NIP Management Services, LLC
c/o Cyberscout
<Return address>
<city><state><zip>

<FirstName> <LastName>
<Address1> <Address2>
<City><State><PostalCode+4>

May x, 2025

Dear <<FirstName>> <<LastName>>:

NIP Management Services, LLC. regrets to inform you that we discovered a data incident which may have resulted in unauthorized acquisition of your personal information as the result of a cyber-attack. While we are not aware of any misuse of your information, we are providing this notice to inform you of the Incident and to call your attention to steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

We sincerely apologize for any inconvenience this may cause you and assure you that we have and continue to deploy measures to avoid these kinds of incidents from happening.

What Happened?

As a result of a phishing attack, a single email account was intermittently compromised by an unknown external third party between June 24 and July 19.

What Information Was Involved?

The elements of personal information involved included **[name, drivers' license, state identification number, Social Security number, and medical information]**. We found that no credit card or financial account information was included in the Incident.

What We Are Doing?

Upon learning of the incident, we took prompt steps to secure our systems and investigate the incident, which included engaging a forensic services company. We then conducted a lengthy, detailed, and thorough review of the emails and files that may have been compromised, and discovered on March 14 that emails in that account acquired by that third party included certain personal information. Upon discovering that personal information may have been compromised, we identified our legal obligation and began to arrange for notification of potentially affected individual as soon as possible, which included, preparing this letter and the attached sheet that describes steps you can take to protect your identity, credit and personal information.

We are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no cost to you. These services provide you with alerts for <Service Length> from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, dedicated call center will be available to provide you guidance on credit monitoring enrollment and identity theft protection services. The call center will include a trained support team to address inquiries concerning the incident as well. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

Enrollment in Credit Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<UniqueCode>**.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do?

The attached sheet describes steps you can take to protect your identity, credit and personal information. We also recommend you enroll in the ID theft resolution and credit monitoring services described above.

For More Information?

Again, we apologize for this situation. We work hard to treat all personal information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring. Unauthorized accesses to personal information are difficult to prevent in all instances, however, we will be reviewing our systems and making improvements where we can to minimize the chances of this happening again. This includes reviewing how we store information, how we train employees, and related safeguards.

If you have questions, you should call me at 1-800-405-6108, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding major U.S. holidays

Sincerely,

NIP Management Services, LLC

What You Should Do To Protect Your Personal Information

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

1. We recommend you closely monitor your financial accounts and access resources concerning identity theft, such as information the Internal Revenue Services has published at: http://www.irs.gov/Individuals/Identity-Protection, and well as https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

2. Contact the nationwide credit-reporting agencies as soon as possible to:
   - Add a fraud alert statement or security freeze 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.
   - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
   - Obtain a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com/consumer	www.transunion.com

3. Please review all bills and credit card statements closely to determine whether you have been charged for items you did not contract for or purchase. 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 delay their use of stolen personal information.

4. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission ("FTC"). You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 1-877-IDTHEFT (1-877-438-4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

5. *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, https://www.marylandattorneygeneral.gov/.

6. *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/; or 2)

NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.