UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d)
of the Securities Exchange Act of 1934

Date of report (Date of earliest event reported): August 20, 2021

T-MOBILE US, INC.
(Exact Name of Registrant as Specified in Charter)

DELAWARE	**1-33409**	**20-0836269**
(State or other jurisdiction of incorporation)	**(Commission File Number)**	**(IRS Employer Identification No.)**

12920 SE 38th Street **Bellevue, Washington** **(Address of principal executive offices)**	**98006-1350** **(Zip Code)**

Registrant's telephone number, including area code: (425) 378-4000

(Former Name or Former Address, if Changed Since Last Report):

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading symbol	Name of each exchange on which registered
Common Stock, $0.00001 par value per share	**TMUS**	**The NASDAQ Stock Market LLC**

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§ 230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§ 240.12b-2 of this chapter).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Item 7.01 Regulation FD Disclosure.

On August 20, 2021, T-Mobile US, Inc. ("T-Mobile," "we," "our" or "us") posted the following statement to its website:

T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack (8/20/21)

We have continued to work around the clock on the forensic analysis and investigation into the cyberattack against T-Mobile systems while also taking a number of proactive steps to protect customers and others whose information may have been exposed.

Our investigation is ongoing and will continue for some time, but at this point, we are confident that we have closed off the access and egress points the bad actor used in the attack. Below is what we know to date.

- We previously reported information from approximately 7.8 million current T-Mobile postpaid customer accounts that included first and last names, date of birth, SSN, and driver's license/ID information was compromised. We have now also determined that phone numbers, as well as IMEI and IMSI information, the typical identifier numbers associated with a mobile phone, were also compromised. Additionally, we have since identified another 5.3 million current postpaid customer accounts that had one or more associated customer names, addresses, date of births, phone numbers, IMEIs and IMSIs illegally accessed. These additional accounts did not have any SSNs or driver's license/ID information compromised.
- We also previously reported that data files with information from about 40 million former or prospective T-Mobile customers, including first and last names, date of birth, SSN, and driver's license/ID information, were compromised. We have since identified an additional 667,000 accounts of former T- Mobile customers that were accessed with customer names, phone numbers, addresses and dates of birth compromised. These additional accounts did not have any SSNs or driver's license/ID information compromised.
- Separately, we have also identified further stolen data files including phone numbers, IMEI, and IMSI numbers. That data included no personally identifiable information.
- We continue to have no indication that the data contained in any of the stolen files included any customer financial information, credit card information, debit or other payment information.
- As we previously reported, approximately 850,000 active T-Mobile prepaid customer names, phone numbers and account PINs were exposed. We have proactively reset ALL of the PINs on these accounts. Similar information from additional inactive prepaid accounts was also accessed. In addition, up to 52,000 names related to current Metro by T-Mobile accounts may have been included. None of these data sets included any personally identifiable information. Further, none of the T-Mobile files stolen related to former Sprint prepaid or Boost customers.

We are continuing to take action to protect everyone at risk from this cyberattack, including those additional persons we recently identified. We have sent communications to millions of customers and other affected individuals and are providing support in various ways. This includes:

- Offering two years of free identity protection services with McAfee's ID Theft Protection Service to any person who believes they may be affected
- Recommending that all eligible T-Mobile customers sign up for free scam-blocking protection through Scam Shield
- Supporting customers with additional best practices and practical security steps like resetting PINs and passwords
- Publishing a customer support webpage that includes information and access to these tools at https://www.t-mobile.com/brand/data-breach-2021

As we support our customers, we have worked diligently to enhance security across our platforms and are collaborating with industry-leading experts to understand additional immediate and longer-term next steps. We also remain committed to transparency as this investigation continues and will continue to provide updates if new information becomes available that impacts those affected or causes the details above to change or evolve.

FORWARD-LOOKING STATEMENTS

This communication includes forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. All statements other than statements of historical fact are forward-looking statements. These forward-looking statements are generally identified by the words "anticipate," "believe," "estimate," "expect," "intend," "may," "could" or similar expressions. Forward-looking statements are based on current expectations and assumptions, which are subject to risks and uncertainties that may cause actual results to differ materially from the forward-looking statements. These risks and uncertainties include those related to the cybersecurity incident discussed above, such as our ability to assess and remedy the cybersecurity incident, and legal, reputational and financial risks resulting from this or other cybersecurity incidents and other risks and uncertainties associated with our business as described in our filings with the Securities and Exchange Commission. Given these risks and uncertainties, readers are cautioned not to place undue reliance on such forward-looking statements. We undertake no obligation to revise or publicly release the results of any revision to these forward-looking statements, except as required by law.

T-Mobile Disclosure Channels

Investors and others should note that we announce material information to our investors using our investor relations website, press releases, SEC filings and public conference calls and webcasts. We also intend to use certain social media accounts as means of disclosing information about us and our services and for complying with our disclosure obligations under Regulation FD (the @TMobileIR Twitter account (https://twitter.com/TMobileIR) and the @MikeSievert Twitter (https://twitter.com/MikeSievert) account, which Mr. Sievert also uses as a means for personal communications and observations). The information we post through these social media channels may be deemed material. Accordingly, investors should monitor these social media channels in addition to following our investor relations website, press releases, SEC filings and public conference calls and webcasts. The social media channels that we intend to use as a means of disclosing the information described above may be updated from time to time as listed on our investor relations website.

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

Date: August 20, 2021

T-MOBILE US, INC.

By: /s/ Peter Osvaldik
Peter Osvaldik
Executive Vice President and Chief Financial Officer