



Ryan M. Cook
1020 Highland Colony Parkway, Suite 310
Ridgeland, Mississippi 39157
Ryan.Cook@lewisbrisbois.com

September 21, 2023

Via electronic-mail: *ldtheft@oag.state.md.us*

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Our Client: Messerli & Kramer, PA
Matter: March 2023 Data Security Incident

Dear Attorney General Brown:

We represent Messerli & Kramer, P.A. ("MK"), headquartered in Minneapolis, Minnesota, with respect to a data security incident described in more detail below. MK takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that MK has taken in response to this incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On March 15, 2023, MK detected and stopped a network security incident. MK immediately shut off all access to the network and engaged a specialized third-party forensic incident response firm to assist with securing the environment. MK's network has been secured and remediated. MK initiated a comprehensive investigation into what sensitive data could have been compromised. Once the forensic investigation identified the potentially affected dataset, MK engaged a third-party vendor to mine the data for personal information. The initial phase utilized a programmatic search to identify instances of personal information within the data set. The second phase consisted of manual document review in which individual's names and contact information was extracted from the files. Once the list of potentially affected individuals was finalized by the data mining vendor, MK moved quickly to send notification letters to these individuals.

Although MK found no evidence that individuals' personal information has been specifically misused, it is possible that individuals' name, social security number, passport and driver's license/ID numbers could have been exposed to the cybercriminal. As of this writing, MK has not received any reports of related identity theft since the discovery of the incident (March 15, 2023 to present).

2. Maryland Residents Notified

A total of two (2) Maryland residents were potentially affected by this security incident. Notification letters were mailed to these individuals on September 6, 2023 by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Upon detecting this incident, MK moved quickly to initiate a response, which included remediating the vulnerability and conducting a comprehensive investigation into the incident. MK has reported this incident to law enforcement. MK has reviewed and altered its policies and procedures relating to the security of its systems and servers.

Although MK is not aware of any evidence of misuse of personal information, MK extended to potentially impacted individuals an offer for free credit monitoring and identity theft protection through IDX. This service will include 12 months of credit monitoring for Maryland residents, along with a fully managed ID theft recovery service, should the need arise.

4. Contact Information

MK remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact Ryan M. Cook, Esq. at: Ryan.Cook@LewisBrisbois.com or 601.826.2604.

Sincerely,



Ryan M. Cook for
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: *Sample notification letter*

RMC

Messerli & Kramer P.A.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07327

September 6, 2023

Notice of Data Security Incident

Dear [REDACTED],

We are writing to inform you of a recent data security incident that may have resulted in unauthorized access to your personal information. We take the privacy of your personal information seriously and want to provide you with information and resources you can use to protect your identity. This letter contains information about the incident and information about how to protect your personal information going forward.

What Happened and What Information was Involved:

Recently, Messerli & Kramer P.A. ("Messerli & Kramer") detected a network security incident. An unauthorized third-party infiltrated our network environment. We immediately engaged specialized third-party forensic and technical resources to respond to the incident. We have secured the network and the data that we maintain.

Upon discovery, we initiated a comprehensive investigation into the cause and extent of the unauthorized activity. An investigation revealed that the following categories of your information may have been exposed during the compromise: name, Social Security Number, driver's license/ID number, passport number, and medical information. Notably, the types of information affected varied by individual, and not every individual had every element exposed.

As of this writing, Messerli & Kramer has not received any reports of related identity theft since the date of the incident. Based on Messerli & Kramer's investigation and consultation with industry experts, Messerli & Kramer does not believe that the above referenced information has been made publicly available or distributed by an unauthorized party.

What We Are Doing:

Messerli & Kramer is committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon detecting this incident, we moved quickly to initiate our incident response plan, which included fully securing our network and the data that we maintain. We conducted an investigation with the assistance of third-party forensic specialists and have reported this matter to law enforcement. We are reviewing our tools, policies, and procedures relating to the security of our systems and servers.

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 twelve (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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/messerlikramer> 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.

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. Call center representatives can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

We recognize that you may have questions not addressed in this letter. Cyberscout representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line 1-833-570-2824 and supply the fraud specialist with your unique code listed above.

Messerli & Kramer values the privacy and importance of your personal data, and we apologize for any inconvenience or concern that this incident has caused.

Sincerely,

Messerli & Kramer P.A.

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well):

- (1) full name, with middle initial and any suffixes;
- (2) Social Security number;
- (3) date of birth;
- (4) current address and any previous addresses for the past five years; and
- (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax ([https://assets.equifax.com/assets/personal/Fraud Alert Request Form.pdf](https://assets.equifax.com/assets/personal/Fraud%20Alert%20Request%20Form.pdf));
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are listed above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For 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 violators. 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. We encourage you to 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.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For 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, and <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.