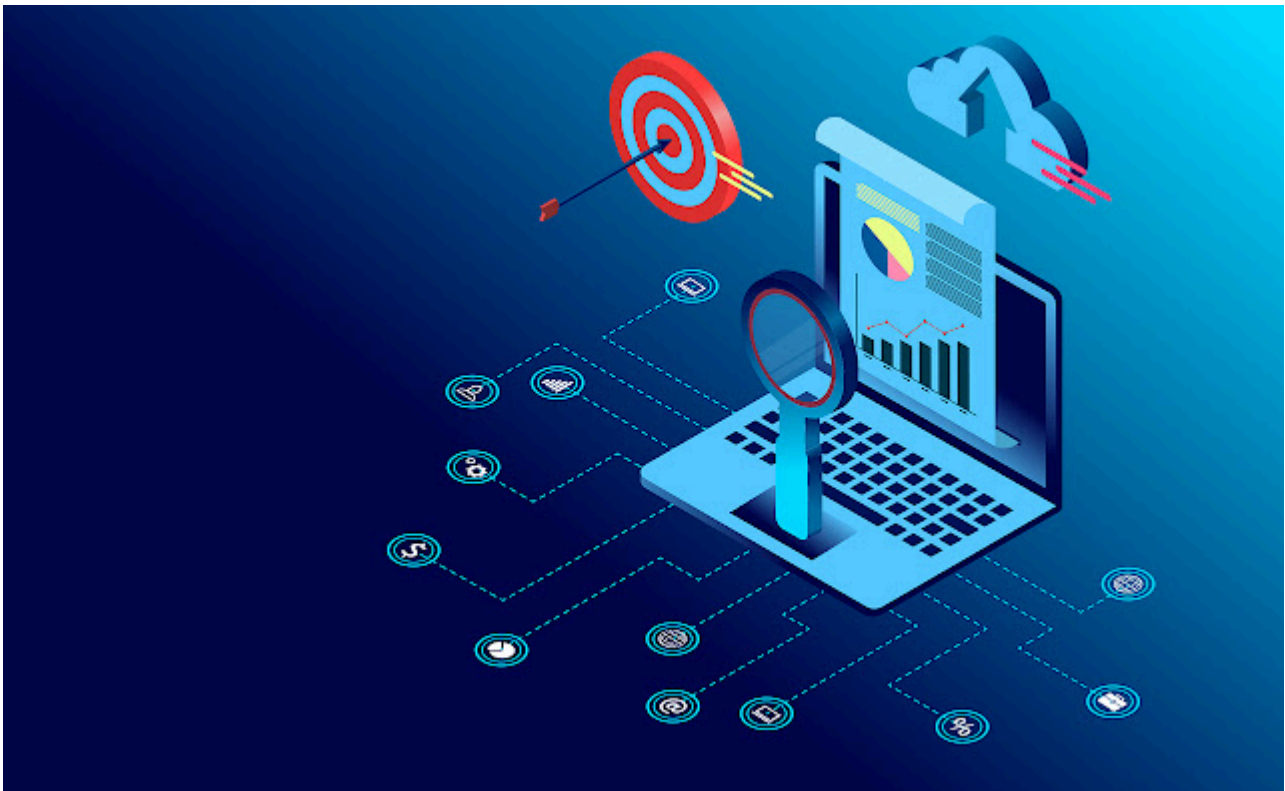


CySecurity News - Latest Information Security and Hacking Incidents: Truist Bank Confirms Data Breach After Information Surfaces on Hacking Forum

By CySecurity News, twitter.com/ehackernews

Archived: 2026-04-05 15:53:32 UTC



Truist Bank, one of the largest commercial banks in the United States, has confirmed a cybersecurity breach after stolen data appeared for sale on a hacking forum. The breach, which occurred in October 2023, was brought to light when a threat actor, identified as Sp1d3r, posted the bank's data online.

Details of the Breach

Headquartered in Charlotte, North Carolina, Truist Bank was formed in December 2019 through the merger of SunTrust Banks and BB&T (Branch Banking and Trust Company). The bank, now with total assets of \$535 billion, offers a variety of financial services, including consumer and small business banking, commercial banking, corporate and investment banking, insurance, wealth management, and payment services.

The breach reportedly involves sensitive information from 65,000 employees, including bank transactions with names, account numbers, balances, and the source code for Truist's Interactive Voice Response (IVR) system. Sp1d3r is attempting to sell this data for \$1 million, according to DarkTower intelligence analyst James Hub, who first spotted the listing.

In a statement, a Truist Bank spokesperson confirmed the October 2023 cybersecurity incident and emphasised that it was swiftly contained. The bank worked with external security consultants to investigate the breach, enhance security measures, and notify affected clients. Initially, only a small number of clients were informed, but additional clients have been notified as the investigation continues to uncover new information.

The spokesperson clarified that this incident is not connected to the ongoing Snowflake attacks, stating, "We have found no evidence of a Snowflake incident at our company." They also noted that Truist Bank regularly collaborates with law enforcement and cybersecurity experts to safeguard its systems and data. To date, there have been no indications of fraud resulting from this breach.

Other Breaches Linked to Sp1d3r

Sp1d3r is also selling data stolen from the cybersecurity firm Cylance for \$750,000. This data reportedly includes 34 million customer and employee emails, along with personally identifiable information. Cylance confirmed that the stolen data is from 2015-2018 and was taken from a third-party platform.

In another incident, Sp1d3r had previously listed 3TB of data stolen from Advance Auto Parts, a provider of automotive aftermarket parts, on the same hacking forum. This data was reportedly taken from Advance's Snowflake account.

The confirmation of Truist Bank's data breach highlights the persistent threat of cyberattacks on major financial institutions. Truist Bank remains committed to securing its systems and protecting client information as investigations continue. In the era of digitalisation it is highly imperative to stay three steps ahead of how technology is being leveraged towards attacking sensitive data and institutional information.

Source: <https://www.cysecurity.news/2024/06/truist-bank-confirms-data-breach-after.html>