**T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack**

August 17, 2021

- Share on Facebook
- Share on Twitter
- Share on LinkedIn

**August 20, 2021**

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.