EXHIBIT "A"

Matt Putterman (CA Bar No. 306845)
PUTTERMAN LAW, APC
23 Corporate Plaza Drive - Suite 150
Newport Beach, CA 92660
Telephone: (949) 271-6382
E-Mail: Matt@Putterman-Law.com

David C. Silver, Esq. (*Pro Hac Vice* - DE 10)
SILVER MILLER
~~11780 W. Sample Road~~4450 NW 126th Avenue - Suite 101
Coral Springs, Florida 33065
Telephone: (954) 516-6000
E-Mail: DSilver@SilverMillerLaw.com

Attorneys for Plaintiff Daniel Fraser

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

DANIEL FRASER, an individual;

Plaintiff,

v.

MINT MOBILE, LLC, a Delaware limited liability company;

Defendant.

Case No. 3:22-cv-00138-WHA

FIRST AMENDED COMPLAINT FOR:
(1) DECLARATORY JUDGMENT
(2) BREACH OF FEDERAL COMMUNICATIONS ACT [47 U.S.C. §§ 206, 222]
(3) VIOLATION OF COMPUTER FRAUD AND ABUSE ACT ("CFAA") [18 U.S.C. § 1030(a)(2)(C) and 1030(a)(4)]
(4) VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW - CAL. BUS. & PROF. CODE § 17200 *et seq*.
(5) VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW - CAL. BUS. & PROF. CODE § 17200 *et seq*.
(6) VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW - CAL. BUS. & PROF. CODE § 17200 *et seq*.
(7) NEGLIGENCE
(8) NEGLIGENT MISREPRESENTATION
(9) NEGLIGENT TRAINING AND SUPERVISION
(10) BREACH OF CONTRACT
(11) BREACH OF IMPLIED CONTRACT
~~**(12) BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING**~~

Plaintiff DANEIL FRASER, an individual (hereafter referred to as "Plaintiff"), by and through undersigned counsel, hereby sues Defendant MINT MOBILE, LLC, a Delaware limited liability company ("Defendant" or "MINT"), for damages and equitable relief. As grounds therefor, Plaintiff alleges the following:

PRELIMINARY STATEMENT

1. This action is brought by Plaintiff, a MINT customer who lost approximately Four Hundred Sixty-Six Thousand Dollars ($466,000.00) worth of cryptocurrency in an ongoing identity theft crime called "SIM hijacking."

2. A subscriber identity module, widely known as a "SIM card," stores user data in phones on the Global System for Mobile (GSM) network -- the radio network used by MINT, operating on T-Mobile's GSM-based network, to provide cellular telephone service to its subscribers.

3. MINT is a mobile virtual network operator ("MVNO") that operates on the infrastructure of T-Mobile's existing network.

4. SIM cards are principally used to authenticate cellphone subscriptions; as without a SIM card, GSM phones are not able to connect to T-Mobile's telecommunications network.

5. Not only is a SIM card vital to using a phone on the MINT network, the SIM card also holds immeasurable value as a tool to identify the user of the phone -- a power that can be corrupted to steal the identity of that user.

6. Preserving the security surrounding a MINT accountholder's SIM card and account with the phone carrier is a duty of paramount importance.

7. MINT expressly acknowledges that MINT's consumers "*have a right, and [Mint Mobile] has a duty, to protect the confidentiality of information regarding your telephone use, the services you purchase from us, the calls you place and the location of your device on our network when you make a telephone call*" and that once MINT "*receive[s] your personal information, we take steps that we believe are reasonable to limit access to your personal information to only those employees and service providers whom we determine need access to the personal information to provide the requested products, services, offers or opportunities that may be of interest to you or that you have ordered*."

8. Likewise, MINT acknowledges "*us[ing] technology and security features and strict policy guidelines to safeguard the privacy of CPNI and protect it from unauthorized access or improper use. Mint Mobile does not disclose CPNI outside of Mint Mobile, its affiliates and their respective agents without customer consent except as required by law*."

9. Those statements are consistent with MINT's duties and obligations under the Federal Communications Act of 1934 and the pertinent implementing regulations.

10. Moreover, MINT is well aware of the pervasive harm posed by SIM hijacking, as its co-founder Rizwan Kassim has publicly acknowledged the issue as far back as 2019.[1]

11. Notwithstanding the importance of the duty MINT concedes that it bears, MINT breached its duty to safeguard the data it had collected from and about Plaintiff; and MINT facilitated the theft of Plaintiff's identity and his assets.

12. As reported by numerous media sources[2], MINT exposed to hackers and countless unauthorized persons on or about June 8, 2021 through June 10, 2021 the personal identifying information of a number of MINT subscribers, including the subscribers' names, addresses, e-mail addresses, phone numbers, account numbers, and passwords.

13. **Plaintiff was among the unfortunate MINT subscribers whose personal information was exposed by MINT in June 2021.**

14. Shortly after the data breach, MINT confirmed in an e-mail to Plaintiff that his MINT account had been compromised and that, as a result, his phone number has been ported to another mobile telecommunications carrier:

---

[1] *See*, *e.g.*, "SIM hijacking/Port Out Fraud: we might be at risk!", *Reddit* (January 7, 2019), https://www.reddit.com/r/mintmobile/comments/adjdw7/sim_hijacking_port_out_fraud_we_might_be_at_risk/.

[2] *See*, *e.g.*, "Mint Mobile hit by a data breach after numbers ported, data accessed," *Bleeping Computer* (July 10, 2021), https://www.bleepingcomputer.com/news/security/mint-mobile-hit-by-a-data-breach-after-numbers-ported-data-accessed/; "Hackers Access Personal and Call Information and Port Numbers in Mint Mobile Data Breach," *CPO Magazine* (July 22, 2021), https://www.cpomagazine.com/cyber-security/hackers-access-personal-and-call-information-and-port-numbers-in-mint-mobile-data-breach/.

From: Mint Mobile VIP <vip@mintmobile.com>
Date: July 9, 2021 at 5:03:55 PM PDT
Subject: Important message from Mint Mobile VIP Care

Between June 8, 2021 and June 10, 2021, a very small number of Mint Mobile subscribers' phone numbers, including yours, were temporarily ported to another carrier without permission. While we immediately took steps to reverse the process and restore your service, an unauthorized individual potentially gained access to some of your information, which may have included your name, address, telephone number, email address, password, bill amount, international call detail information, telephone number, account number, and subscription features.

Attached hereto as **Exhibit "A"** is a true and correct copy of the entire July 9, 2021 message sent by MINT to Plaintiff.

15. MINT ported out Plaintiff's phone number to an unauthorized person in an unauthorized manner on June 11, 2021 even though just days earlier (June 8, 2021), Plaintiff had implemented "PIN verification" on his MINT account which, for security purposes, required anyone contacting MINT to provide a one-time temporary passcode to make any changes on Plaintiff's account, including transferring his phone service to a different telecommunications provider.

16. On June 11, 2021, swiftly following MINT's release of Plaintiff's personal identifying information and account to an unauthorized person, Plaintiff was robbed of his assets -- an act that would not have happened but for MINT providing the unauthorized person all of the tools needed to commit such a heinous and devastating act.

17. "SIM hijacking" is not merely an ongoing crime; it is a booming crime -- especially one that targets cryptocurrency investors.

18. Over the past three years alone, undersigned counsel has represented nearly three hundred (300) SIM hijacking victims across the country whose individual cryptocurrency losses have ranged from as little as $3,000.00 to as much as $12,500,000.00.

19. Notwithstanding MINT's knowledge of the prevalence of SIM hijacking and its assurance that it was actively protecting its customers, those measures did not adequately protect Plaintiff from the harm he suffered.

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.