



Jackson Lewis P.C.
666 Third Avenue
29th Floor
New York, NY 10017
(212) 545-4063
www.jacksonlewis.com

Damon W. Silver
Direct: (212) 545-4063
damon.silver@jacksonlewis.com

By Email: idtheft@oag.state.md.us

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

Re: Data Incident Notification¹

February 23, 2024

Dear Sir or Madam:

We are writing to notify your office that New York Public Interest Research Group (“NYPIRG”) was the subject of a criminal cyberattack (the “Incident”) that impacted one (1) NYPIRG laptop. The Organization immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope and the identities of those the Incident may have affected.

Through its extensive investigation, NYPIRG determined that a limited set of files stored on the impacted laptop may have been subject to unauthorized access. The Organization then undertook the time- and resource-intensive step of reviewing the contents of those files to determine whether they contained personally identifiable information (“PII”) and to identify the data subjects to whom that PII related.

On or about January 19, 2024, NYPIRG determined that, on or about October 6, 2023, files containing PII related to one (1) Maryland resident may have been accessed by the bad actor. The Organization has not found any evidence that this information was misused as a result of the Incident. Out of an abundance of caution, and in accordance with applicable law, the Organization will provide notice to the affected Maryland resident, in the form enclosed as Exhibit A, so that they can take steps to minimize the risk that their information will be misused.

As set forth in the enclosed letter, NYPIRG has taken a number of steps to further secure its systems. Specifically, it has examined all company devices, including staff computers, to ensure software is up to date; strengthened security measures on company devices to ensure that external installation of software is prohibited without internal IT approval; amended administrative safeguards, including procedures regarding use of personal computers for company business; and provided security

¹ Please note that New York Public Interest Research Group does not, by providing this letter, agree to the jurisdiction of the State of Maryland, nor waive its right to challenge jurisdiction in any subsequent actions.

training for management-level employees. The Organization is also in the process of engaging a third-party firm to conduct security training for all employees.

We 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.

Sincerely,

JACKSON LEWIS, P.C.

/s/ *Damon W. Silver*

Damon W. Silver

cc: Melissa Pascualini (Jackson Lewis P.C.)

4867-0605-1999, v. 4

EXHIBIT A



NYPIRG

NEW YORK PUBLIC INTEREST RESEARCH GROUP

To Enroll, Please Call: 1-800-939-4170
Or Visit: <https://app.idx.us/account-creation/protect>
Enrollment Code: <<Enrollment Code>>
Enrollment Deadline: May 31, 2024

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

February 22, 2022

Notice of Data Breach

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

What Happened

We are writing to notify you that New York Public Interest Research Group ("NYPIRG" or "the Organization") was the subject of a criminal cyberattack ("the Incident") that impacted one (1) NYPIRG laptop. The Organization immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope and the identities of those the Incident may have affected.

Through its extensive investigation, NYPIRG determined that a limited set of files stored on the impacted laptop may have been subject to unauthorized access. The Organization then undertook the time- and resource-intensive step of reviewing the contents of those files to determine whether they contained personally identifiable information ("PII") and to identify the data subjects to whom that PII related.

On or about January 19, 2024, NYPIRG determined that, on or about October 6, 2023, files containing PII related to you may have been accessed without authorization. The Organization has not found any evidence that your information was misused as a result of the Incident.

What Information Was Involved

The impacted files may have contained your name, along with your address, date of birth, social security number, and/or health insurance information.

What We Are Doing

Out of an abundance of caution, 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.

9 Murray Street, Lower Level • New York, NY 10007 • (212) 349-6460 • Fax (212) 349-1366
Regional Offices in: Capital District & Hudson Valley, Long Island & New York City, Western & Central New York

NEW YORK PUBLIC INTEREST RESEARCH GROUP FUND • NYPIRG.ORG

As an added precaution, we are offering identify theft protection services through IDX, A ZeroFox Company, a data breach and recovery services expert. IDX identity protection services include 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the enrollment code provided above. IDX representatives are available Monday through Friday from 9:00 am to 9:00 pm Eastern Time.

NYPIRG treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since the Incident, the Organization has taken a number of steps to further secure its systems. Specifically, it has examined all company devices, including staff computers, to ensure software is up to date; strengthened security measures on company devices to ensure that external installation of software is prohibited without internal IT approval; amended administrative safeguards, including procedures regarding use of personal computers for company business; and provided security training for management-level employees. The Organization is also in the process of engaging a third-party firm to conduct security training for all employees.

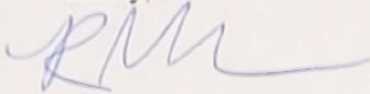
What You Can Do

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

We apologize for any inconvenience this Incident may cause you. If you have additional questions, please contact us at (518) 436-0876 or rhaven@nypirg.org.

Sincerely,



Russ Haven
General Counsel

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

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
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
800-525-6285
securitymonitoring@equifax.com
m

Experian
Experian Security Assistance
P.O. Box 9554
Allen, TX 75013
888-397-3742
businessrecordsvictimassistance@experian.com
m

TransUnion
Consumer Relations &
Fraud Victim Assistance
P.O. Box 2000
Chester, PA 19016
800-372-8391
databreach@Transunion.com
m

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, 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 Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

5. *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>.