



Freeman
Mathis & Gary ^{LLP}

1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009

www.fmglaw.com

Nicholas Jajko
Partner
D: 215.279.8070
nicholas.jajko@fmglaw.com

August 16, 2024

Via E-Mail ONLY

Maryland Office of the Attorney General

Attn: Security Breach Notification

Email: Idtheft@oag.state.md.us

RE: Sharp Law, LLP- Notice of Data Event

Dear Sir or Madam:

We represent Sharp Law, LLP ("Sharp Law"), a plaintiffs class action law firm based in Prairie Village, KS. This submission is provided pursuant to the Maryland Personal Information Protection Act, MD. CODE. ANN. COM. LAW §14-3501, *et seq* which requires notice to your office in the event of a breach in the security of personal information affecting residents of the State of Maryland.

In February 2024, Sharp Law identified unusual activity within an employee email account. Upon identifying the activity, Sharp Law immediately secured the accounts and partnered with computer forensic specialists to conduct a thorough investigation. While the investigation could not confirm with certainty whether any emails or attachments were accessed, Sharp Law learned the unauthorized user had access to the accounts between November 6, 2023 and February 19, 2024. Therefore, Sharp Law commenced a thorough and time-consuming review of the entire contents of the account that concluded on June 21, 2024. After confirming last known address information for all individuals, Sharp Law is now notifying individuals out of an abundance of caution. The types of personal information impacted include names and Social Security numbers.

On or about August 16, 2024, Sharp Law provided notice via U.S. regular mail of the incident to the potentially affected individuals. A sample copy of the notice is attached as Exhibit "A" for your records. Sharp Law provided this notification to a total of 3,350 individuals, fourteen (14) of whom are residents of the State of Maryland.

As an added precaution, Sharp Law offered the affected Maryland residents twelve (12) months of Credit Monitoring Fraud Consultation, and Identity Theft Restoration services through Kroll. The notice to the affected individuals includes instructions on the use of this product as well as encouragement to remain vigilant for incidents of fraud or misuse, by reviewing and monitoring

www.fmglaw.com



Maryland Office of Attorney General
August 16, 2024
Page 2

account statements and credit reports, immediately reporting errors or suspicious activity to the financial institution or issuing bank, and filing a report with law enforcement, their state attorney general, and/or the Federal Trade Commission in the event fraud or misuse is discovered. Sharp Law also included contact information for the major consumer reporting bureaus, state-specific regulators, and additional steps individuals may take to protect the impacted information from misuse, should they find it appropriate to do so.

After discovering the incident, Sharp Law partnered with data privacy and security professionals to thoroughly investigate the nature and scope of the event. Sharp Law reset account passwords and implemented multi-factor authentication for Sharp Law email accounts. Sharp Law will continue to evaluate ways to strengthen the existing data security protections that it has in place. Sharp Law is also reporting the incident to other state regulators, as necessary.

I believe this provides you with all information necessary for your purposes and to comply with Maryland law. However, if anything further is needed, please contact me directly.

Respectfully,

FREEMAN MATHIS & GARY, LLP

/s/ Nicholas Jajko

Nicholas Jajko

Exhibit “A”

SHARP LAW

August 16, 2024

[REDACTED]

Re: <<b2b_text_1 (Notice of Data Event/Breach)>>

Dear [REDACTED]

Sharp Law, LLP is committed to protecting the privacy and security of the information we maintain. We are writing to inform you of a data security incident that may have involved some of your information. While there is no evidence of any actual or attempted misuse of your information, we are notifying you out of an abundance of caution and providing you with resources to protect your information. This letter explains the incident, measures we have taken, and some steps you may consider taking in response.

What Happened?

We recently concluded our investigation of an incident that involved authorized access to certain employee email accounts. Upon identifying the incident, we immediately secured the accounts and partnered with computer forensic specialists to conduct a thorough investigation, which concluded on June 21, 2024. Through the investigation, we determined that between November 6, 2023 and February 19, 2024, an unauthorized user had access to certain email accounts and could not rule out that emails or attachments were accessed. After confirming last known address information for impacted individuals, we are now notifying you out of an abundance of caution.

What Information Was Involved?

You are receiving this letter because your [REDACTED] were present in emails and/or attachments within one or more of the affected accounts.

What We Are Doing.

We regret any concern this may cause you. To help prevent a similar incident from occurring in the future, we have implemented additional safeguards and technical security measures to enhance the security of our network. We have also secured the services of Kroll to provide identity monitoring at no cost to you for twelve (12) months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until [REDACTED] to activate your identity monitoring services.

Kroll Membership Number: [REDACTED]

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

What You Can Do.

We also encourage you to remain vigilant for incidents of fraud or misuse, from any source, by reviewing and monitoring your account statements and credit reports. We also recommend you report errors or suspicious activity immediately. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. Please refer to the enclosed documentation which contains additional steps you may take to protect your information from misuse, should you find it appropriate to do so. Please review the enclosed “Additional Resources” section included with this letter. This section describes additional steps you can take to help protect yourself, 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 additional questions, please call our dedicated assistance line at [REDACTED], which is available from 8:00 a.m. — 5:30 p.m. Central Time, Monday through Friday (excluding major U.S. holidays). Please have your Kroll membership number ready when you call.

Sincerely,

Rex Sharp

Rex Sharp
Managing Partner
Sharp Law

Additional Steps to Help Protect Your Information

Review Personal Account Statements and Credit Reports. It is recommended that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. 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 (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, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax
1-888-298-0045
P.O. Box 105069
Atlanta, GA 30348

www.equifax.com

Experian
1-888-397-3742
P.O. Box 9554
Allen, TX 75013

www.experian.com

TransUnion
1-800-680-7289
P.O. Box 2000
Chester, PA 19022

www.transunion.com

Report Suspected Fraud. You may contact law enforcement and have the right to file a police report to report suspected identity fraud of theft. Please note that 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 should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. For more information, visit <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

Obtain Additional Information about the steps you can take to avoid identity theft from the following entities:

- **District of Columbia Residents:** District of Columbia Attorney General at 400 6th Street NW, Washington D.C. 20001; (202) 727-3400; and <https://oag.dc.gov/>.
- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division at 200 St. Paul Place, 16th Flr., Baltimore, MD 21202; toll-free at (888) 743-0023 or (410) 576-6574; and www.marylandattorneygeneral.gov.
- **New Mexico Residents:** You have certain rights under the FCRA, which you can read about by visiting <https://consumer.ftc.gov/articles/0070-credit-your-consumer-rights> and https://consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0070-credit-and-your-consumer-rights_1.pdf. For more information review www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf; or contact Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, DC 20580.
- **New York Residents:** New York Attorney General at Office of Attorney General, The Capitol, Albany, NY 12224-0341; (800) 771-7755; and <https://ag.ny.gov>.
- **North Carolina Residents:** Office of the Attorney General of North Carolina at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; and <https://ncdoj.gov>.

- **Rhode Island Residents:** Office of the Rhode Island Attorney General at 150 South Main Street, Providence, Rhode Island 02903; (401) 274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain a police report.  [Rhode Island residents were impacted by this incident](#);
- **All U.S. Residents:** The Identity Theft Clearinghouse, Federal Trade Commission may be contacted at 600 Pennsylvania Avenue, NW Washington, DC 20580; 1-877-IDTHEFT (438-4338); and www.consumer.ftc.gov. This notification was not delayed by law enforcement.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.