UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF NEW YORK

Reginald Middleton, and Veritaseum, LLC, Plaintiffs, v. T-Mobile US, Inc., Defendant.	**COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Reginald Middleton and Veritaseum LLC (collectively, "Plaintiffs" and individually "Mr. Middleton" and "Veritaseum"), by and through their counsel, complain and allege as follows against T-Mobile US, Inc. ("Defendant" or "T-Mobile"):

NATURE OF THE CASE

1. This action arises out of T-Mobile's failure to protect its customers' highly sensitive personal and financial information. As a result of T-Mobile's gross negligence in protecting Plaintiffs' information, its negligent hiring and supervision of T-Mobile employees who were responsible for safeguarding that information, and its violation of laws that expressly protect the information of wireless carrier customers, Plaintiffs lost $8.7 million in cryptocurrency and Mr. Middleton suffered and continues to suffer severe anxiety, fear and emotional distress relating to the repeated instances of identity theft that

he experienced as a result of T-Mobile's inadequate protection of his personal and financial information.

2. T-Mobile is one of the three largest wireless carriers in the United States. As a leading wireless carrier, T-Mobile holds itself out, and is required by law to be equipped to protect the personal and financial information of its customers. Consistent with its duty to protect such information, T-Mobile promises its customers that it uses a variety of administrative, technical, and physical security measures designed to protect its customers' personal data—and particularly their data-rich SIM cards— against accidental, unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or use while it is under their control.

3. As T-Mobile is aware, and has been widely reported in the press and by the government regulators, including the Federal Trade Commission ("FTC") and Federal Communications Commission ("FCC"), fraudsters have been increasingly using schemes to access customer personal and financial information by causing unauthorized changes in customers' wireless accounts. The purpose of these schemes is to compromise customers' mobile identities, access confidential data, take over their financial accounts, and effectuate fraudulent transactions.

4. One of the most damaging and pervasive schemes is fraudulent SIM card swapping. In SIM card swapping schemes, a hacker convinces a mobile phone carrier to transfer access of a targeted person's phone number from her registered SIM card — the small portable chip that houses identification information connecting an account to the cell network — to the hacker's SIM card. Once the hacker has access to this information,

the hacker takes over the user's cell phone. Often, the hacker targets individuals who are known, or expected, to hold large quantities of cryptocurrency. If the target has cryptocurrency account information on his or her phone, the hacker can transfer that cryptocurrency to his or her own accounts.

5. In 2016, the FTC's Chief Technologist described these issues in a widely read post about her experience as a victim of an identity theft scheme and specifically called attention to the insidious "SIM swapping" scheme in which thieves use a victim's hijacked phone number to gain access to financial accounts that use two-factor authentication through text messages. *See* "Your mobile phone account could be hijacked by an identity thief," Lorrie Cranor, FTC Chief Technologist (Jun 7, 2016). https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief. T-Mobile was undoubtedly aware of this scheme and represented to its customers that they were protected against this type of identity theft scheme.

6. Nevertheless, in 2017, hackers began a campaign to victimize Reginald Middleton, a well-known holder of cryptocurrency and founder and sole owner of Veritaseum, a cryptocurrency company, through, and with the assistance of, his wireless carrier T-Mobile. On or about July 23, 2017, hackers targeted Mr. Middleton's cryptocurrency account by accessing his account at T-Mobile which he maintained for the use of Veritaseum and himself. In order to gain access to Mr. Middleton's financial accounts, a party unknown to Plaintiffs called T-Mobile pretending to be Mr. Middleton and seeking to conduct a SIM card swap. T-Mobile denied that request. The same or a

related party proceeded to call three more times, each time seeking to conduct a SIM card swap. On the next two attempts, T-Mobile denied the request. On the fourth attempt, T-Mobile granted access to this unknown party without Mr. Middleton's authorization.

7. T-Mobile then swapped Mr. Middleton's SIM card and transferred control of Mr. Middleton's phone number to a device under the control of the unknown party. That party was a hacker, who immediately took control of Mr. Middleton's phone, accessed multiple accounts of Mr. Middleton and Veritaseum on his phone, accessed Mr. Middleton's personal and financial information, and ultimately accessed his corporate and personal cryptocurrency addresses, wallets and online exchange accounts for holding cryptocurrency, using the access provided by T-Mobile to bypass the two-factor authentication (also known as "2FA") security measures.

8. Mr. Middleton's corporate and personal cryptocurrency addresses, wallets and online exchange accounts contained $8.7 million of cryptocurrency. The hacker proceeded to transfer $8.7 million of cryptocurrency from Mr. Middleton's corporate and personal cryptocurrency addresses, wallets and online exchange accounts to a separate cryptocurrency address and wallet owned and controlled by the hacker.

9. Mr. Middleton immediately contacted T-Mobile and spoke with T-Mobile representatives, including members of T-Mobile's security department about the issue. T-Mobile's representatives confirmed that T-Mobile permitted an unauthorized SIM swap and that T-Mobile would take steps to avoid future SIM swap occurrences.

10. Nevertheless, after the initial SIM swap, hackers continued to gain access to Mr. Middleton's phone by performing additional unauthorized SIM swaps with T-

Mobile's assistance. Despite T-Mobile's promise to Mr. Middleton that it would prevent future SIM swaps, hackers persuaded T-Mobile employees to authorize SIM swaps on August 22, 2017, September 16, 2017, and twice on October 4, 2017. After each unauthorized SIM swap, Mr. Middleton reported the issue to T-Mobile and T-Mobile confirmed the unauthorized SIM swap, however, T-Mobile did not take sufficient action to prevent future SIM swaps from occurring. Indeed, Mr. Middleton was on a call with T-Mobile's security representatives, discussing the unauthorized October 4, 2017 SIM swap, and receiving assurance that T-Mobile had addressed the issue and taken steps to avoid any future SIM swaps, when the phone cut off because T-Mobile had permitted yet another unauthorized SIM swap.

11. Even after those five unauthorized SIM swaps in 2017, Mr. Middleton continued to be victimized by unauthorized SIM swaps in 2018 and 2019. Mr. Middleton made repeated complaints to T-Mobile in 2018 and 2019 regarding these instances of unauthorized access to his T-Mobile account. After each such complaint, T-Mobile failed to take corrective action or do anything to stop the unauthorized access to his T-Mobile account.

12. Most striking, T-Mobile, itself, conceded its own failure to act in response to this unauthorized hacking of Mr. Middleton's account. In a letter to Mr. Middleton dated June 20, 2018, nearly one year after T-Mobile gave hackers unauthorized access to Mr. Middleton's account and caused $8.7 million in losses, T-Mobile reported:

> *We recently detected* unauthorized activity on your T-Mobile account, during which an unknown party would have had access to Customer Proprietary Network Information ("CPNI").

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.