HALVORSEN
FAMILY LAW GROUP

250 Executive Park Blvd.
Suite 150
Winston-Salem, North Carolina 27103
phone 336.760.8500
fax 336.760.8585

Deborah S. Halvorsen
Board Certified Specialist in Family Law

Mary Beth Davis
Associate Attorney

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

October _____, 2025

Notice of Data Breach

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

We are writing to provide you with information regarding an incident that may have exposed information maintained about you by Halvorsen Law Group, PLLC, doing business as Halvorsen Family Law Group (the "Firm").

We assure you that client confidentiality and the security of the information we maintain is of upmost importance to us, and we want you to know that we take seriously the responsibility to protect that information. We sincerely regret that this incident occurred, and we apologize for any inconvenience it may have caused you. Please review the rest of this letter for details about the incident and our response.

What Happened

On July 14, 2025, the Firm was contacted by a third-party who claimed to have infiltrated the Firm's systems and stolen data. A subsequent investigation, with assistance from our outside information technology ("IT") support team and additional cybersecurity professionals, has confirmed that certain portions of the Firm's systems were compromised on July 6, 2025.

What Information Was Involved

As part of our investigation, we were able to obtain a list of files the cybercriminal claims to have stolen. Our review of these files, most of which contain unstructured data, is ongoing. ***At this time, we do not have any knowledge that your personal information contained in these files has been misused.*** Out of an abundance of caution, however, we are notifying persons whose information was exposed on a rolling basis so that you can take steps to protect your information, if you feel it is appropriate to do so.

We receive and maintain a variety of information about our clients and other persons involved in the matters we work on for our clients. The types of personal information that we maintain in our files that has been exposed through this incident could include: name; Social Security Number; passport information, driver's license or other state identification number; date of birth; address; protected health information; and, in some clients' cases, payment and other financial account information.

What We Are Doing

The Firm has taken steps to address the threat, including by notifying and working with the Firm's outside IT support to mitigate the impact and to limit any further outside access to Firm data. In addition to working with IT support, we have engaged cybersecurity professionals experienced in handling these types of incidents to assist us with our response and to assess the full scope of information impacted. This is an ongoing process. We have also notified and are cooperating with state regulators and law enforcement in connection with this incident.

The Firm is committed to maintaining the privacy and confidentiality of the information we maintain, and we have taken precautions to safeguard it. We continue to work with cybersecurity professionals to evaluate and modify our practices and internal controls to enhance the security and privacy of the information we maintain.

What You Can Do

The enclosed "Further Information" document provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for suspicious activity and to detect errors.

Notice to Opposing Parties

Please note that the Firm will be giving notice to opposing parties whose information may have been exposed through this incident. Though these other individuals are not our clients, state law requires us to provide notice to persons whose personally identifiable information was affected. In some instances, notice will be accomplished through outreach to an opposing party's attorney of record.

For More Information

If you have questions that are not answered by this letter or the enclosed information, you may contact us between 9 AM and 4:30 PM ET, Monday – Friday, excluding holidays. Please feel free to contact us as you normally would with those questions at 336-760-8500 extension 310.

Sincerely,

Halvorsen Law Group, PLLC

_____

Deborah S. Halvorsen (Enclosure)

FURTHER INFORMATION TO HELP PROTECT YOUR PRIVACY

Place a fraud alert on your credit report. You have the option of placing a fraud alert on your credit report. A fraud alert is free of charge and easy to place. You may contact toll-free any one of the three major credit bureaus listed below. As soon as one bureau confirms your report, the others are simultaneously notified on your behalf.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

Obtain a copy of your free credit report. You may also obtain a free copy of your credit report from each of the three major credit reporting bureaus once every 12 months by visiting www.annualcreditreport.com, calling toll-free (877) 322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, Georgia 30348. It is recommended that you monitor your free credit reports for incidents of fraud and identity theft. You may purchase a copy of your credit report by contacting one of the three major credit reporting bureaus above.

Place a 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.

Review your account statements and monitor credit reports. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing your financial account statements and monitoring your free credit reports for unauthorized access. Doing so can help you spot problems and address them quickly.

Notify law enforcement of any suspicious activity. You should also notify the appropriate law enforcement authorities, your state attorney general, and/or the U.S. Federal Trade Commission (FTC) of any suspected identity theft.

Federal and State resources to protect against identity theft. You can find additional information to help protect yourself from identity theft, including information about fraud alerts and credit report security freezes, by contacting one of the three major credit bureaus listed above, or by visiting the FTC's website at www.ftc.gov/idtheft, by calling 1-877-ID-THEFT (1-877-438-4338), or by writing to the Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580. You may also wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov, by calling (877) 566-7226, or by writing to the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699.

The Following 2 Pages are Attachment 1 to Notice Form

(Note, this portion will not appear with notification letter. The following two pages are only to provide additional information to the online form.)

NEBRASKA SECURITY BREACH REPORTING FORM
PURSUANT TO THE NEBRASKS FINANCIAL DATA PROTECTOIN AND CONSUMER NOTIFICATION OF DATA SECURITY BREACH ACT OF 2006
(Neb. Rev. Stat. § 87-801 *et seq.*)

ATTACHMENT 1

Halvorsen Law Group, PLLC

***

This attachment provides additional details relating to a data breach in which a third-party gained unauthorized access to the computer systems of the small family law firm Halvorsen Law Group, PLLC, doing business as Halvorsen Family Law Group (the "Firm"). The Firm, consisting of two attorneys and a small support staff, is located in Winston-Salem, North Carolina.

This incident stems from a cyber-attack perpetrated against the Firm. On July 14, 2025, the Firm was contacted by a third-party who claimed to have infiltrated the Firm's systems and stolen data. A subsequent investigation, with assistance from the Firm's outside information technology ("IT") support team and additional cybersecurity professionals, confirmed that certain Firm systems were compromised on July 6, 2025.

After the Firm learned that its systems had been compromised, it took immediate steps to mitigate the exposure, including by wiping and rebuilding all desktop computers, isolating its servers, and engaging cybersecurity professionals to assist the Firm's existing IT contractors in securing Firm systems. The Firm has taken other steps to mitigate the risk of further exposure beyond the initial access and theft of data.

While system restoration was ongoing, the Firm undertook an investigation to assess the full scope of information impacted. On September 9, 2025, with the assistance of cybersecurity professionals, the Firm was able to complete a review of exposed files and identify affected persons. The review of the materials was cumbersome because much of the exposed data existed in scanned images of documents that could not be easily searched. On September 9, it was determined that one (1) Nebraska resident had been affected.

The Firm is cooperating with law enforcement in the investigation of this attack. The Firm notified the Federal Bureau of Investigation on July 14, 2025.

Prior to the incident, the Firm utilized updated anti-virus software, multi-factor authentication, EDR protection, a VPN, firewall protection, and other measures.

The Firm has also taken the following steps to further strengthen its cyber defenses:

- Reviewed and updated existing security practices, including with respect to access to Firm systems;
- Moved all client files to a cloud-based platform;
- Engaged trusted cybersecurity professionals to further strengthen Firm IT systems; and
- Changed storage and access procedures for closed client files.

This is an ongoing process and, moving forward, the Firm will work with trusted third-party IT providers and cybersecurity professionals to implement additional technical security measures and will redouble its efforts to train employees in cybersecurity best practices.

If you have any other questions or need additional information, please contact:

Will Quick, Esq.
Brooks, Pierce, McLendon,
Humphrey & Leonard, LLP
150 Fayetteville Street
1700 Wells Fargo Capitol Center
Raleigh, NC 27601
(919) 839-0300
E-mail: wquick@brookspierce.com