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 27, 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	98006-1350
(Address of principal executive offices)	(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 27, 2021, T-Mobile US, Inc. ("T-Mobile," "we," "our" or "us") posted the following statement to its website:

The Cyberattack Against T-Mobile and Our Customers:
What happened, and what we are doing about it.

By Mike Sievert
CEO, T-Mobile

The last two weeks have been humbling for all of us at T-Mobile as we have worked tirelessly to navigate a malicious cyberattack on our systems. Now with the breach having been contained and our investigation substantially complete, I wanted to take a moment to provide an update and some perspective on where things stand, what we have been doing to take care of impacted people, and the measures we are taking to better protect consumers from future incidents like this.

On August 17th we confirmed that T-Mobile's systems were subject to a criminal cyberattack that compromised data of millions of our customers, former customers, and prospective customers. Fortunately, the breach did not expose any customer financial information, credit card information, debit or other payment information but, like so many breaches before, some SSN, name, address, date of birth and driver's license/ID information was compromised. To say we are disappointed and frustrated that this happened is an understatement. Keeping our customers' data safe is a responsibility we take incredibly seriously and preventing this type of event from happening has always been a top priority of ours. Unfortunately, this time we were not successful.

Attacks like this are on the rise and bad actors work day-in and day-out to find new avenues to attack our systems and exploit them. We spend lots of time and effort to try to stay a step ahead of them, but we didn't live up to the expectations we have for ourselves to protect our customers. Knowing that we failed to prevent this exposure is one of the hardest parts of this event. On behalf of everyone at Team Magenta, I want to say we are truly sorry.

As our initial investigation into the incident winds down, I felt it was important to share an update on our work and, importantly, what's next. We're fully committed to take our security efforts to the next level as we work to rebuild trust and I want to tell you more about what we have in progress.

What we know about the incident

Through our investigation into this incident, which has been supported by world-class security experts Mandiant from the very beginning, we now know how this bad actor illegally gained entry to our servers and we have closed those access points. We are confident that there is no ongoing risk to customer data from this breach.

We recognize that many are asking exactly what happened. While we are actively coordinating with law enforcement on a criminal investigation, we are unable to disclose too many details. What we can share is that, in simplest terms, the bad actor leveraged their knowledge of technical systems, along with specialized tools and capabilities, to gain access to our testing environments and then used brute force attacks and other methods to make their way into other IT servers that included customer data.

In short, this individual's intent was to break in and steal data, and they succeeded.

Since confirming this breach, we have worked around the clock to understand impact and risk to customers and others and have done our very best to be transparent about those impacts as quickly as possible. This is not a one-and-done process. There is much work to do, and this will take time, and we remain committed to doing our best to ensure those who had information exposed feel informed, supported, and protected by T-Mobile.

Taking care of our customers

As our internal investigation has continued, our teams have made supporting our customers a top priority—from answering questions to helping customers get access to tools and best practices that will help them protect their information.

As of today, we have notified just about every current T-Mobile customer or primary account holder who had data such as name and current address, social security number, or government ID number compromised. T-Mobile customers or primary account holders who we do not believe had that data impacted will now see a banner on their MyT-Mobile.com account login page letting them know. We are also now working diligently to notify former and prospective customers. Our goal is to ensure that we are providing clear information about how customers and those affected can protect themselves. So, we have published a web page where we are:

- offering two years of free identity protection services with McAfee's ID Theft Protection Service to all persons who may have been affected
- recommending customers sign up T-Mobile's free scam-blocking protection through Scam Shield
- making Account Takeover Protection available for postpaid customers, which makes it more difficult for customer accounts to be fraudulently ported out and stolen
- suggesting other best practices and practical security steps like resetting PINs and passwords for all customers.

Our Path Forward

We know that the bad actors out there will continue to evolve their methods every single day and attacks across nearly every industry are on the rise. However, while cyberattacks are commonplace, that does not mean that we will accept them. T-Mobile is taking significant steps to enhance our approach to cybersecurity.

Today I'm announcing that we have entered into long-term partnerships with the industry-leading cybersecurity experts at Mandiant, and with consulting firm KPMG LLC. We know we need additional expertise to take our cybersecurity efforts to the next level—and we've brought in the help. These arrangements are part of a substantial multi-year investment to adopt best-in-class practices and transform our approach. This is all about assembling the firepower we need to improve our ability to fight back against criminals and building a future-forward strategy to protect T-Mobile and our customers.

As I previously mentioned, Mandiant has been part of our forensic investigation since the start of the incident, and we are now expanding our relationship to draw on the expertise they've gained from the front lines of large-scale data breaches and use their scalable security solutions to become more resilient to future cyber threats. They will support us as we develop an immediate and longer-term strategic plan to mitigate and stabilize cybersecurity risks across our enterprise.

Simultaneously, we are partnering with consulting firm KPMG, a recognized global leader in cybersecurity consulting. KPMG's cybersecurity team will

bring its deep expertise and interdisciplinary approach to perform a thorough review of all T-Mobile security policies and performance measurement. They will focus on controls to identify gaps and areas of improvement. Mandiant and KPMG will work side-by-side with our teams to map out definitive actions that will be designed to protect our customers and others from malicious activity now and into the future. I am confident in these partnerships and optimistic about the opportunity they present to help us come out of this terrible event in a much stronger place with improved security measures.

As we learn and evolve, we will always work to keep you informed of any important updates or relevant changes. I also commit to you that while we're starting on this path with humility, we will bring to it the same Un-carrier energy that we have used for years to help transform the wireless industry for the benefit of consumers and businesses everywhere.

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 (https://investor.t-mobile.com), newsroom website (https://t-mobile.com/news), 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, newsroom 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 27, 2021

T-MOBILE US, INC.

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