Financial Breach Exposes 40,000 Unencrypted Customer Records

December 5, 2017

(TNS) — TAMPA, Fla. — A Tampa-based financial company that caters to consumers with damaged credit exposed 40,000 customers' extremely sensitive personal data. The National Credit Federation's data exposure was discovered by security research firm UpGuard, which recently published a report on the incident.

"These are agencies that we are trusting to take care of our credit and information," Sri Sridharan, executive director of the Florida Center for Cybersecurity in Tampa, said. "That they are so careless about it is appalling."

NCF is a credit repair company that disputes incorrect or "misleading" items on its customers' credit reports to build customers' financial standing over time. It operates around the country.

"Our mission is to help people who are currently in or have successfully come through a financial crisis take back control of their finances and credit," the firm's website says.

NCF did not return requests for comment for this article. However, the URL was disabled, according to California-based UpGuard, which found the exposed data in early October. The URL was not indexed by search engines.

It includes some of the most sensitive personal information: names, addresses, dates of birth, images of driver's licenses and social security cards, full credit card numbers, full bank account numbers, credit reports from all three major agencies and detailed financial histories.

"There really is no other information that is more sensitive in terms of what it can do in dollars-and-cents damage to people," said Joseph Jerome, policy counsel at the Center for Democracy and Technology. Jerome specializes in privacy and data.

In the wrong hands, that information could be used to empty bank accounts, file fake tax returns, take out mortgages, buy big-ticket items and steal identities.

As far as the researchers know, the data does not appear to have been used maliciously yet.

"Fortunately — hopefully — I think we were the first ones to find it," said Dan O'Sullivan, analyst with UpGuard's cyber risk team.

The issue, he said, arose when the method for accessing the information was changed.

The server with the affected data is password-protected by default, O'Sullivan said. But someone turned off that feature and enabled the data to be accessed by a URL, meaning anyone who had the URL could see the data.

"You have to take an affirmative action to change it," O'S ullivan said, as opposed to changing access by accident.

It is unclear how long the data was exposed for.

Compounding the issue is that the data was in plain text, not encrypted. Typically, sensitive data is protected by encryption, which "scrambles" the data so it can't be understood by someone who shouldn't have access to it. Because this information was not encrypted, anyone who accessed the URL could read NCF customer data the same way that you are reading this sentence.

When UpGuard found the data, it was still being updated with new customer information.

"(A criminal could have) sat there and watched it and had a constantly-refreshing source for identity theft and fraud," O'S ullivan said.

The breach comes just months after Equifax, a major credit reporting agency, announced that data for 143 million customers was stolen.

For customers affected by the NCF incident, the outlook is somewhat grim. While it's good news that the data does not appear to have been accessed, that's not a guarantee.

"In my estimation, (the exposure) is very bad especially when we consider that these people already have financial difficulties and were put in a position of being victimized again," O'S ullivan said.

It is unclear if affected customers have been notified about the breach. Experts suggest NCF customers freeze their credit and monitor their bank accounts.