we want you to feel good about using every single one of them.[1]

12. Apple controls what applications may be sold or provided to consumers through the App Store by a rigorous vetting process that involves provision of the proposed application's purpose and a copy of the application itself and any relevant source code, users' guides, and software documentation.[2]

13. Apple customers in fact have no other practical or convenient manner in which to download applications for their iPhones or iPads, as Apple maintains rigorous control over applications that can be placed on their devices.[3]

14. The monopolistic App Store therefore generates tens of billions in dollars of revenue per year for Apple, through Apple's charging of a 70/30 percent split on all revenue generated through applications downloaded through the App Store, whether through fees for downloads, subscriptions, in-app purchases, or service fees.[4]

---

[1] https://www.apple.com/app-store/ (last accessed September 3, 2021 at 5:31PM).

[2] *See, e.g.,* https://developer.apple.com/app-store/review/guidelines/#business (last accessed September 3, 2021, at 1:27PM EST).

[3] *See, e.g.,* https://www.lifewire.com/get-apps-not-in-app-store-1999916 (last accessed September 3, 2021, at 5:31PM).

[4] *See, e.g.,* https://www.cnbc.com/2021/01/08/apples-app-store-had-gross-sales-around-64-billion-in-2020.html (last accessed September 3, 2021, at 5:34PM); https://www.marketwatch.com/story/how-profitable-is-apples-app-store-even-a-landmark-antitrust-trial-couldnt-tell-us-11622224506; (last accessed September 3, 2021, at 5:35PM); https://www.theverge.com/2019/3/20/18273179/apple-icloud-itunes-app-store-music-services-businesses (last accessed September 3, 2021, at 5:33PM).

15. Furthermore, even when Apple does not directly profit from an application downloaded from the App Store, drawing consumers to its selling forum, as opposed to other fora, has considerable business advantage to Apple, as it dissuades consumers from using other devices.

16. Because Plaintiff knew, or at least thought she knew, that Apple thoroughly vets applications before it allowed them on the App Store, Plaintiff downloaded the application known as Toast Plus from the Apple App Store on or about March of 2020 onto her iPhone.

17. Plaintiff believed that Toast Plus was a version of Toast Wallet, a well-known cryptocurrency wallet, as the names were similar and the logo used for the application in the App Store was the same or nearly identical.

18. On or about January 2, 2018, Plaintiff caused approximately 474 Ripple ("XRP") cryptocurrency coins to be transferred from the Bittrex cryptocurrency exchange to a secure cryptocurrency wallet, called Rippex.

19. Rippex shut down February 2nd, 2018; however, Plaintiff could still access her coins from any secure wallet. Plaintiff thereafter linked her private XRP key, or a seed phrase, into Toast Plus in March of 2021.

20. As Plaintiff intended to hold the XRP as an investment and not to actively trade it, she did not check the Toast Wallet Plus application after entering her seed phrase into it.

21. In August of 2021, Plaintiff checked her account on Toast Plus, and discovered that not only did she have no XRP in the Wallet, her account was "deleted" on March 3, 2021.

22. Plaintiff thereupon began investigating the matter, and discovered that Toast Plus was not in fact a version of the legitimate Toast Wallet application, but was instead a "spoofing" or "phishing" program created for the sole purpose of stealing cryptocurrency, by obtaining consumers' cryptocurrency account information and thereafter routing the same to the hackers' personal accounts.

23. Plaintiff took the following steps to investigate the theft of her property: contacting or attempting to contact Toast Plus; investigating Toast Plus through online resources; contacting Apple; contacting the Federal Trade Commission and the Federal Bureau of Investigations; and identifying co-conspirators involved in the fraudulent acts through online research.

24. While the App Store does have terms and conditions, including limitations on liability, those terms and conditions are the product of adhesion, in that consumers have no other practical ability to access applications for the iPhones and iPads if they do not use the App Store; those terms and conditions are therefore not applicable to this case.

25. Plaintiff has no power to negotiate any terms whatsoever and no other source from which to get applications for her Apple products, and or many of the terms of which are unenforceable as being in violation of public policy.

26. Furthermore, those contractual terms are expressly exempted when there are State laws that either forbid such contractual terms or legislation that otherwise controls the subject matter.

27. Furthermore, the fact that Toast Plus was not an actual application, but instead a medium for the commission of fraud, makes any existing contract using it as

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.