Daniels Law Group, LLC
c/o Cyberscout
<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<FirstName>> <<LastName>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<PostalCode+4>>

<<Date>>

NOTICE OF DATA BREACH

Dear <FirstName> <LastName>,

We write to inform you of a recent incident that may have affected personal data about you and/or your minor child(ren) held by our firm. We take the security of your personal information very seriously. This letter provides details of the incident, our response, and steps you may take to better protect against the possible misuse of your information and that of your minor child(ren) if you feel it is appropriate to do so.

WHAT HAPPENED?

We recently learned that on or before July 1, 2025, an unidentified individual or group used illegal methods to gain unauthorized access to our firm's file servers. We took immediate steps to eliminate the unauthorized access and retore security to our system, to engage counsel, to report the incident to law enforcement, and to hire third-party forensics consultants to investigate and resolve this incident. A few days later, on July 9th, we determined that some of your family's personal information was likely contained in the potentially affected data. In an abundance of caution, we are reaching out both to notify you that this happened and to offer credit and identity monitoring services.

WHAT WE ARE DOING.

To date we have spent countless hours working with experts to ensure appropriate security, mitigate risk, and to protect ourselves from further unauthorized access, including implementing additional security measures to help prevent a similar incident from occurring in the future. In addition, we are offering identity theft protection services and online identity monitoring through Cyberscout, a TransUnion company. These identity protection services include:

- **For adults only**, **Credit Monitoring Services**. These services provide you with **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for <<service length>> from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.
    - **Signup Instructions**: Your code to enroll in these services is <<unique code>>. The enrollment requires an internet connection and email account. You may be asked to verify personal information for your own protection to confirm your identity. ***Note****: See instructions for children in next paragraph.*

- **For minors only**, **Cyber Monitoring services.** If our files had information about your minor children, we are offering Cyber Monitoring services for you and your minor child for <<service length>> at no charge. Cyber monitoring will look out for your and your child's personal data on the Internet and alert you if your personally identifiable information or your child's is found online.
    - **Signup Instructions**: **After enrolling the adult,** enroll the minor children with the codes provided below using a **different email address** than the one used for the parent.
    - Once you have enrolled yourself, click on your name in the top right of your dashboard and select "**Manage Account**," then choose "**Family Protection**," and finally "**Add Family Member**" to enroll your child. The code(s) to enroll your children (if applicable to you) are:

<<minor name-1>> <<menrollment code-1>>

<<minor name-2>>	<<menrollment code-2>>
<<minor name-3>>	<<menrollment code-3>>
<<minor name-4>>	<<menrollment code-4>>

***Note**: Children must be registered with **one email address** different from the email used for the adult.*

***Note also**: Children who were minors at the time of service who are now over 18 will receive a **separate notification letter** with their own enrollment code.*

These services provide proactive fraud assistance to help with any questions that you might have or in the event you become a victim of fraud. With this protection, Transunion will help you quickly resolve issues if your identity is compromised. Due to privacy laws, we cannot enroll you into these services directly; you must enroll yourself if you wish to take advantage of this complimentary service. Enrolled individuals will also have access to $1,000,000 in insurance coverage to protect against potential damages related to identity theft and fraud, including identity theft expenses as well as unauthorized electronic fund transfer fraud.

WHAT INFORMATION WAS INVOLVED?

We believe these attackers accessed and may have acquired personal data belonging to you and or/your family members or loved ones. The information affected varies by individual, but for most individuals the information that may have been compromised includes specifically:

- All information provided to us by you directly or on your behalf, by the opposing party or attorney and/or your legal guardians, to include <<data elements>>.

To our knowledge, there has been no misuse of any information as a result of the incident, and we are taking a number of precautionary measures to protect your data and ensure that it is not misused. While it is impossible to guarantee that something like this would never happen in the future, we are doing everything that we can.

WHAT YOU CAN DO.

We encourage you to enroll in the free identity protection services by going to **https://bfs.cyberscout.com/activate** and entering your enrollment code(s). Please note the deadline to enroll is **90 days from the date of this letter**. Representatives are available at 1-833-397-9403 Monday through Friday from 8:00 am – 8:00 pm Eastern Time for enrollment support only. Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

There is also more information in the attachment about placing a fraud alert and/or credit freeze. In addition, even if you choose not to use these services, we are strongly urging all parents to contact the credit bureaus and ensure that no credit file exists in the name of your minor child(ren).

FOR MORE INFORMATION.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code when calling or enrolling online, so please do not discard this letter.

WHAT IF I HAVE OTHER QUESTIONS ABOUT THIS INCIDENT NOT ABOUT THE IDENTITY PRTOECTION SERVICES?

We are available to speak with you and address any questions you have during normal business hours. Please call our regular office number if you'd like to speak with us.

We take our responsibilities to protect your personal information very seriously and thank you for your understanding.

Sincerely,
Daniels Law Group, LLC

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to **https://bfs.cyberscout.com/activate** and follow the instructions for enrollment using your Enrollment Code provided.

2. Activate the credit monitoring provided as part of your identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, representatives will be able to assist you.

3. 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.

If you discover any suspicious items and have enrolled in identity protection, notify TransUnion immediately by calling or by logging into the website and filing a request for help.

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.

4. 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
Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Transunion Credit Freeze P.O. Box 160 Woodlyn, PA 19094

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.

5. 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.

6. 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. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Colorado Residents: You can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

District of Columbia Residents: You can obtain information about steps to take to avoid identity theft from the Federal Trade Commission (contact information above) and The District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, https://oag.dc.gov/, (202) 737-3400.

Illinois Residents: You can obtain information from the credit reporting agencies and the Federal Trade Commission about fraud alerts and security freezes (contact information above). You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, 1-800-964-3013.
https://illinoisattorneygeneral.gov/about/email_ag.jsp,

Kentucky Residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

Massachusetts Residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

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: Information regarding security breach response and identity theft prevention and protection is available from the FTC (information below) and the Office of the New York 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

Pennsylvania Residents: You may contact the Pennsylvania Office of the Attorney General, Bureau of Consumer Protection, 15th Floor, Strawberry Square, Harrisburg, PA 17120, www.attorneygeneral.gov, 1-800-441-2555.

Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800-621-0508. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

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