UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

CALVIN CHENG, **Plaintiff,** **– against –** **T-MOBILE USA, INC.,** **Defendant.**	**Case No.: _____** **COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff CALVIN CHENG ("**Plaintiff**") by and through his attorneys, WILSON & CHAN, LLP, upon information and belief, complain and allege as follows against **Defendant T-MOBILE USA, INC.** ("**T-Mobile**") as follows:

NATURE OF THE CASE

1. This action arises out of T-Mobile's systemic and repeated failures to protect and safeguard its customers' highly sensitive personal and financial information against common, widely reported, and foreseeable attempts to illegally obtain such information.

2. As a result of T-Mobile's gross negligence in protecting customer information, including its negligent hiring and supervision of customer support personnel and its violations of Federal laws designed to protect wireless service consumers, Plaintiff lost in excess of $450,000

in cryptocurrency due to an account takeover scheme (also known as "SIM-swapping") which could not have occurred but for T-Mobile's negligent practices and its repeated failure to adhere to federal and state law.

3. T-Mobile is one of the nation's largest wireless carriers, having recently merged with Sprint and is governed by numerous federal statutes, including the Federal Communications Act (FCA).

4. T-Mobile regularly holds itself out as a secure custodian of customer data, including customer financial and personal information.

5. T-Mobile maintains that is uses a "variety of administrative, technical, procedural, contractual, and physical security measures" to protect customer data against "accidental, unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or use while it is under our control."[1]

6. Moreover, T-Mobile states that it maintains "authentication procedures when [customers] contact us by phone or in retail locations to help ensure that access is provided only to the primary account holder or authorized users of the account."[2]

7. As T-Mobile is aware, SIM-swapping and other forms of account takeover fraud have been widely reported in the press and by government regulators, including the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC), as well as by academic research teams.

---

[1] Available at https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (last accessed Jan. 27, 2021).

[2] Id.

8. Account takeover schemes involve criminals and fraudsters gaining access to or "hijacking" customer wireless accounts, which often include sensitive personal and financial information, to induce third parties to conduct transactions with individuals they believe to be legitimate or known to them.

9. One of the most damaging and pervasive forms of account takeover fraud is "SIM-swapping" whereby a criminal third-party convinces a wireless carrier like T-Mobile to transfer access to one of its legitimate customers' cellular phone number from the legitimate customer's registered SIM-card – a small portable chip that houses identification information connecting an account to the wireless carrier's network[3] – to a SIM-card controlled by the criminal third-party.

10. This sort of account takeover is not an isolated criminal act, *per se*, as it requires the wireless carrier's active involvement to swap the SIM to an unauthorized person's phone.

11. As such, by directly or indirectly exceeding the authorized access to customer accounts, wireless carriers such as T-Mobile may be liable under the Computer Fraud and Abuse Act (CFAA).

12. Unlike a direct hack of data where a company like T-Mobile plays a more passive role, SIM-swaps are ultimately actualized by the wireless carrier itself. It is T-Mobile, in this case, that effectuates the SIM card change. This action remains operative and in force when the victim's

[3] A SIM ("subscriber identity module") card is a small, removable chip that allows a cell phone to communicate with the wireless carrier and to know which subscriber is associated with that phone. The SIM card associated with a wireless phone can be changed, allowing customers to move their wireless number from one cell phone to another and to continue accessing their carrier network when they switch cell phones. The wireless carrier must effectuate the SIM card reassignment.

phone activity is used to hack other online accounts, extort the victim, or cause other foreseeable injuries, such as the one suffered by Plaintiff here.[4]

13. Once the third-party has access to the legitimate user's SIM-card data, it can seamlessly impersonate the legitimate wireless customer.

14. A common target of SIM-swapping and account takeover fraud are individuals known to, or expected to, hold large quantities of cryptocurrency as account information is often contained on users' cellular phones, allowing criminals to transfer the legitimate user's cryptocurrency to an account the criminal controls.

15. SIM-swapping is not a new unforeseeable phenomenon but, instead, has been discussed by federal agencies since at least 2016.

16. In June 2016, the FTC's Chief Technologist, herself the victim of an account takeover, recounted her experience and offered advice to wireless carriers to help consumers avoid these takeover attacks, stating:

> The mobile carriers are in a better position than their customers to prevent identity theft through mobile account hijacking and fraudulent new accounts. In fact, many of them are obligated to comply with the Red Flags Rule, which, among other things, requires them to have a written identity theft prevention program.
>
> Carriers should adopt a multi-level approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions …
>
> [M]obile carriers and third-party retailers need to be vigilant in their authentication practices to avoid putting their customers at risk of major

[4] Wireless carriers such as T-Mobile have superior knowledge of their own and their customers' experience with SIM-swap attacks and can foresee identity theft and impersonation of their customers following their effectuating of the SIM change. That a criminal may act as an intervening agent does not break the sequence of causation where T-Mobile had reasonable ground to anticipate such injuries to third-parties such as Plaintiff.

financial loss and having email, social network, and other accounts compromised.[5]

17. Attention in the media and by government regulators, however, did not ensure that wireless carriers like T-Mobile took security seriously enough to prevent account takeover accounts and SIM-swapping schemes from increasing or, worse, to convince themselves, company-wide, to stop engaging in practices that were clearly violative of federal law.

18. An empirical study conducted by researchers at Princeton University in early 2020, the results of which were aware to T-Mobile prior to publication, concluded that they "identified weak authentication schemes and flawed policies" at several major wireless carriers in the United States, including T-Mobile.[6]

19. The researchers also concluded that "these flaws enable straightforward SIM swap attacks."[7]

20. One particularly weak form of customer authentication used by T-Mobile – the use of recent call logs – was identified as a "severe vulnerability," allowing criminals to authenticate a legitimate account by using information that can be manipulated without authentication.[8]

---

[5] "*Your Mobile Phone Account Could be Hijacked by an Identity Thief*," L. Cranor, Tech@FTC blog (June 7, 2016); Ms. Cranor also detailed her concerns about SIM-swapping in her reply comments before the Federal Communications Commission in July 2016 (In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunication Services; WC Docket No. 16-106; July 6, 2016).

[6] "*An Empirical Study of Wireless Carrier Authentication for SIM Swaps*," K. Lee, et al., Dept. of Comp. Sci. and Ctr. for Info. Tech. Policy, Princeton University (Jan. 10, 2020), at p. 10; *see also* p. 2 (discussing T-Mobile's discontinuation of call log verification based on the study's research in January 2020).

[7] Id.

[8] Id. at p. 6.

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.