

Melissa Ventrone
T (312) 360-2506
Email: mventrone@clarkhill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

March 10, 2026

VIA PORTAL SUBMISSION

Office of the Attorney General
1445 K St
Lincoln, NE 68508

Dear Attorney General Hilgers:

We represent Sprouse Shrader Smith PLLC (“Sprouse Shrader Smith”) with respect to a data security incident involving personal information as described below. Sprouse Shrader Smith takes the security of the information in its control seriously and is committed to answering any questions you may have regarding this event.

1. Nature of security incident

On or around February 25, 2025, Sprouse Shrader Smith discovered suspicious activity associated with its network. Sprouse Shrader Smith immediately disconnected its systems, notified the FBI and local law enforcement, and engaged independent cybersecurity specialists to assist. The investigation found that documents containing a limited amount of personal information may have been copied from Sprouse Shrader Smith’s network during the incident. Sprouse Shrader Smith worked with a vendor to identify and extract any personal information present in the impacted documents. Because of the complexity of the documents, this process took time and was completed on December 29, 2025.

Impacted information may include names, and some combination of addresses, Social Security numbers, driver’s license or state ID numbers, government identification numbers, passport numbers, financial account information, payment card numbers, medical information, and health insurance policy information.

2. Number of Nebraska residents affected

Fifteen (15) residents of Nebraska were notified of the incident. Notification letters were sent to potentially affected individuals on March 10, 2026. A copy of the notification letter is attached as Exhibit A.

3. Steps taken in response to the incident

In response to the incident, Sprouse Shrader Smith changed all passwords, added additional endpoint monitoring software, and implemented additional security controls to further enhance the security of its network. Additionally, affected individuals were offered 12 months of credit monitoring and identity protection services through IDX.

4. Contact information

Sprouse Shrader Smith takes the security of the information in its control seriously. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,

CLARK HILL

Melissa Ventrone
Member

cc: Sunaina Ramesh – sramesh@clarkhill.com



P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

Enrollment Deadline: June 10, 2026

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

March 10, 2026

NOTICE OF DATA <<Variable Header: BREACH/SECURITY INCIDENT>>

Dear <<First Name>> <<Last Name>>,

We wanted to let you know of a data security incident that may have impacted some of your personal information. Sprouse Shrader Smith PLLC (“Sprouse Shrader”) is a law firm and may have received your personal information in connection with legal services provided to individuals or businesses. This letter contains information about steps you can take to protect your information, and resources we are making available to you.

What Happened?

On or around February 25, 2025, we discovered suspicious activity associated with our network. We immediately disconnected our systems, notified the FBI and local law enforcement, and engaged independent cybersecurity specialists to assist. The investigation found that documents containing a limited amount of personal information may have been copied from Sprouse Shrader’s network during the incident. We worked with a vendor to identify and extract any personal information present in the impacted documents. This process was completed on December 29, 2025.

What Information Was Involved?

From our review, it appears your name, <<Variable Text 1>> may have been affected.

What We Are Doing:

We have taken steps to prevent this kind of event in the future, including changing all passwords, adding additional endpoint monitoring software, and implementing additional security controls to further enhance the security of our network. In addition, while we are not aware of any misuse of your personal information, we have arranged for you to receive credit monitoring and identity protection services at no cost to you through IDX for <<12/24>> months.

What You Can Do:

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-844-848-1317, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am – 8 pm Central Time, excluding holidays.

Again, at this time, there is no evidence that any personal information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer

questions or concerns you may have regarding protection of your information. We also encourage you to remain vigilant against incidents of identity theft by reviewing bank accounts and other financial statements.

For More Information:

If you have questions regarding the incident, please call 1-844-848-1317 Monday through Friday, 8 am – 8 pm Central Standard Time. Protecting your information is important to us, and we sincerely apologize for any inconvenience this may cause you.

Sincerely,

Sprouse Shrader Smith PLLC

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is June 10, 2026.

2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

3. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia Residents: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, Iowa 50319; 515-281-5926; consumer@ag.iowa.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 1024 Capitol Center Drive, Suite 200 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, <https://oag.maryland.gov>, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.