BARCLAY DAMON LLP

Kevin D. Szczepanski
Partner

March 11, 2025

VIA ELECTRONIC MAIL (IDTHEFT@OAG.STATE.MD.US)

Attorney General Anthony G. Brown
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Brown,

I am writing on behalf of my client, Olinsky & Associates, PLLC ("Olinsky"), to notify you of a data security incident involving two Maryland residents. Unauthorized criminal actors gained access to some of Olinsky's electronic systems. Upon learning of the attack on January 28, 2025, Olinsky immediately took steps to secure its systems and began an investigation with the assistance of a forensic firm. The investigation determined that Olinsky was the victim of a phishing attack, which allowed the threat actors to use trusted systems to infiltrate the computer systems. Further, it was concluded that some files on a shared drive on the network were compromised, however, a vast majority of the network was not breached. Olinsky secured its systems immediately after learning of the attack and did not pay the ransom demand by the criminals.

Olinsky conducted a thorough investigation of the systems to ensure that they are secure and to identify the nature and potential scope of the unauthorized access. Olinsky has reported this incident to the police, and they, too, are investigating. Olinsky has also reported this incident to the FBI, and Olinsky is waiting to hear from them. As part of our ongoing commitment to information security, Olinsky has implemented several additional security features, including, but not limited to, multi-factor authentication for VPN connections, web filtering, and installation of additional cybersecurity software such as SSL deep inspection and SentinelOne. Additionally, Olinsky has retrained its employees on security measures and protocols.

On January 30, 2025, Olinsky provided initial notice to all conceivably impacted individuals—that is, individuals whose names and email addresses were in our systems that Olinsky thought might have been exposed. Following, Olinsky learned that only a small subset of clients' data was exposed and, by e-mail dated February 7, 2025, provided additional notice to those individuals for whom we had e-mail addresses and whose personal or health information was exposed. On March 11, 2025, Olinsky mailed notification letters via United States Postal Service First-Class mail to the Maryland residents whose information may have been involved. A sample copy of the notification letter is enclosed. Olinsky has implemented additional

measures to enhance security protocols to protect all information.

Please do not hesitate to contact me if you have any questions regarding this matter.

Very truly yours,
/s/ Kevin Szczepanski

Kevin D. Szczepanski

Olinsky Law Group
A NATIONAL DISABILITY LAW FIRM

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Dear <<Full Name>>:

We are writing to tell you about a data security incident at Olinsky & Associates, PLLC ("Olinsky") that might have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What Happened? We recently completed an investigation involving a cyber-attack against Olinsky in which unauthorized criminal actors gained access to some of our electronic systems. Upon learning of the attack on January 28, 2025, we immediately took steps to secure our systems and began an investigation with the assistance of a forensic firm.

They concluded that some files on a shared drive on our network were compromised. The vast majority of our network was not breached. It was determined that criminals first accessed our shared drive through a "phishing" attack in which the threat actor used trusted systems to infiltrate the computer systems. We were able to secure our systems immediately after learning of the attack, and we did not pay the ransom demand by the criminals.

What Information Was Involved? After completing our investigation in early February, 2025, we determined that the unauthorized person accessed personal or health information we have on file for you, including, for example, your SSN, account information, financial information, medical records, or disability-payment information. Some of the information was truncated, only exposing the last four or five digits of the social security number or bank account information.

What Is Olinsky's Doing? Immediately after we discovered this incident, we took steps to secure our employees' e-mail accounts and restrict the threat actor's access to our computer system. We conducted a thorough investigation of our systems to ensure that they are secure and to identify the nature and potential scope of the unauthorized access. We have reported this incident to the police, and they, too, are investigating. We have also reported this incident to the FBI, and we are waiting to hear from them. By email dated January 30, 2025, we provided initial notice to all conceivably impacted individuals—that is, individuals whose names and email addresses were in our systems that we thought might have been exposed. After an investigation, we learned that only a small subset of clients' data was exposed and, by e-mail dated February 7, 2025, we provided additional notice to those individuals for which we had e-mail addresses and whose personal or health information was exposed.

We want to assure you that we take this incident and the security of your personal data very seriously. As part of our ongoing commitment to information security, we have implemented several additional security features, including, but not limited to, multi-factor authentication for VPN connections, web filtering, and installation of additional cybersecurity software such as SSL deep inspection and SentinelOne.

What Can You Do? We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. In order to assist you, we have secured credit-monitoring services for you. Those services will include monitoring from three credit bureaus for two years. Your credit monitoring services include 3-bureau credit monitoring with email notifications, webscan notifications, automatic fraud alerts, identity restoration assistance, and up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses.

For instructions on how to activate your complimentary two-year membership, please see the attached correspondence below.

Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. If you have any questions, please call 855-659-0092, Monday through Friday from 9:00 A.M. through 9:00 P.M. Eastern Time.

Sincerely,

Howard D. Olinsky, Esq.

ADDITIONAL RESOURCES

EQUIFAX®

<<Full Name>>
Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[6].
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of **<<Activation Code>>** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

[1]The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness. [2]Credit monitoring from Experian and TransUnion will take several days to begin. [3]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [4]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [5]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.co [6]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.