# Data Breach Exposes Consumers of T-Mobile to SIM Swap Attacks

*MDF Law recommends that users do not use their cell phones for two factor authentication*


Marc D. Fitapelli

NEW YORK, NEW YORK, USA, January 24, 2023 /EINPresswire.com/ -- T-Mobile, one of the largest telecommunications providers in the United States, reported a significant data breach to the Securities and Exchange Commission (SEC) on January 19, 2023, exposing millions of its customers to SIM swap attacks. The company filed a Form 8-K with the SEC, which disclosed that hackers first accessed T-Mobile's systems on November 25, 2022, but their activities were not detected by T-Mobile until January 5, 2023. This hacking attack has left many current and former T-Mobile customers exposed to malicious activity, including SIM swapping. A copy of the full Form 8-k can be accessed by clicking here. It is also attached to the end of this press release.

If you or someone you know was a victim of a T-Mobile SIM swap, our attorneys want to speak to you. Please call 800-767-8040 or visit www.mdf-law.com to receive a free and confidential consultation.

A SIM swap attack is a type of identity theft in which a criminal takes over a victim's cell phone number by convincing the carrier to transfer the number to a SIM card under the criminal's control. This can be done by either tricking the carrier's customer service representative or by gaining access to a victim's account through a phishing attack. Once the criminal has control of the victim's phone number, they can use it to receive two-factor authentication codes and gain access to the victim's bank accounts, cryptocurrency exchanges, and other sensitive information.

According to the SEC disclosure, T-Mobile identified that a malicious actor obtained data from an API, or application programing interface, without permission or authorization. The company stated that the breach did not expose any customer credit cards, social security numbers, or driver's license information. However, the incident did result in hackers accessing customers' name, phone numbers, billing and email addresses, and dates of birth. The incident impacted 37

> If you were a victim of SIM swapping and had money or cryptocurrency stolen, call me at 800-767-8040 for a free and confidential consultation."
>
> *Marc D. Fitapelli, Esq.*

million current prepaid and postpaid customers, which is a significant portion of T-Mobile's customer base.

The filing with the SEC warns T-Mobile investors that the company "may incur significant expenses in connection with the incident." This is because T-Mobile, like all cell phone providers, is responsible for protecting customer's personal confidential information under the Federal Communications Act (FCA). Under the FCA, a telecommunications carrier is prohibited from disclosing a customer's "propriety network information" to unauthorized third-parties. Civil penalties under the FCA include the "full amount of damages sustained in consequence of any such violation...together with a reasonable counsel or attorney's fee..."

To prevent SIM swapping attacks, it is recommended that users do not use cell phones for two-factor authentication and instead use hardware tokens. If users do use their cell phones for 2FA, they should contact their carrier and inquire about whether the SIM could be locked or prevented from porting. Customers should also be vigilant about monitoring their accounts for suspicious activity and be prepared to take action if they suspect that their phone number has been compromised.

The recent T-Mobile data breach is a reminder of the importance of data security and the potential consequences of a data breach. It is crucial for companies to implement robust security measures to protect customer's personal confidential information, and for customers to be aware of the risks and take steps to protect themselves. As the world becomes more and more digital, the importance of data security will continue to grow, and companies that fail to protect their customer's data will face significant financial and reputational risks.

When did the recent hacking event occur?

T-Mobile reported that customer information was first accessed on November 25, 2022, but was not detected by the company until January 5, 2023, more than one month later. T-Mobile's disclosure to the Securities and Exchange Commission did not explain why it took so long to identify the breach.

Were social security numbers, credit cards or driver's licenses compromised?

According to T-Mobile, hackers were only able to access customers' phone numbers, email addresses, physical addresses, and dates of birth.

Does T-Mobile offer account takeover protection?

Yes.  Like many mobile carriers, T-Mobile offers account takeover protections, which are features that are designed to block unauthorized users from accessing or transferring SIM information. MDF Law recommends that all T-Mobile customers take advantage of these protections by enabling them as soon as possible.

What else could T-Mobile customers do to protect themselves from SIM attacks?

Customers should realize that using a cell phone for two factor authentication is not recommended. Instead, customers should use other means for two factor authentication, which include the use of a physical security token. If customers hold cryptocurrency, they should further consider protecting their assets by utilizing a cold storage device, such as a ledger.

What information is T-Mobile required to gather before providing customer information over the phone?

The regulations accompanying the FCA require mobile carriers to request a password from the customer if a request for a SIM swap or number port is made over the phone.  If a password is not provided, the carrier can only disclose personal information by mailing it to the address of record or calling the phone number on file.

What information is required if a request is made at a store location?

If an individual requests a SIM swap at a retail store location, the carrier may only disclose information to an individual who has a valid photo ID, which matches the customer information on file.

Are mobile carriers required to notify users about SIM swapping?

Mobile carriers are required to notify both the federal government as well as the effected consumer immediately after a SIM attack or other event, which results in the disclosure of customer personal confidential information.

What can users do if they were a victim of a SIM swap attack?

If a user was a victim of a SIM swap attack, they could pursue an individual case against their mobile carrier for money damages.  These cases are generally filed before the American Arbitration Association and not in court due to the compulsory arbitration provisions contained in most cell phone provider's terms of service.

Who can users contact if they were a victim of a T-Mobile SIM swap?

You can call MDF Law at 800-767-8040 for a free and confidential case evaluation. You can also visit www.mdf-law.com for more information.

ATTORNEY ADVERTISING
PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME

MDF Law PLLC's phone number is 800-767-8040 and its principal address is 28 Liberty Street, 30th Floor, New York, New York 10005.

Marc Fitapelli
MDF Law
+1 212-203-9300
marc@mdf-law.com

---