Lakeview Loan Servicing Faces Multiple Lawsuits Over Data Breach

Katie Jensen
MAY 26, 2022

At least a dozen civil lawsuits have been filed against the company, all seeking class-action status.

Florida-based Lakeview Loan Servicing LLC, the fourth largest loan-servicing company in the nation, is facing at least two proposed class action lawsuits as a result of a late-2021 data breach that reportedly affected more than 2.5 million consumers.

At least a dozen civil lawsuits have been filed against the company, all seeking class-action status. These lawsuits have been consolidated in federal court in Florida, although one South Carolina case is still pending separately.

The lawsuits claim that, because of the data breach, class members suffered ascertainable losses, including out-of-pocket expenses and time incurred to remedy or mitigate the effects of the attack. Those affected also face substantial risk of having their personal information compromised, including their name, address, loan number, and Social Security number.

The data breach occurred from Oct. 27 through Dec. 7, 2021, yet Lakeview did determine what information was accessed until Jan. 31, 2022. Lakeview is also accused of sitting on information about the breach for over a month, failing to notify the affected consumers until March 18, 2022. Not only had Lakeview exposed its customers to a heightened risk of

identity theft and fraud, it made matters worse by delaying to notify victims, the lawsuit claims.

“Every moment is precious to ensure that that data is not then weaponized against the rightful owner of that data through identity theft,” the lawsuit filed by Andrew Guarino states. “Sitting on this information allowed Lakeview to dodge responsibility and inevitably worsened the Data Breach victims’ chances at weathering the storm that Lakeview created.”

Class members may incur out-of-pocket costs through having to purchase credit monitoring systems, credit freezes, or other protective measures to deter and detect identity theft, the suits claim. Class members are seeking compensatory damages, reimbursement for out-of-pocket expenses, and injunctive relief including improvements to Lakeview data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the company itself.

Despite Lakeview’s responsibility to safeguard customers’ private information, the company is accused of failing to properly encrypt its data or otherwise protect its systems and files from unauthorized access.

One particular lawsuit filed by Jennifer Morril claims that exposed personal information is already listed for sale on the "dark web." “Plaintiff and Class Members have already been the victims of actual fraud perpetrated with the PII stolen from Defendant, and face a present and immediate lifetime risk of identity theft, which is heightened here by the loss of their birthdates and Social Security numbers,” Morril claims.

“Numerous sources cite dark web pricing for stolen identity credentials,” the lawsuit continues. “For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. Criminals can also purchase access to entire company data breaches from $900 to $4,500.”

A dishonest person who has your Social Security number can use it to get other personal information about you, Morril’s lawsuit explains. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don’t pay the bills, it damages your credit. You may not find out that someone is using your number until you’re turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems overall.

Some law enforcement officials say that stolen data may be held for up to a year or more before being used to commit identity theft. Once stolen data have been sold or posted on the internet, fraudulent use of that information may continue for years. For that reason, it is difficult to measure the resulting harm from data breaches.

As the fourth-largest servicer in the industry, Lakeview controls 4.6% of all agency loans being serviced with a $374.8 billion portfolio based on total unpaid-principal loan balance, according to a report from Recursion.

Although the amount in compensatory damages has yet to be defined, Lakeview likely will have to pay a hefty bill because the class action involves more than 100 class members and the amount in controversy exceeds $5 million, exclusive of interest and costs.

Nearly all cases were filed in U.S. District Court in Miami, with one outlier filed in U.S. District Court in South Carolina in Spartanburg. However, there is a pending motion filed by Lakeview to consolidate the case with the master case now pending in federal court in Miami.