

2016 APR 28 7 11 58

NewLeaders 

Attorney General Brian E. Frosh  
Attorney General of Maryland  
200 St. Paul Place  
Baltimore, MD 21202

April 15, 2016

VIA FIRST CLASS MAIL

Dear Mr. Attorney General:

I am writing on behalf of New Leaders regarding an incident that occurred on March 17, 2016, in which employee and former employee W-2 Forms from 2014 and 2015 were disclosed to an unknown party in response to a “spoofed” email that appeared to come from an authorized internal New Leaders’ email account. Pursuant to Section 36a-701b of the §§14-3504 – 14-3508 of the Maryland Code, Commercial Law, we notified affected Maryland residents in a letter dated March 22, 2016 that was distributed by U.S. mail and email (when available). I am enclosing a copy of the notification letter.

New Leaders has investigated the cause of the disclosure as well as the scope of the information disclosed. We are actively reviewing the incident and discussing appropriate steps to address the cause of this disclosure. In particular:

- We are communicating and cooperating with federal, state, and local law enforcement and tax authorities including the IRS Cyber Crimes Unit, the Federal Bureau of Investigation, and the U.S. Secret Service.
- We are reviewing protocols for handling of sensitive information with applicable staff.
- We are reviewing our technology systems to consider any upgrades that might be needed.
- We have established a dedicated email address for all affected individuals.

It appears that the personal information of 34 Maryland residents was included in the disclosed information. Notice has not been delayed because of a law enforcement investigation. To protect affected individuals, New Leaders is offering identity protection services from AllClear ID for 24 months from the date of the notice.

If you have any questions relating to this incident, please do not hesitate to contact me.

Sincerely,



Laura B. Kadetsky  
General Counsel

Enclosures: Notice of Data Breach dated March 22, 2016

[REDACTED]

---

**From:** Jean Desravines  
**Sent:** Tuesday, March 22, 2016 4:03 PM  
**To:** [REDACTED]  
**Subject:** Re: Notice of Data Breach

**By Email and Hard Copy**

Dear [REDACTED]

I am writing to you about an extremely serious situation which was brought to our attention late last week regarding an email scam targeting New Leaders resulting in a data breach. This data breach included the W-2 information of New Leaders personnel, and unfortunately your information was included in this breach. The intent of this letter is to share what we are doing to address it, and to provide some information and resources for steps you can take to protect your personal information.

Given the nature of this issue for our personnel, we have given addressing it top priority. Our people are our highest priority, because you allow us to work toward our mission in support of all students. The privacy and protection of your personal information is a matter we take very seriously. We began investigating the incident as soon as we became aware of it and are working closely with law enforcement as well as our service providers to investigate the breach. We are also prepared to provide identity protection services should you choose to enroll.

**What Happened**

We have learned that a cybercriminal using a spoofing scam led to an unauthorized third party obtaining certain W-2 information from 2014 and 2015 for New Leaders current and former employees. Based on our review of the information that was disclosed, we understand that your W-2 form was among the information obtained by the third party. We swiftly began investigating the incident as soon as we became aware and are working closely with a range of law enforcement authorities to investigate and respond. While our specific case remains under investigation, similar cases have been widely reported in the press in recent months.

**What Information Was Involved**

The information in your W-2 form was disclosed to the third party. This includes your name, social security number, and address.

**What We Are Doing**

New Leaders has investigated the cause of the disclosure as well as the scope of the information disclosed. We are actively reviewing the incident and discussing appropriate steps to address the cause of this disclosure. In particular:

- We are communicating and cooperating with federal, state, and local law enforcement and tax authorities including the IRS Cyber Crimes Unit, the Federal Bureau of Investigation, and the U.S. Secret Service.
- We are reviewing protocols for handling of sensitive information with applicable staff.
- We are reviewing our technology systems to consider any upgrades that might be needed.
- We have established a dedicated email address – [cyberissue@newleaders.org](mailto:cyberissue@newleaders.org) – for all affected individuals to send in questions.

**What You Can Do**

We recommend that you take the following steps:

- Call the IRS identity theft number (1-800-908-4490) to determine if a fraudulent tax return has been filed under your name.
- Complete and file IRS Form 14039, Identity Theft Affidavit (available at <https://www.irs.gov/pub/irs-pdf/f14039.pdf>). Instructions for filing this form are included at that link.
- If you have been unfortunately impacted by tax fraud, please take the additional action steps outlined in the document from the IRS titled "Identity Theft Information for Taxpayers" (available at <https://www.irs.gov/pub/irs-pdf/p5027.pdf>).
- If you receive a tax refund in response to a tax return that you did not file, including a cashier's check or a pre-paid card, please send the cashier's check or pre-paid card to the following address to be voided:
  - Jeremy Tendler
  - Special Agent
  - IRS-Criminal Investigation
  - 915 Lafayette Blvd., Suite 215
  - Bridgeport, CT 06604
- As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice, and you can use them at any time through March 22, 2018.
  - AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.
  - AllClear PRO: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at [enroll.allclearid.com](http://enroll.allclearid.com) using the following redemption code: 
  - Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.
- We recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.
- You may set up electronic protections or blocks to your Social Security account by visiting the Social Security Administration's online access portal (available at <https://secure.ssa.gov/RIL/SiView.do>).
- For more information, the attached Exhibit A includes contact information for the FTC and the national credit reporting agencies, as well as other disclosures and recommendations.
- Do not respond to any suspicious emails or internet requests for personal or sensitive information. Please contact our IT helpdesk at [helpdesk@newleaders.org](mailto:helpdesk@newleaders.org) if you receive any such requests.

### For More Information

We know that this news may be upsetting to learn, and we deeply regret any inconvenience or stress this incident might cause. The privacy and protection of your information is a matter we take very seriously. We realize that you may have questions as to what this means and what you can do to protect yourself. For additional information, you may contact (1) Laura Kadetsky, General Counsel, at [lkadetsky@newleaders.org](mailto:lkadetsky@newleaders.org) or (202) 315-2037; or (2) [cyberissue@newleaders.org](mailto:cyberissue@newleaders.org). While you should feel free to contact Laura at any time, she will hold open sessions for you to call her individually at the following times, and you should reach out to her by email to reserve a slot within these times:

- Wednesday, March 23, 1:00-4:00pm ET
- Thursday, March 24, 1:30-4:30pm ET
- Friday, March 25, 12:30-2:30pm ET

Your trust is a high priority for the organization and me personally. I sincerely apologize for any inconvenience or difficulty this issue may cause. As someone whose information was also taken as part of this cybercrime against New

Leaders, I share your frustration and concern. We strongly encourage you to take the preventive measures outlined in this letter to help prevent, detect, and report any misuse of your information.

Jean

## Exhibit A - Additional Information

### STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

You may wish to visit the website of the U.S. Federal Trade Commission at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or reach the FTC at 1-877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft.

We recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission.

To file a complaint with the FTC, go to [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

### FRAUD ALERTS AND SECURITY FREEZES

You may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. A fraud alert permits creditors to get your report as long as they take steps to verify your identity. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit report, you need to send a request to each national credit reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee (up to \$5.00 for Massachusetts residents) to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the national credit reporting agency. Visit the websites of each consumer reporting agency for more information about placing a freeze, as they may have different requirements depending on the state in which you reside.

### CONTACT INFORMATION FOR THE THREE NATIONAL CREDIT REPORTING AGENCIES

Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 680-7289
<a href="http://www.equifax.com">www.equifax.com</a>	<a href="http://www.experian.com">www.experian.com</a>	<a href="http://www.transunion.com">www.transunion.com</a>
P.O. Box 740241	P.O. Box 9532	Fraud Victim Assistance Division
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 6790
		Fullerton, CA 92834-6790

### COPY OF CREDIT REPORT

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You may also elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies.

### ADDITIONAL STATE REQUIREMENTS

**California Residents:** Your receipt of this notice has not been delayed as the result of any law enforcement investigation activity.

**Maryland Residents:** You may contact the Office of the Maryland Attorney General at 1 (888) 743-0023 by visiting the website <https://www.oag.state.md.us/> or by writing to the Office of the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can obtain information on the steps you can take to avoid identity theft from the FTC and the Office of the Maryland Attorney General.

**Massachusetts Residents:** Under Massachusetts law, you have the right to obtain any police report filed in regard to the incident.

**North Carolina Residents:** You may contact the North Carolina Attorney General's Office at 919-716-6400, or by visiting the website <http://www.ncdoj.gov>, or by writing to the Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001.