Texas sues PowerSchool over breach exposing 62M students, 880k Texan

Data: 2025-09-04 18:05:13

Autor: Inteligência Against Invaders

Texas Attorney General Ken Paxton has filed a lawsuit against education software company PowerSchool, which suffered a massive data breach in December that exposed the personal information of62 million students, including over880,000 Texans.

PowerSchool is a cloud-based software solutions provider for K-12 schools and districts, with more than 18,000 customers and supporting over 60 million students worldwide.

In January, the education software giant disclosed that its PowerSource customer support portal was breached on December 19, 2024, using a subcontractor's stolen credentials. The attacker demanded a $2.85 million ransom in Bitcoin on December 28, 2024, after stealing the full names, physical addresses, phone numbers, passwords, parent information, contact details, Social Security numbers, and medical data of impacted students and faculty.

As BleepingComputer first reported, the threat actor behind the December 2024 PowerSchool breach claimed to have stolen the personal data of 62.4 million students and 9.5 million teachers from 6,505 school districts across the U.S., Canada, and other countries.

“PowerSchool's failures violate both the Texas Deceptive Trade Practices Act and the Identity Theft Enforcement and Protection Act by misleading customers about its security practices and failing to take reasonable measures to protect sensitive information entrusted by Texas families and school districts,” the Office of the Attorney General of Texas said.

“If Big Tech thinks they can profit off managing children's data while cutting corners on security, they are dead wrong. Parents should never have to worry that the information they provide to enroll their children in school could be stolen and misused. My office will do everything we can to hold PowerSchool accountable for putting Texas students, teachers, and families at risk,” Attorney General Paxton added on Wednesday.

Attacker extorts schools, pleads guilty

In a private FAQ shared with customers and reviewed by BleepingComputer at the time, PowerSchool acknowledged that it had made a ransom payment to stop the data from being disclosed and received a video from the attacker claiming that the stolen data had been erased.

However, the threat actor did not keep their promise, as it began individually extorting school districts in early May, threatening to release the previously stolen student and teacher data if a ransom was not paid.

Later that month, 19-year-old college student Matthew D. Lane from Worcester, Massachusetts, pleaded guilty to orchestrating the massive cyberattack on PowerSchool with the help of several other conspirators and attempting to extort millions of dollars in exchange for not leaking the stolen data of millions.

According to school notices and a DataBreaches.net report, the ransom demands sent to school districts claimed to be from ShinyHunters, a high-profile group of threat actors linked to a wide range of breaches that had impacted hundreds of millions of people.

In March, PowerSchool also published a CrowdStrike investigation into the incident, which revealed that threat actors had also breached PowerSource in August and September 2024, using the same compromised credentials. However, the cybersecurity company was unable to find evidence that the same attacker was responsible for all three breaches.

[IMAGEM REMOVIDA]