

Aaron J. Solomon, Esq.  
OVED & OVED LLP  
Attorneys for Plaintiffs  
401 Greenwich Street  
New York, NY 10013

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----X

TIGRAN OHANIAN, INDIVIDUALLY AND ON  
BEHALF OF ALL OTHER PERSONS SIMILARLY  
SITUATED, AND REGGE LOPEZ, INDIVIDUALLY  
AND ON BEHALF OF ALL OTHER PERSONS SIMILARLY  
SITUATED,

CASE No.: 20-cv-05162

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

*Plaintiffs,*

- against -

APPLE INC. AND T-MOBILE USA, INC.

-----X

Plaintiffs Tigran Ohanian (“Ohanian”) and Regge Lopez (“Lopez”) (collectively, “Named Plaintiffs”), by their attorneys, Oved & Oved LLP, complaining of Defendants Apple Inc. (“Apple”) and T-Mobile USA, Inc. (“T-Mobile”) allege upon knowledge as to themselves, and upon information and belief as to all other matters, as follows:

**SUMMARY OF CLAIMS**

1. This is a class action brought to redress Apple’s deceptive acts and practices and material omissions regarding the data privacy and security of its mobile devices, namely the iPhone and the iMessage and FaceTime features that are unique to the iPhone, as well as T-Mobile’s deceptive acts and practices and material omissions related to its subscriber identification modules (“SIM cards”), by which it provides telecommunications services to consumers through the iPhone.

2. During the time period in question, Apple represented to consumers, through a variety of marketing campaigns both in print and through digital mediums, that the iPhone was

designed to protect the privacy of users' data and confidential personal information, and that the iMessage and Facetime features unique to the iPhone were highly secure methods of communication. As such, Apple was able to command premium prices for the sale of the iPhone as compared to other smartphones that were available for purchase on the market.

3. At the same time, however, Apple deceived consumers by failing to disclose a significant security flaw in the Apple iOS software – the operating system for the iPhone – known only to Apple that allowed iMessage correspondence sent by iPhone users and FaceTime calls made by iPhone users to be improperly directed to and accessed by third parties.

4. During that same time period, T-Mobile marketed and sold iPhone-compatible SIM cards to consumers for use in the iPhone. However, T-Mobile deceived consumers – who were under the reasonable belief that the SIM cards would provide them with a private and secure means to communicate through the iPhone on T-Mobile's wireless network – by failing to disclose that its practice of recycling phone numbers linked to SIM cards, and selling those SIM cards to consumers without requiring prior users to manually disassociate their Apple IDs from the phone numbers associated with the recycled SIM cards, did not protect the privacy of users' data and confidential personal information.

5. Apple's failure to disclose the security flaw in the Apple iOS software used in the iPhone, as well as T-Mobile's failure to disclose the fact that its SIM card practices did not protect the privacy of users' data and confidential personal information, caused consumers who purchased iPhones and/or utilized T-Mobile SIM cards in iPhones to become the unsuspecting victims of extensive data security breaches when their iMessage correspondence and FaceTime calls were improperly accessed by third parties without their knowledge or authorization.

6. Apple's release of the iOS 12 software on or about September 17, 2018 purportedly resolved these data security issues for iPhone users that actually installed the software, yet Apple never informed iPhone users, consumers, or the general public of the fact that the known security flaw in the iOS software led to innumerable unintended disclosures of iPhone users' iMessage correspondence and FaceTime calls to third parties for nearly seven years prior to that. Indeed, even to this day, not all consumers that purchased iPhones or T-Mobile SIM cards for use in iPhones have installed the iOS 12 software on their iPhones, and the data security breaches alleged herein still may be affecting those consumers.

7. Named Plaintiffs, both of whom are iPhone users that purchased T-Mobile SIM cards in order to utilize the communications features of the iPhone including iMessage and FaceTime, bring this proposed consumer class action on their own behalf and on behalf of all other persons similarly situated who, from the applicable limitations period through the present (the "Class Period") purchased Apple iPhones and/or T-Mobile SIM cards for use in iPhones, and utilized the iMessage and FaceTime features included in all iPhones.

### **THE PARTIES**

8. Ohanian is a natural person presently residing in Moscow, Russia.

9. Lopez is a natural person presently residing in the State of Florida.

10. Apple is a multinational company that manufactures, advertises, markets, distributes, and sells, *inter alia*, computer hardware, software, and mobile devices, including the iPhone. Apple is a California corporation with its principal place of business located at One Apple Park Way, Cupertino, California 95014.

11. T-Mobile is a wireless mobile network operator that manufactures, advertises, markets, distributes, and sells, *inter alia*, SIM cards. T-Mobile is a Delaware Corporation with

its principal place of business located at 12920 SE 38th St., Bellevue, Washington 98006.

**JURISDICTION / VENUE**

12. This Court has original jurisdiction over this matter pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action, as defined by 28 U.S.C. § 1332(d)(1)(B), in which there are 100 or more class members, a member of the putative class is a citizen of a different state than Apple and T-Mobile, and the amount in controversy exceeds the sum or value of \$5,000,000.00, excluding interest and costs.

13. This Court has personal jurisdiction over Apple pursuant to CPLR § 302(a)(1) because it transacts business in the State of New York by advertising, marketing, distributing, and selling its consumer product, the iPhone, throughout New York State to consumers in New York State, including Named Plaintiffs and members of the class, and it engaged in the wrongdoing alleged herein in New York State. Further, Apple has sufficient minimum contacts with New York State and has intentionally availed itself of the consumer market in New York State, rendering the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

14. This Court has personal jurisdiction over T-Mobile under CPLR § 302(a)(1) because it transacts business in the State of New York by advertising, marketing, distributing, and selling SIM cards throughout New York State to consumers in New York State, including Named Plaintiffs and members of the class, and it engaged in the wrongdoing alleged herein in New York State. Further, T-Mobile has sufficient minimum contacts with New York State and has intentionally availed itself of the consumer market in New York State, rendering the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in this District.

### **CLASS ALLEGATIONS**

16. This action meets the prerequisites of a Class Action under Rule 23(a) of the Federal Rules of Civil Procedure.

17. This action is brought on behalf of Named Plaintiffs and a class consisting of similarly situated individual consumers who (i) purchased one or more iPhones, or purchased one or more T-Mobile SIM cards for use in iPhones, during the Class Period; and (ii) utilized the iMessage and/or FaceTime features of the iPhones through the SIM cards during the Class Period, by which they became victims of the pervasive data security breaches as alleged herein.

18. This action meets the numerosity requirement because the putative class is so numerous that joinder of all members is impracticable. The exact size of the putative class in New York State is not yet known, but it is believed to be in excess of 1 million consumers.

19. This action meets the commonality requirement because common questions of law and fact arise from the wrongful conduct of Apple and T-Mobile directed at Named Plaintiffs and members of the class as described herein that violated New York General Business Law § 349 (“NY GBL § 349”) and New York General Business Law § 350 (“NY GBL § 350”), and also give rise to common law claims for fraudulent misrepresentation and unjust enrichment. Such questions include, *inter alia*:

- a. Whether Named Plaintiffs and members of the class purchased iPhones or T-Mobile SIM cards for use in iPhones during the Class Period, and utilized the iMessage and FaceTime features unique to iPhones during the Class Period;
- b. Whether Apple possessed material information regarding a security flaw in the iOS software utilized in the iPhone that allowed iMessage correspondence and FaceTime calls to be improperly accessed by third parties without the knowledge or authorization of iPhone users;

# 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.