COMPLIANCE WEEK
FOR THE WELL-INFORMED CHIEF COMPLIANCE OFFICER AND AUDIT EXECUTIVE

T-Mobile the least surprising data breach of 2021



By Kyle Brasseur | Wed, Aug 18, 2021 11:10 AM

Despite their rising frequency this year, data breaches still have a way of catching companies and their customers off guard. You never think it'll be you in the crosshairs.

T-Mobile might be an exception. The telecommunications company's **latest data breach**, first reported by news outlet Vice over the weekend and confirmed by T-Mobile on Monday, is **still under investigation**, but it appears at least 47 million people—mostly former or prospective customers—were affected. Details compromised in some cases include customers' first and last names, dates of birth, Social Security numbers, and driver's license/ID information, though the company assures no financial information was breached.

The hackers behind the cyber-attack **told Vice** they had data related to more than 100 million customers, so T-Mobile's ongoing investigation might uncover more in the days ahead.

T-Mobile is no stranger to being in this position. The breach is at least the company's fifth to be publicly acknowledged since 2018, though none of the others have come close to matching the extent of this most recent attack.

However, it does call into question how seriously T-Mobile takes cyber-security that it would be subject to so many breaches in such a short time. The **2018 vulnerability** saw a hacker/hackers with unauthorized access obtain customer names, billing zip codes, phone numbers, email addresses, account numbers, account types, and dates of birth and reportedly affected roughly 2 million users.

Then came **two breaches** in a span of roughly four months from November 2019 to March 2020, each including the access of similar personally identifiable information (PII) on a relatively small scale. The latter of the two incidents appeared to occur via a third-party email vendor.

In **December 2020**, T-Mobile was once again the victim of unauthorized access to its servers, which reportedly exposed the call-related information of approximately 200,000 customers.

Thus, it seems it was only a matter of time until a hacker hit the motherload via access to a T-Mobile server. Regarding its most recent breach, the company stated it is "confident that the entry point used to gain access has been closed," but the same refrain was part of its statements regarding the other attacks. As was the obligatory "we take our customers' protection very seriously" line that loses its luster with each incident.

Granted, T-Mobile is part of an incredibly vulnerable industry when it comes to cyber-attacks. IBM's **X-Force Threat Intelligence Index 2021** listed media (which included telecommunications) as the eighth most targeted sector for cyber-attacks in 2020. A year prior, it was No. 4, with COVID-19 cited as a factor in other industries' rises.

Verizon **was the victim of a breach in 2017** that the company said exposed the data of 6 million customers. And AT&T in 2015 agreed to pay $25 million in a **settlement with the Federal Communications Commission** regarding investigations into three breaches.

To gain access to a telecom's server is to potentially obtain the information needed to phish a person's most relied upon piece of technology—their phone. Beyond robocalls, spam texts are becoming increasingly prevalent. I can't tell you how many times I've won a Costco sweepstakes despite never having shopped at the store.

All this is to say T-Mobile needs to do better at protecting its users' information. The company is taking steps to work with customers affected by its latest breach—including offering two years of free identity protection services—but the most crucial action it could take would be to invest in firming up its systems to prevent such frequent incidents from occurring.

Further, T-Mobile must do more to explain how these breaches continue occurring. To say a bad actor gained unauthorized access to a system is not enough when it keeps happening. The company must be more transparent and acknowledge where specifically it has failed in protecting PII. That's the least it owes its users.

Otherwise, T-Mobile might not have as many as 100 million customers to be affected the next time it is the victim of an attack.

RATE THIS RESOURCE