Truist Bank confirms breach after stolen data shows up on hacking forum

By **Sergiu Gatlan**

June 13, 2024 07:17 PM 0

Leading U.S. commercial bank Truist confirmed its systems were breached in an October 2023 cyberattack after a threat actor posted some of the company's data for sale on a hacking forum.

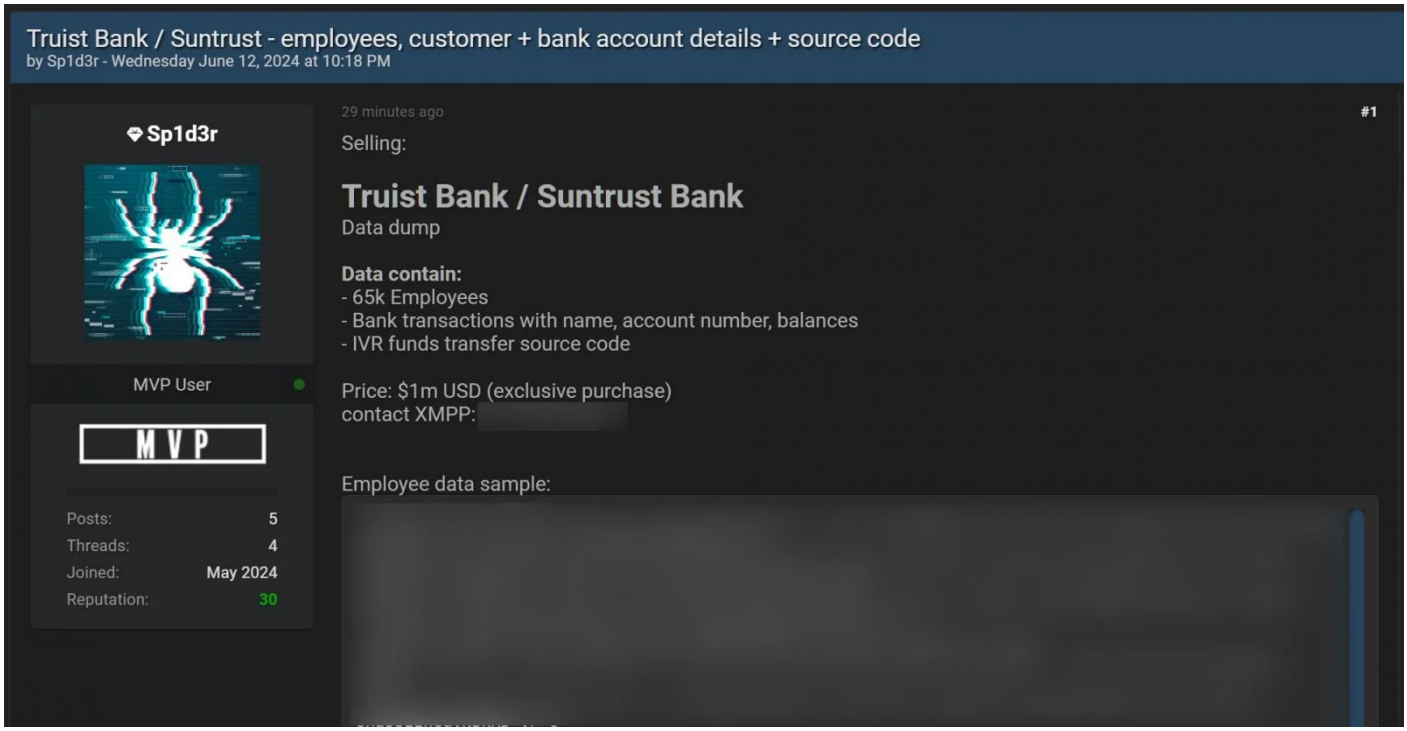
Headquartered in Charlotte, North Carolina, Truist Bank was formed after SunTrust Banks and BB&T (Branch Banking and Trust Company) merged in December 2019.

Now a top-10 commercial bank with total assets of $535 billion, Truist offers a wide range of services, including consumer and small business banking, commercial banking, corporate and investment banking, insurance, wealth management, and payments.

A threat actor (known as Sp1d3r) is selling what they claim is stolen data containing information belonging to 65,000 employees for $1 million, as first spotted

by DarkTower intelligence analyst James Hub.

While BleepingComputer could not independently verify these claims, the data also allegedly contains bank transactions with names, account numbers, balances, and IVR funds transfer source code.



STOLEN TRUIST BANK DATA UP FOR SALE (BLEEPINGCOMPUTER)

"In October 2023, we experienced a cybersecurity incident that was quickly contained," a Truist Bank spokesperson told BleepingComputer when asked to comment on the threat actor's claims.

"In partnership with outside security consultants, we conducted a thorough investigation, took additional measures to secure our systems, and notified a small number of clients last Fall,

When asked if this was connected to the ongoing Snowflake attacks, the spokesperson said, "That incident is not linked to Snowflake. To be clear, we have found no evidence of a Snowflake incident at our company."

"We regularly work with law enforcement and outside cybersecurity experts to help protect our systems and data," the Truist Bank spokesperson added.

"Based on new information from the ongoing investigation of the October 2023 incident, we have notified additional clients. We have found no indication of fraud arising from this incident at this time."

The same threat actor also sells data stolen from cybersecurity company Cylance for $750,000, including databases allegedly containing 34,000,000 customer and employee emails and personally identifiable information belonging to Cylance customers, partners, and employees.

Cylance confirmed the legitimacy of their claims, stating that it's old data (from 2015-2018) stolen from a "third-party platform."

Sp1d3r also previously put up for sale 3TB of data belonging to automotive aftermarket parts provider Advance Auto Parts on the same hacking forum, stolen after breaching Advance's Snowflake account.

BANK | DATA BREACH | SECURITY BREACH | TRUIST BANK

SERGIU GATLAN

Sergiu is a news reporter who has covered the latest cybersecurity and technology developments for over a decade. Email or Twitter DMs for tips.

PREVIOUS ARTICLE

NEXT ARTICLE