

Scott Koller
T (213) 226-4736
F (213) 488-1178
Email: skoller@clarkhill.com

Clark Hill LLP
555 South Flower Street, 24th Floor
Los Angeles, CA 90071
T (213) 891-9100
F (213) 488-1178

December 27, 2024

VIA ELECTRONIC MAIL

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown:

We represent McWhirter, Bellinger, & Associates, P. A. (“MBA”) with respect to a data security incident involving the potential exposure of certain personal information described in more detail below. MBA 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 16, 2024, MBA identified suspicious activity associated with its network. As soon as it became aware of the activity, it took steps to secure its environment and at the direction of outside counsel, engaged outside computer forensic experts to assist. The investigation determined that a computer server that stores client information was accessed without authorization. MBA conducted a thorough review of the files stored on the computer server and on November 22, 2024, determined that certain information regarding legal matters were potentially accessible, including individual names, addresses, Social Security numbers, medical records and bills, and driver’s license numbers.

2. Number of residents affected.

One (1) Maryland resident was notified of the incident. We began notifying the affected individual on December 27, 2024 (a copy of the form notification letter is enclosed as Exhibit A).

3. Steps taken in response to the incident.

Since the incident, MBA worked to restore its systems, tightened access controls, and is evaluating additional technical safeguards to strengthen the security of its systems. In addition, MBA is offering identity theft protection services through IDX, a company specializing in fraud assistance and remediation services, for 12 months.

4. Contact information.

MBA 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 skoller@clarkhill.com or (310) 928-7524.

Sincerely,

CLARK HILL PLC

Scott Koller

Scott Koller
Member

cc: Mariah Leffingwell – mleffingwell@clarkhill.com

December 27, 2024

Via USPS and Email to

We are writing to let you know about a recent data security incident that may have involved some of your information. This letter contains information about steps you can take to protect your information and the resources we are making available to help you.

What Happened?

On October 16, 2024, we identified suspicious activity associated with our network. As soon as we became aware of the activity, we took immediate steps to secure the environment and engaged outside computer forensic experts to assist. Our investigation determined that a computer server that stores client information was accessed without authorization.

What Information Was Involved?

On November 22, 2024, we were notified though a company we hired to assist with the data breach what documents were potentially accessible, including your name and address, Social Security number, and Driver's license number. The incident also involved the personal information of individuals affiliated with your legal matter.

What We Are Doing:

We have no evidence that your specific information was accessed or misused in connection with this incident. Furthermore, we do not believe this situation poses any risk to our ability to effectively represent you or to the integrity of our ongoing work on your legal matter. Nevertheless, we wanted to let you know this had occurred and assure you that we are taking steps to minimize the risk of this happening in the future. Since the incident, we have worked to restore our systems, tightened access controls, and are evaluating additional technical safeguards to strengthen the security of our systems. In addition, we are offering identity theft protection services through IDX, a company specializing in fraud assistance and remediation services, for 12 months. With this protection, IDX will help you resolve issues if your identity is compromised. In addition, for those individuals affiliated with your matter, we will also notify those affected individuals on your behalf.

What You Can Do:

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 866-329-9984 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided below. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is April 23, 2025.

For More Information:

If you have questions, please call 803-252-5523 Monday through Friday from 8:00 a.m. to 5:00 p.m. Eastern Time. Protecting your information is important to us, and we sincerely apologize for any concern this incident may cause you.

Sincerely,



McWhirter, Bellinger & Associates, P.A.

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

1. **Website and Enrollment.** To Enroll, Please Call: 866-329-9984 Or Visit: <https://app.idx.us/account-creation/protect>. Enrollment Code: WRXWKJHPVK
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.

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 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.

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.