Richard Halm
T (312)985-5564
F (312) 517-7572
Email: rhalm@ClarkHill.com

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

May 29, 2025

Via Portal

Nebraska Attorney General
2115 State Capitol
Lincoln, NE 68509

Dear Attorney General Hilgers,

We represent Gleason, Flynn, Emig, and McAfee, Chartered ("GFEM") with respect to a data security incident involving the potential exposure of certain personally identifiable information described in more detail below. GFEM is a law firm located in Rockville, Maryland. GFEM is committed to answering any questions you may have about the data security incident, the response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On October 31, 2024, GFEM discovered suspicious activity on its computer systems. GFEM immediately implemented its incident response protocols and began an internal investigation. External computer forensic specialists were engaged to help determine what occurred and whether any information was at risk. On December 13, 2024, the forensic investigation determined some files from its network may have been accessed by an unauthorized actor during this incident. A third party was engaged to review the files and determine the individuals and data elements potentially impacted. This review was completed on May 8, 2025. Potentially impacted information may include name, address, Social Security number, passport number, driver's license number, financial account information, health insurance information, and medical information.

2. Number of residents affected.

Three (3) Nebraska residents were notified of the incident. A notification letter was sent to the potentially affected individuals on May 29, 2025 (a copy of the form notification letter is enclosed as Exhibit A).

3. Steps taken in response to the incident.

GFEM took steps to address this incident and prevent similar incidents in the future. GFEM changed all passwords and deployed enhanced endpoint monitoring software. The FBI was also notified of this incident. Additionally, affected individuals were offered 12 months of credit monitoring and identity protection services through Cyberscout, a TransUnion company.

4. Contact information.

GFEM takes the security of the information in its control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at rhalm@clarkhill.com or (312) 985-5564.

Sincerely,

CLARK HILL

Richard Halm

Richard Halm
Senior Attorney

cc: Mariah Leffingwell – mleffingwell@clarkhill.com

Gleason, Flynn, Emig & McAfee, Chartered
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

GLEASON FLYNN EMIG & McAFEE
ATTORNEYS AT LAW

[redacted]

0000101026G0500

P

May 29, 2025

Notice of Data Security Incident

Dear [redacted]

We wanted to let you know about a data security incident that may have impacted your personal information. Gleason, Flynn, Emig, and McAfee, Chartered ("GFEM") may have been provided your information in the course of its representation of clients in the defense of an actual or threatened lawsuit. We take the privacy and security of your information seriously and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

What Happened?

On October 31, 2024, we discovered suspicious activity on our computer systems. We immediately implemented our incident response protocols and took systems offline. External computer forensic experts were engaged to assist with the investigation. The investigation helped us determine what occurred and whether any information was at risk. On December 13, 2024, the forensic investigation determined some files from our network may have been accessed by an unauthorized actor during this incident. A third party was engaged to review the files and determine the individuals and data elements potentially impacted. On May 8, 2025, this process determined that some of your personal information may have been impacted. We wanted to inform you of this incident and provide you with resources to protect your information.

What Information Was Involved?

The potentially impacted information includes your name, address, and the following data elements: Social Security number, financial account number, username and access information for a non-financial account, individual health insurance policy number and medical condition or treatment information.

What We Are Doing:

We have taken steps to prevent a similar incident from happening in the future. In addition, we are offering identity theft protection services through Transunion. In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 12 months 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do:

Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information:

If you have any questions or concerns, please call **833-998-8439** Monday through Friday from 8 am - 8 pm Eastern Time, excluding holidays or go to https://bfs.cyberscout.com/activate.Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Gleason, Flynn, Emig, and McAfee, Chartered

Recommended Steps to Help Protect Your Information

1. Website and Enrollment.

You can enroll in the complimentary credit monitoring services being offered to you by logging on to https://bfs.cyberscout.com/activate and following the provided instructions. When prompted, please provide the following unique code: [redacted] The enrollment requires an internet connection and email account and may not be available to minors. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	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.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 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, www.oag.state.md.us/Consumer, 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.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. A total of 11 Rhode Island residents were notified of this incident.

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.