

Data Privacy Event

Sprouse Shrader Smith PLLC (“Sprouse Shrader Smith”) is reaching out to individuals regarding a recent event. Sprouse Shrader Smith identified unusual activity within its systems and immediately took steps to protect its digital environment. At this time, there is no indication that any data about individuals has been or will be misused. Safeguarding details belonging to those we serve is important to us, and we sincerely apologize for any inconvenience this may cause.

On or around February 25, 2025, Sprouse Shrader Smith discovered unusual activity involving its systems. We disconnected the systems, informed the FBI and local authorities, and engaged independent specialists to assist with an investigation. The review determined that documents containing a limited amount of information about individuals may have been copied from the network during the event. We worked with a vendor to identify and extract any details contained in the impacted documents. This process was completed on December 29, 2025.

Based on the review, the files may have included individuals’ names, and some combination of the following data elements: addresses, dates of birth, Social Security numbers, driver or state license numbers, governmental identification numbers, financial account numbers, payment card numbers, taxpayer ID numbers, health insurance policy numbers, and medical information.

We have taken steps to prevent this kind of event in the future, including changing all passwords, adding additional endpoint monitoring tools, and implementing further safeguards to strengthen their systems.

Letters were mailed to individuals for whom we have addresses. These letters contain details about the event as well as instructions for enrolling in credit monitoring and identity protection services through IDX.

Impacted individuals should be vigilant for the next 12 to 24 months and review credit reports, bank accounts and other financial statements, and immediately contact their financial institution if they identify suspicious activity.

Individuals may call 1-844-848-1317 between 8 am to 8 pm Eastern Standard Time Monday through Friday with any questions. Protecting data entrusted to us remains a top priority, and we sincerely apologize for any concern this event may cause.