Evolve Bank & Trust confirms its data was stolen in cyber attack

June 27 2024, by Teresa Xie, Charles Gorrivan, Bloomberg News

Credit: Pixabay/CC0 Public Domain

Evolve Bank & Trust confirmed it was the victim of a cyber attack and that customer data had been posted on the dark web, less than two weeks after the Arkansas-based lender was ordered by regulators to improve its

risk management and get approval before entering into any new partnerships.

The Russian-linked hacker group LockBit 3.0 on June 25 posted data taken from Evolve's systems after claiming that it had hacked the U.S. Federal Reserve, giving U.S. officials until the afternoon to pay an undisclosed amount in exchange for the information purportedly stolen from the central bank's systems. So far, it does not appear that any sensitive data from the Fed has been released by the group.

A spokesperson for Evolve said in an email that the incident has been contained and the company is currently investigating the situation with "appropriate law enforcement authorities." The bank also said it will offer all affected customers complimentary credit monitoring with identity theft protection services. It's still unclear exactly what information was included in the data, which Evolve said was stolen by a "known cybercriminal organization" without naming LockBit.

The disclosure of the hack follows a June 14 wide-ranging cease-and-desist order issued by the Federal Reserve and the Arkansas State Bank Department to Evolve Bank & Trust and its parent, Evolve Bancorp Inc., after examiners discovered shortcomings in the bank's oversight of partnerships with financial-technology companies and anti-money laundering requirements.

Following the order, a spokesperson for the bank said it had "made significant investments in technology and personnel" to strengthen oversight and "enhance the risk framework," Bloomberg Law reported.

Evolve is best known for its partnerships with fintechs, which rely on traditional institutions to offer bank-like services to customers and recently have fallen under closer scrutiny by regulators. West Memphis, Arkansas-based Evolve works with popular fintechs including Affirm

Holdings Inc., Marqeta Inc., Dave Inc. and others.

Evolve was one of four banks that teamed up with Synapse Financial Technologies Inc., the Andreessen Horowitz-backed fintech that filed for bankruptcy protection in April. Synapse, a "banking as a service" provider that worked as a middleman between banks and fintechs, partnered with approximately 100 fintechs covering around 10 million customers, according to bankruptcy court filings.

Jelena McWilliams, the former Federal Deposit Insurance Corp. chairman serving as the bankruptcy trustee, estimated that the shortfall in end-user funds ranges between $65 million and $95 million, according to a June 13 status report filed with the bankruptcy court.

Lockbit 3.0, the hacking group behind the Evolve leak, functions as a ransomware-as-a-service gang, in which members lease their technical tools to affiliates and demand a cut of any extortion payments.

The group posted the Evolve information on a darkweb forum tied to Lockbit, a prolific ransomware gang that has received millions of dollars in payments following attacks on thousands of victims, including the Industrial & Commercial Bank of China Ltd., Boeing Co and the UK's Royal Mail. By 2022, the group had rebranded itself as LockBit 3.0.

In February, law enforcement agencies from 11 countries—led by the UK's National Crime Agency and aided by the U.S. Federal Bureau of Investigations—seized LockBit's technical tools in an operation that targeted its malware deployment system. But the group's hacking tools have remained widely used since they were leaked to the public in 2022, and members of the group are believed to remain active.

The release of the Evolve data on the LockBit website suggests some of the group's core actors could have been behind the hack, said Brett

Callow, a threat researcher at the cybersecurity firm Emsisoft. Still, the lack of a release of genuine Fed data suggests that the group is "dead in the water," Callow added.

"The Fed claim was really a desperate play to stay relevant," he said.