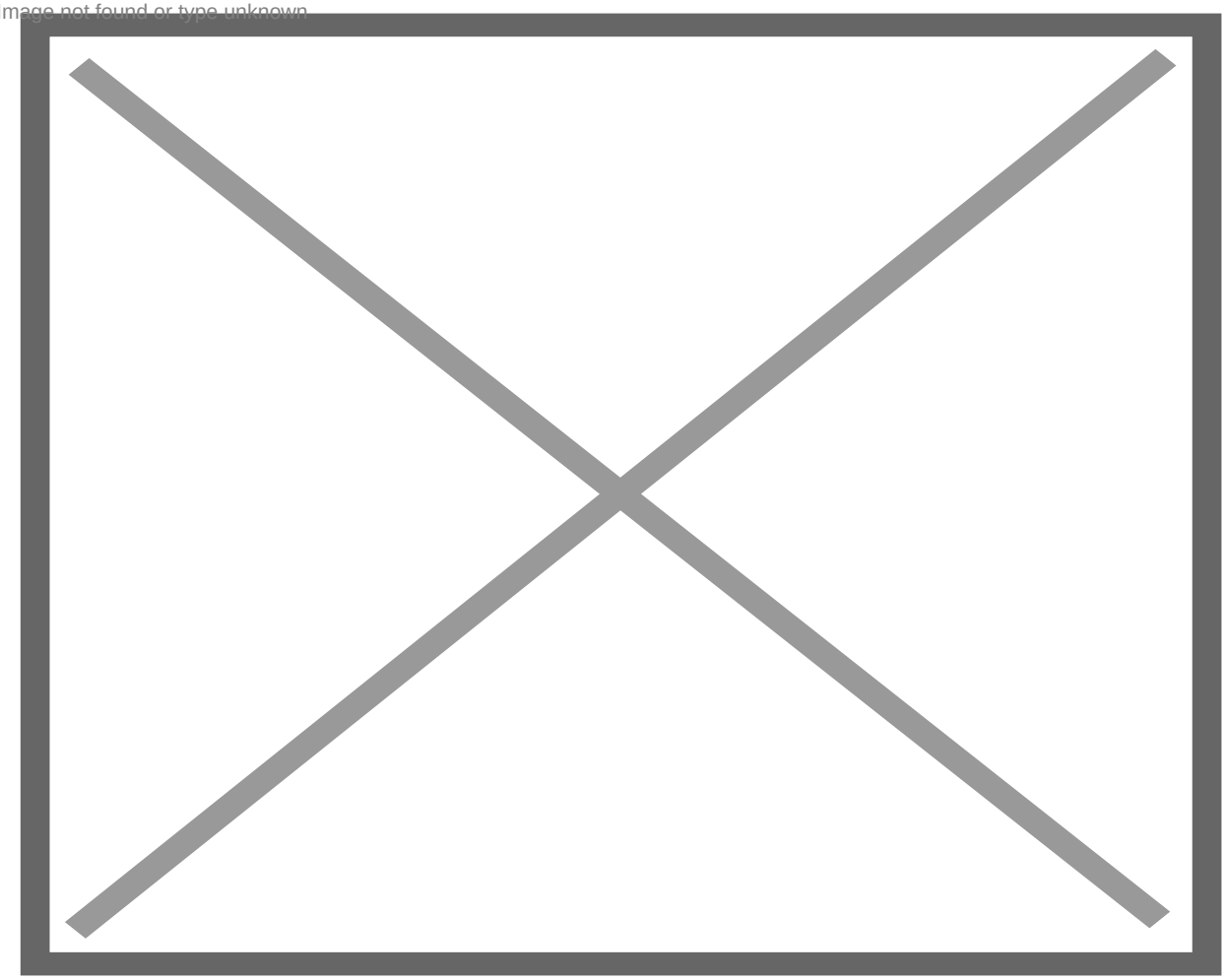
Data of 37 Million T-Mobile Customers Compromised Following Breach

Technology / **Published On January 19, 2023 06:50 PM /**

Staff Consortium January 19, 2023

Image not found or type unknown



T-Mobile announced in a statement Thursday that hackers accessed sensitive data of 37 million customers, including billing addresses and birth dates, and that it was working with law enforcement officials and cybersecurity experts.

The company said it discovered the breach on Jan. 5, however it believes the hackers had access to the data since Nov. 25, 2022, according to regulatory filing T-Mobile made public Thursday.

The massive breach is the second T-Mobile has suffered. In August 2021, the company announced that hackers had breached its security protocols and accessed data of more than 40 million customers. The stolen data at the time included Social Security numbers and other sensitive information, according to the Wall Street Journal.

T-Mobile has a robust operation in the U.S. Virgin Islands, having absorbed Sprint's customers in the territory following the August 2020 merger of the two mobile carriers.

The company said data accessed by the hackers in the Nov. 25 breach did not lead to safety concerns for its customers. "While no information was obtained for impacted customers that would compromise the safety of customer accounts or finances, we want to be transparent with our customers and ensure they are aware," T-Mobile said in a statement.

It further states, "No passwords, payment card information, social security numbers, government ID numbers or other financial account information were compromised. Some basic customer information (nearly all of which is the type widely available in marketing databases or directories) was obtained, including name, billing address, email, phone number, date of birth, account number, and information such as the number of lines on the account and service plan features.

"We understand that an incident like this has an impact on our customers and regret that this occurred. While we, like any other company, are unfortunately not immune to this type of criminal activity, we plan to continue to make substantial, multi-year investments in strengthening our cybersecurity program."