

From: Victoria Sulerzyski <vsulerzyski@gmail.com>
Sent: Sunday, September 22, 2024 3:55 PM
To: IDTheft
Subject: Notification of Cybersecurity Incident
Attachments: General Letter of Breach..docx; Data Breach Notification Steps.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Data breach

Mr. Karberg,

I am writing to inform the Maryland Office of the Attorney General of a cybersecurity unauthorized access to my work laptop. I am a solo practitioner that is not on a network. I work off of a laptop that is protected by a VPN. I also use 2-step verification and use complex passwords which I change frequently. I work primarily out of my home. My practice involves estates and trusts, guardianships, estate administration and special needs planning.

On September 5, 2024, I called Microsoft Tech support as my Microsoft Office 365 email with one of my law firm clients was giving me an error message. This was an 877 number. The person on the line started asking me questions regarding my email account and then told me that in order for Microsoft to restore the email, that they had to put a patch on my computer. They ran a program on my computer and I was told to let it run for a couple of hours. He gave me a Microsoft support ticket of DL110035. He then gave me his direct number of (408) 521-3961 and said his name was Mike Ross. After I hung up, I was not comfortable so I shut my laptop down and unplugged it from the wall. I did not open it again. I then spoke with an IT expert for one of the other law firm clients of mine who said that it was a hack. She arranged for my laptop to undergo a forensic review by an IT specialist that is an expert in that area. I provided him with my laptop immediately. Last week, he finished the forensic check and told me that they accessed the hard drive through a program called Ultra Viewer at two points on September 5th - One at 2:45 pm and one at 3:15 pm. This corresponds to the time I called Microsoft Support and about the time that I shut down my computer and hung up on the call. The IT specialist told me that the IP address of the unauthorized computer is 182.69.180.20. He said it could also be a proxy. He also said that the two points of entry did not look suspicious but since they used Ultra Viewer there is no way for him to get into Ultra Viewer to see what they ultimately were able to reach. He also said that the IP address was from India.

The data on my computer contains some sensitive PI and some HIPAA data (of my special needs daughter). Client data points include certificates for guardianships that contain health information (diagnosis information) and IEPs that may include the same type of health information. I also prepare fiduciary income tax returns and a couple of individual returns for individuals. While the tax returns themselves are on a third-party tax program, the back-up of some of the clients were on my laptop. I did not do any tax returns after the regular tax season this past April 2024. No other personal information was on the laptop.

Pursuant to my written data privacy and security plan, I have notified the Internal Revenue Service, the FBI, the Comptroller of Maryland (waiting for a return call) and your office.

I have reviewed my laptop's backup from my external drive and have determined that there have been 47 client files that have been affected.

I have prepared the attached draft notice to my clients that have been affected by the unauthorized access.

This has been a very upsetting matter for me.

Please let me know if you have any questions. Once I hear back from your office, I will send the notice to the clients that have been affected.

Best regards,

Victoria

--

Victoria Z. Sulerzyski, Esquire
Special Needs Law, LLC
206 Windrush Farm Lane
Severna Park, Maryland 21146
(410) 991-3014
vsulerzyski@gmail.com

This e-mail is confidential, intended only for the named recipient(s) above and may contain information that is privileged, attorney work product or exempt from disclosure under applicable law. If you have received this message in error, or are not the named recipient(s), please immediately notify the sender at 410-991-3014 and delete this e-mail message from your computer. Thank you.

Circular 230 Disclosure: Pursuant to recently-enacted U.S. Treasury Department Regulations, we are now required to advise you that, unless otherwise expressly indicated, any federal tax advice contained in this communication, including attachments and enclosures, is not intended or written to be used, and may not be used, for the purpose of either (i) avoiding tax-related penalties under the U.S. Internal Revenue Code or (ii) promoting, marketing or recommending to another party any tax-related matters addressed herein.

September 24, 2024

TO [CLIENT]:

I am writing to inform you about a cybersecurity incident that may have involved some of your personal information. We are contacting you directly to explain the circumstances of the incident, the measures we are taking in response, and offer steps you may consider taking.

On September 5, 2024, we called the toll-free number for Microsoft Tech Support due to an issue with a Microsoft email account. After the call, it became apparent that the toll-free number that was called was a fraudulent phone number for Microsoft Tech Support. Access to our system was breached. Within 24 hours, a forensic computer expert was engaged. The forensic team determined that the unauthorized access to the computer was very brief and that due to our actions to mitigate access and our data privacy security matters we follow daily, that there was no suspicious activity found. The data that may have been accessed includes names, addresses, phone numbers, student health information and tax information.

We recommend you monitor your accounts and watch for any suspicious activity. If you suspect or discover that your information has been used inappropriately, please notify your local law enforcement or consumer protection agency. For more information on additional steps you can take to protect your information, please see the pages that follows this letter.

Should you have any questions, please call me at (410) 991-3014, write to me at 206 Windrush Farm Lane, Severna Park, Maryland 21146, or email at vsulerzyski@gmail.com. We apologize for any inconvenience resulting from this matter.

Sincerely,

Victoria Z. Sulerzyski
Managing Member

ADDITIONAL STEPS YOU CAN TAKE

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit

www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- Equifax, P.O. Box 74021, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111.
- Experian, P.O. Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742.
- TransUnion, P.O. Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Maryland Attorney General's office. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, 1-877-438-4338, www.ftc.gov/idtheft.

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect that you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit report? 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 above.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within

one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

You may also contact the Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 or (410) 576-6300; www.oag.state.md.us.

A Summary of Your Rights Under the Fair Credit Reporting Act: the federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, D.C. 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.