

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

May 31, 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 three (3) Maryland residents. We are submitting this notice as counsel for TPG Architecture, LLP ("TPG"), whose mailing address is 132 West 31st Street, 5th Floor, New York, NY 10001.

TPG was subject to a ransomware attack on December 14, 2023 ("Incident"). With assistance from third-party experts, TPG took immediate steps to secure its systems and investigate the nature and scope of the Incident. As part of TPG's extensive investigation, it worked diligently to identify any personal information that may have been subject to unauthorized access or acquisition as a result of the Incident. TPG has not found any evidence that personal information was misused as a result of the Incident.

On or about April 5, 2024, TPG determined that the Incident may have impacted personal information related to three (3) Maryland residents. The categories of personal information involved in the Incident are names, social security numbers, financial account numbers, and dates of birth.

Out of an abundance of caution, and in accordance with applicable law, TPG 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, TPG has arranged for the individuals to enroll in free credit monitoring and related services for 12 months.

TPG treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since the Incident, TPG has taken a number of steps to further secure its systems. Specifically, it has rebuilt all of the systems impacted by the Incident; has enhanced its existing endpoint detection and response within its environments, including 24/7 managed detection and response services, and will continue to utilize this enhanced solution on a going forward basis; reset passwords; strengthened its email security system; and thoroughly reviewed and upgraded its data security policies and procedures.

Office of the Attorney General

May 31, 2024

Page 2

TPG 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 TPG 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”



May 31, 2024

Incident Notice

Dear [REDACTED],

What Happened

We are writing to notify you that TPG Architecture, LLP was subject to a ransomware attack on December 14, 2023 (the "Incident"). 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 April 5, 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 Incident may have impacted the following categories of PII related to you: name, social security number, financial account number, date of birth.

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 TransUnion to provide you 12 months of free credit monitoring and related services. To enroll, please visit www.firstwatchid.com or call 888-498-3994. Your enrollment code is [REDACTED]. To receive these services, please be sure to enroll by August 29, 2024.

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 additional cybersecurity enhancements.

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.

For More Information

If you have questions or concerns, please call us at 888-498-3994, Monday through Friday 9:00 a.m. - 5:30 p.m., Eastern Time. We sincerely apologize for this situation and any concern or inconvenience it may cause you.

Sincerely,

James T. Doherty
Managing Executive
TPG Architecture
888-498-3994

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 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

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. *For District of Columbia Residents:* You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, DC 20001, (202) 727-3400, www.oag.dc.gov.
5. *For 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, (515) 281-5164, www.iowaattorneygeneral.gov.
6. *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, marylandattorneygeneral.gov.
7. *For 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov. In addition, New Mexico consumers 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. For more information about New Mexico consumers obtaining a security freeze, go to https://www.ffnm.org/_kcms-doc/1254/38712/Credit-Freeze-Q-A-New-Mexico-Sept-2017.pdf.

8. *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or <https://ag.ny.gov/internet/resource-center>; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or <https://dos.ny.gov/consumer-protection>.
9. *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, (877) 566-7226, www.ncdoj.gov.
10. *For 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, (877) 877-9392, www.doj.state.or.us/.
11. *For 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:
<https://www.experian.com/freeze/center.html>
- Transunion:
<https://www.transunion.com/credit-freeze>

Mailing addresses for the credit reporting agencies are provided above. Credit reporting agencies may 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.