

JacksonLewis

Jackson Lewis P.C.
666 Third Avenue
New York NY 10017-4030
(212) 545-4000 Main
(212) 972-3213 Fax
jacksonlewis.com

DIRECT DIAL: (212) 545-4006
EMAIL ADDRESS: GREGORY.BROWN@JACKSONLEWIS.COM

December 13, 2024



VIA FIRST-CLASS MAIL

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

Re: *Data Incident Notification*

Dear Sir or Madam:

We are writing to notify your office of a data security incident affecting 93 Maryland residents. We are submitting this notice as counsel for Ott Cone & Redpath, P.A. ("Ott Cone"), whose mailing address 445 Dolley Madison Rd., Ste 306, Greensboro, NC, 27410.

Ott Cone was subject to a criminal cyberattack that impacted a Firm email account ("Incident"). With assistance from third-party experts, Ott Cone took immediate steps to secure its systems and investigate the nature and scope of the Incident. As part of Ott Cone's extensive investigation, it worked diligently to identify any PII that may have been subject to unauthorized access or acquisition as a result of the Incident. Ott Cone has not found any evidence that PII was misused as a result of the Incident.

On or about October 31, 2024, Ott Cone determined that the Incident may have impacted PII related to 93 Maryland residents. The categories of personal information involved in the Incident are names, dates of birth, social security numbers, medical treatment information, and health insurance information.

Out of an abundance of caution, and in accordance with applicable law, Ott Cone will provide notice to the affected Maryland residents, in the form enclosed as Exhibit A, so that they can take steps to minimize the risk that their information will be misused. Additionally, Ott Cone has arranged for the individuals to enroll in free credit monitoring and related services for 12 months.

Ott Cone treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since the Incident, Ott Cone has taken a number of steps to further secure its systems. Specifically, it has deployed endpoint detection and response within its environment, including 24/7 managed detection and response services, and will continue to utilize this solution on a going forward basis; strengthened its email security system, including its existing multi-factor authentication protocol; increased the frequency and complexity of cyber security training for its employees; and thoroughly reviewed and upgraded its data security policies and procedures.

Ott Cone will continue to monitor this situation and will update you on any significant developments. If you require any additional information on this matter, please contact me.¹

Sincerely,

JACKSON LEWIS P.C.

/s/ Gregory C. Brown, Jr.

Gregory C. Brown, Jr.

Enclosure.

¹ Please note that Ott Cone is not, by submitting this letter, agreeing to the jurisdiction of State of Maryland, nor waiving its right to challenge jurisdiction in any subsequent actions.

Exhibit A

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:



Or Visit:
<https://response.idx.us/OttCone>

December 13, 2024

Incident Notice

Dear <<First Name>> <<Last Name>>,

What Happened

We are writing to notify you that Ott Cone & Redpath, P.A. (“Ott Cone”) was subject to a criminal cyberattack (the “Incident”) that impacted a Firm email account. With assistance from third-party experts, we took immediate steps to secure our systems and investigate the nature and scope of the Incident. As part of our extensive investigation, we worked diligently to identify any personally identifiable information (“PII”) that may have been subject to unauthorized access or acquisition as a result of the Incident. On or about October 31, 2024, we determined that the Incident may have impacted PII related to you. However, we have not found any evidence that your information was misused.

What Information Was Involved

The affected email account may have contained the following categories of PII related to you: name, <<Variable Data - Impacted Information>>.

What We Are Doing

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we have arranged for IDX to provide you <<12/24 months>> of free credit monitoring and related services. To enroll, please visit <https://response.idx.us/OttCone> or call 1-877-720-2768. Your enrollment code is <<ENROLLMENT>>. To receive these services, please be sure to enroll by March 13, 2025.

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since the Incident, we have implemented a series of cybersecurity enhancements and will soon roll out others.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

For More Information

If you have questions or concerns, please call us at 1-877-720-2768, Monday through Friday, 9am to 9pm Eastern, excluding major US holidays. We sincerely apologize for this situation and any concern or inconvenience it may cause you.

Sincerely,

Ott Cone & Redpath, P.A.

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

- Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
- You can also receive information from these agencies about avoiding identity theft, such as by placing a “security freeze” on your credit accounts.
- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
- Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax
P.O. Box 740256
Atlanta, GA 30374
(866) 510-4211
psol@equifax.com
www.equifax.com

Experian
P.O. Box 2390
Allen, TX 75013
(866) 751-1323
Databreachinfo@experian.com
www.experian.com/

TransUnion
P.O. Box 1000
Chester, PA 19022
(800) 888-4213
<https://tudatabreach.tnwreports.com/>
www.transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
3. The Federal Trade Commission (“FTC”) offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a “security freeze” on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement or the attorney general, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580

4. *Iowa Residents:* You may contact law enforcement or the Iowa Attorney General’s Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.
5. *Maryland Residents:* You may obtain information about avoiding identity theft from the Maryland Attorney General’s Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.
6. *New York Residents:* You may obtain information about preventing identity theft from the New York Attorney General’s Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.
7. *North Carolina Residents:* You may obtain information about preventing identity theft from the North Carolina Attorney General’s Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

8. *Oregon Residents:* You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.
9. *Washington D.C. Residents:* You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.
10. *New Mexico Residents:* You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

- a. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
- b. Proper identification to verify your identity; and
- c. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

11. *Rhode Island Residents:* You may contact and obtain information from and/or report identity theft to your state attorney general at:

Rhode Island Attorney General's Office
150 South Main Street
Providence, RI 02903
Phone: (401) 274-4400
Website: www.riag.ri.gov

You have the right to obtain a copy of the applicable police report, if any, relating to this incident. You may want to place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, please follow these instructions:

- Equifax: <https://www.equifax.com/personal/credit-report-services/credit-freeze/>
- Experian: <http://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/>
- Transunion: <https://www.transunion.com/credit-freeze>

Mailing addresses for the credit reporting agencies are provided above. Credit reporting agencies charge a \$5.30 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft, in which case there is no fee. A copy of your police report or an investigative report or written FTC complaint documenting identity theft must be included to avoid a fee. In your request, you also must include: (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.), address, Social Security number, and date of birth; (iii) if you have moved in the past five years, the address of each residence you lived at during that time period; (iv) proof of current address, such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable, (vi) payment by check, money order, or credit card (Visa, Master Card, American Express, or Discover cards only.)

You can also place a fraud alert with the credit reporting agencies. This will flag your file with a statement that says you may be a victim of fraud and that creditors should phone you before extending credit. To place a fraud alert on your credit file call the fraud department of one of the three credit reporting agencies – Experian, Equifax, or TransUnion (see above). When you request a fraud alert from one agency, it will notify the other two for you. You can place an initial fraud alert for 90 days and may cancel the fraud alerts at any time.