



CHIESA SHAHINIAN & GIANTOMASI PC

ONE BOLAND DRIVE
WEST ORANGE, NJ 07052

csglaw.com

MICHELLE A. SCHAAP

mschaap@csglaw.com

(O) 973.530.2026

(F) 973.530.1501

March 4, 2022

via Electronic Mail

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
ldtheft@oag.state.md.us

Re: Notice of Security Incident

To Whom It May Concern:

This firm serves as legal counsel to Klein Mirky LLC, a limited liability company with its principal address at 2900 Logan Road, Ocean, NJ 07712 (the "Company"). This letter has been submitted as notice pursuant to Md. Code Ann. Com. Law § 14-3504(h) regarding a security incident suffered by the Company and potentially impacting one (1) Maryland resident.

NATURE OF THE DATA SECURITY INCIDENT

On February 9, 2022, the Company confirmed that a malicious actor gained unauthorized access on or about February 7, 2022 to the Company's computer server using a remote desktop protocol ("RDP"), which was open to the internet (the "Security Incident"). Based on the Company's preliminary findings in conjunction with a third-party cybersecurity expert retained through this firm, the malicious actor gained access to a spreadsheet containing certain client information.

At this time, as to the single Maryland resident, the categories of personally identifiable information believed compromised during the Security Incident is the resident's name, address, email address, phone number, and date of birth. The impacted Maryland resident's social security number may also have been exposed.

NUMBER OF MARYLAND RESIDENTS AFFECTED

The Company believes that the Security Incident potentially impacted one (1) Maryland resident, who will be notified imminently by way of written notice, with a copy of the form of such notice appended to this letter.

STEPS TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

Shortly after learning of the Security Incident, the Company immediately responded by hiring external security forensic consultants to confirm and assess the scope of the Security Incident. The affected server was disconnected from the network and was deleted entirely several hours later. Additionally, port forwarding was disabled, ensuring that remote desktop is no longer publicly accessible. Further, multi-factor authentication has been implemented for user accounts. The email account which was infiltrated was deleted. The Company will also be offering twenty-four (24) months of free credit monitoring services to the impacted Maryland resident through Experian.¹

While the Company already had in place technological, administrative and operational procedures, the Company has made—and continues to make—further improvements to its security technology, processes and procedures.

CONTACT INFORMATION

The Company is treating the Security Incident as its highest priority and will provide any further relevant information upon the conclusion of its investigation. Please reach me at 973-530-2026 or mschaap@csglaw.com if you have any questions or need further information.

Respectfully yours,

Michelle A. Schaap

MAS:fxw
Enc.

¹ The written notice to the Maryland resident will be issued on Company letterhead and will also include instructions on how to sign-up for such services, which have not been attached to the sample provided herein.

Dear [REDACTED],

At Klein Mirsky LLC, we value transparency and respect the privacy of your information.

Following up on our prior correspondence to you; based on the findings of our third-party cybersecurity professionals and legal experts, we have confirmed that a malicious actor gained unauthorized access on or about February 7, 2022 to the Company's computer server and had access to a spreadsheet which included your name, physical address, email address, phone number, and date of birth. Your social security number may also be at risk.

While such incidents unfortunately have become all too common, we recognize that this news can be unsettling. We take your privacy very seriously, and we want you to have all the information you need to respond appropriately. To that end, we want you to know what we did in response, and the steps you can take to help protect yourself against possible misuse of the information.

In response to this incident, we hired outside cybersecurity and legal experts to analyze the incident. We have further enhanced our cyber defenses. We have also informed law enforcement. To date, we are not aware of any unauthorized use of sensitive personal information.

If we learn of any additional information pertinent to you, we will share it with you.

Should you receive a call, an email, or other communication from someone who claims to have your personal information:

- Do not engage with the caller/correspondent, and do not offer details about the attack or what may have occurred.
- Listen carefully and immediately following the call, make notes about what you were told.
- As soon as possible, report the same to your local police and to your state cybercrimes unit. The enclosed resource page provides this information.

We strongly recommend you remain vigilant. Monitor and review all your financial and account statements, and immediately report any unusual activity to the institution that issued the record and to law enforcement. Attached to this letter is a resource sheet with additional information for your reference.

Out of an abundance of caution, we are also offering you free credit monitoring services for a period of time. Attached here is additional information as to how to sign up.

If you have any questions regarding this information, please contact [REDACTED].

We thank you for your understanding and consideration.

Respectfully,

Gary Klein & Alison Mirsky

STEPS YOU CAN TAKE:

- **Local Police Reporting**

File a report with your local police department.

- **Passwords, Passcodes**

We strongly encourage you to change passwords and passcodes on all personal accounts and devices. Often, people will use the same password that they use for one account or device for multiple accounts and/or devices. When you change passwords, this should include your personal social media accounts, online banking accounts, cellphones, tablets, home computers, etc. Best practice is not to use the same password for more than one account or device, nor to “recycle” or reuse passwords that were used in the last several years. If your accounts offer multi-factor authentication, we suggest you enable this for those accounts.

- **IRS**

Complete IRS Form 14039. The form can be found at: <https://www.irs.gov/newsroom/tips-for-taxpayers-victims-about-identity-theft-and-tax-returns-2014> and a copy is attached here for your convenience.

You can contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

- **The Social Security Administration**

We recommend that you review your record on your Social Security Statement if you suspect someone has misused your Social Security number. The Statement is available online to workers age 18 and older. To get your Statement, go to www.ssa.gov/myaccount and create an account.

We also recommend that you contact the Social Security Administration by visiting www.ssa.gov to apply for benefits; get useful information; find publications; and get answers to frequently asked questions. You may also contact 1-800-772-1213 for further assistance or 1-800-325-0778 (TTY) if you're deaf or hard of hearing. For more information, please visit <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

To file with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. The postal address for the Bureau of Consumer Protection and Federal Trade Commission is provided below:

Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

- **Copy of Credit Report**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Experian
(888) 397-3742
www.experian.com
535 Anton Blvd., Suite 100
Costa Mesa, CA 92626

TransUnion
(800) 916-8800
www.transunion.com
P.O. Box 6790
Fullerton, CA 92834

Equifax
(800) 685-1111
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

- **Fraud Alert**

We recommend placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

- **Credit Freezes**

You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and

instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
- TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com
- Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique PIN or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specific period of time.

To remove the security freeze, you must submit a request through a toll-free number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one hour after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

The State of Maryland also offers a resource page on identity theft, which can be found at: <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>.

The Attorney General's Identity Theft Unit has tools available to help victims of identity theft address their problems, and to help all consumers protect themselves from identity thieves. The Identity Theft Unit can give you step-by-step advice on how to protect yourself from identity thieves using, or continuing to use, your personal information. You may contact the Identity Theft Unit by calling (410) 576-6491 or by sending an e-mail to idtheft@oag.state.md.us.