Third Flagstar Bank data breach since 2021 affects 800,000 customers

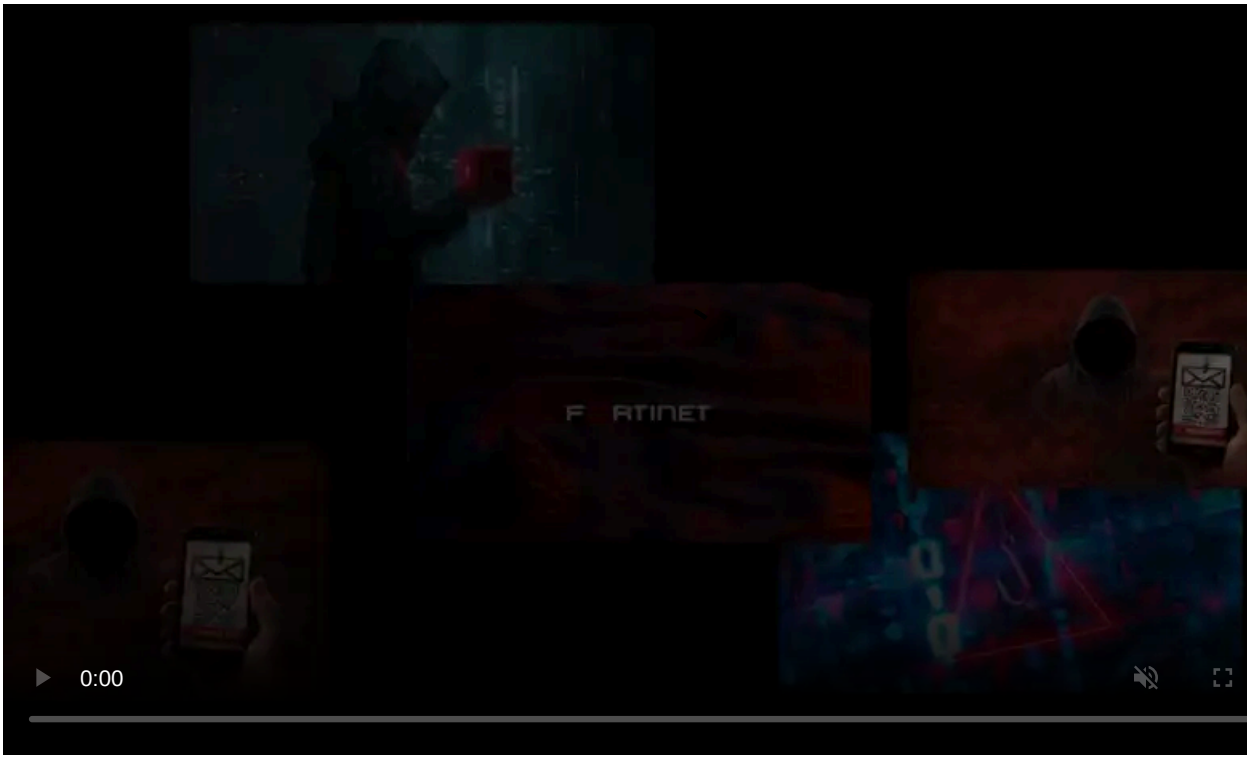
By Bill Toulas

Published: 2023-10-08 · Archived: 2026-04-05 20:28:25 UTC

Flagstar Bank is warning that over 800,000 US customers had their personal information stolen by cybercriminals due to a breach at a third-party service provider.

Flagstar, now owned by the New York Community Bank, is a Michigan-based financial services provider that, before its acquisition last year, was one of the largest banks in the United States, having total assets of over $31 billion.

A data breach notification sent to impacted customers explains that Flagstar was indirectly impacted by Fiserv, a vendor it uses for payment processing and mobile banking services.


F RTINET
0:00

Fiserv was breached in the widespread CLOP MOVEit Transfer data theft attacks that have impacted over 64 million people and two thousand organizations worldwide, according to a report by Emsisoft.

The attackers exploited a zero-day vulnerability in the MOVEit Transfer product to access Fiserv's systems and, from there, stole Flagstar customer data the vendor held to provide services.

The types of data that were compromised are redacted in the sample data breach notification letters. However, the entry on Maine's data breach portal lists at least names and Social Security Numbers (SSNs) as stolen by the threat actors.

The total number of Flagstar Bank customers impacted by this incident is 837,390 in the United States.

A third breach in two years

This latest breach is the third for Flagstar since March 2021, when it disclosed it suffered a breach from the Clop ransomware gang, who, at that time, hacked its Accellion file transfer server in January of that year.

Based on the data samples posted by the ransomware gang, the hackers managed to steal customer and employee information, including names, addresses, phone numbers, tax records, and SSNs.

In June 2022, Flagstar disclosed another breach of its corporate network that impacted over 1.5 million of its customers in the U.S.

The data compromised in that incident includes at least names and Social Security Numbers. At the time, the company opted again to censor the relevant section on the published notification samples.

What is more worrying is that Fiserv offers services to hundreds of banks, which it has indirectly exposed in the past due to other security lapses.

BleepingComputer has contacted Fiserv to ask if the MOVEit breach affects more financial institutions and their customers, and we will update this post as soon as we receive a response.
