



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

February 3, 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 letter serves as notice pursuant to Md. Code Ann., Com. Law § 14-3504(h) regarding a security incident potentially impacting one (1) Maryland resident suffered by this firm's client, OTR Global Holdings II, Inc., an industry research company located at 4 Manhattanville Road, Purchase, NY 10577 (the "Company").

NATURE OF THE DATA SECURITY INCIDENT

On January 20, 2022, the Company detected unusual activity on the Company's computer network. On January 25, 2022, the Company confirmed the presence of an unauthorized entity on the Company's servers and a possible security compromise of its servers as the result of an apparent ransomware attack (the "Security Incident"). After retaining outside counsel and upon the completion of a third party external forensics review, the Company determined that on January 18, 2022, the Company's systems experience an intrusion, which resulted in the execution of a ransomware attack by an unknown cybercriminal organization. At this time, as to the single Maryland resident, the only categories of personally identifiable information believed compromised during the Security Incident are employee names, physical addresses, email addresses, and Company phone numbers. To date, there is no evidence the Security Incident has resulted in the compromise of sensitive personal data or resulted in identity theft, fraud, or financial losses to consumers. Certain sensitive information of independent contractors outside the United States may have been exposed, and reporting has been made to local authorities. In addition, at present, there is confirmation of the exposure of one US employee's sensitive information.

NUMBER OF INDIVIDUALS AFFECTED AND DATE OF NOTICE

The Company believes that the Security Incident potentially impacted one (1) Maryland resident, and potentially one hundred thirty-four (134) other persons outside of Maryland. The affected Maryland individual will be notified of the Security Incident by written notice via U.S. Mail on February 4, 2022.

DESCRIPTION OF SECURITY MEASURES IN PLACE AT THE TIME OF THE INCIDENT

At the time of the Security Incident, the Company had in place the following administrative and technical security measures, including but not limited to: (1) firewalls at all office locations that access the Company's core cloud infrastructure, which disallow all inbound connections except those coming from IPsec VPN tunnels and limits all inbound connections to the ports necessary for the service and only allows access from source IPs where applicable; (2) endpoint protection and antivirus software on all servers and workstations; (3) email malware protection/gateway service, before delivery to our network or users; (4) backups, which are stored at multiple locations on and offsite, and tested regularly; (5) installation and deployment of applicable critical and high severity patches that are reviewed and deployed regularly; (6) auto-lock on network workstations after a period of inactivity; (7) authorized use policies, whereby users do not have local administrative permissions on networked workstations; (8) group policies, whereby users are prohibited from installing software; (9) password policies, including robust password requirements, regular scheduled expirations, and immediate removal of user access if an employee leaves the company; (10) strict access configuration (e.g., sensitive applications and systems) configured on an as-required basis according to need-to-know and removed on a timely basis when no longer required; and (11) implementation of multiple services to monitor network and services and alert system administrators to problems.

STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

Shortly after confirmation of the Security Incident on January 25, 2022, the Company responded by hiring external security forensic consultants to assess the scope of the Security Incident and conduct a forensic investigation. Systems have been, or are in the process of being rebuilt and restored, and monitoring software has been installed. The Company has also augmented its administrative and technological safeguards, including, but not limited to (1) resetting domain administrator passwords and personnel passwords; (2) revising password policies and including increasing the frequency of password reset and lockout period after failed login attempts; (3) deploying additional endpoint protection software; (4) implementing software for notifications for the detection of brute-force authentication attempts; and (5) hardening all systems and servers in the Company's network.

The Company reported the incident to the Federal Bureau of Investigation and filed a SARS report with Financial Industry Regulatory Authority. Additionally, although there is no evidence that any personal information which may have been accessed has been used for fraudulent purposes, the Company is providing complimentary credit monitoring services to the affected individuals for a period of twelve (12) months.

February 3, 2022
Page 3

As noted above, the Company already had in place technological, administrative and operational procedures in place. As a result of the incident, the Company has made, and continues to make, improvements to its security technology, processes and procedures.

CONTACT INFORMATION

Please feel free to contact 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: Copy of form of notification to the affected Maryland

Dear XXXXX,

At OTR Global, we value transparency and respect the privacy of your information. That is why I am writing personally to let you know about a data security incident that was detected on January 20, which may have exposed your personal information.

While such incidents unfortunately have become all too common, we recognize that this news can be unsettling. We take the wellbeing and privacy of our personnel very seriously, and we want you to have all the information you need to respond appropriately. To that end, I 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.

We hired outside cybersecurity and legal experts to aid our in-house professionals and analyze the incident. We also informed law enforcement and, to date, authorities have not reported any unauthorized use of personal information.

Should you receive a call, 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, share the information with Elena Coppola in Human Resources at 914-908-3930.
- We will make sure you receive the information you need to properly respond to the situation.

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. You will be receiving additional information by mail on how to sign up.

Fortunately, our effective safety protocols enabled us to quickly transition to backup systems and minimize disruption. To help us successfully counter any future attempt to compromise our systems, we are instituting additional security measures, some of which require changes to our current protocols. We will require all personnel to change their OTR Global passwords more frequently going forward and advise you to regularly change all your passwords on all accounts (business and personal) as a best practice. Further, please do not use the same password for multiple accounts and do not “recycle” passwords from one account to another.

We are doing everything possible to ensure the safety and security of your information. We have supplemented our already robust protocols to further protect against these types of breaches. As mentioned above, we have informed appropriate governmental authorities and will continue to cooperate fully with law enforcement. If we learn of any additional information pertinent to you, we will share it with you.

If you have any questions regarding this information, please contact Elena Coppola in Human Resources at 914-908-3930.

We thank you for your continued hard work and digital diligence. OTR Global would not be what it is without your commitment and dedication to our mission and our success.

Respectfully,



Mark Conley

President, Director of Research

OTR Global

To date, and based on our investigation in conjunction with a third-party forensics team, the only categories of your personally identifiable information believed to have been compromised during the security incident were your name, physical address, email address, and/or Company phone numbers. To date, there is no credible evidence the security incident has resulted in the compromise of your sensitive data or resulted in identity theft, fraud, or financial losses to our employees. If we learn of information to the contrary, we will provide you with further information accordingly. However, in addition to signing up for free credit monitoring services and considering the information that we have provided you, we nevertheless encourage you to take the following steps and consider the following additional guidance and resources below.

IF YOUR IDENTITY IS COMPROMISED STEPS YOU CAN TAKE:

- **Local Police Reporting**

File a report with your local police department.

- **Passwords, Passcodes**

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. If 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.

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

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.

- **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.