NATIONAL EDUCATION ASSOCIATION
nea.org
Great Public Schools for Every Student

1201 16th St., N.W. | Washington, DC 20036 | Phone: (202) 833-4000

Notice of Data Breach

January 21, 2020

Name
Street Address
City, State Zip Code

Dear [NAME]:

We are writing to notify you of a recent incident that may affect the security of your personal information. This letter will provide you with information concerning the event, measures we have taken since discovering the incident, and suggestions on how to protect your personal information.

What Happened? NEA recently became aware of suspicious activity related to an employee e-mail account. We immediately blocked further access to the affected account, and conducted an investigation to determine the reason for the suspicious activity. With the assistance of forensics experts, we determined that the employee's account was accessed without authorization from November 13-15, 2019.

Upon learning this information, we performed a comprehensive review of the affected e-mail account to determine whether it contained any personal information. This review found that the compromised e-mail account held documents containing the full names and social security numbers of some individuals.

While we are unable to determine whether any bad actors viewed this information, it was potentially accessible at the time of the incident. Because your information was present in the compromised e-mail account, we are notifying you in an abundance of caution so that you can take appropriate steps to protect your personal information.

What Information Was Involved? We cannot confirm whether any information was viewed by the unauthorized individual(s). However, NEA's investigation confirmed that information

present in the account at the time of the incident included your full name and social security number.

What We Are Doing. NEA values your privacy and deeply regrets that this incident occurred. We have security measures in place that allowed us to quickly identify and contain this incident, and we continue to confirm and strengthen the security of our systems. We have also provided relevant regulatory notices.

We are notifying potentially affected individuals, including you, so that you can take further steps to protect your information. To assist you in doing so, we have secured the services of CyberScout to provide identity monitoring services at no cost you for 18 months. To learn more about these services, including how to sign up, please review the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud."

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud." This document contains instructions on how to activate the free identity monitoring services we are making available to you, as we are unable to activate those services on your behalf. It also provides information on additional steps you can take to protect your personal information, including contact information for regulators and credit reporting agencies that may be able to provide assistance.

For More Information. If you have questions about this incident that are not addressed in this letter, please contact Rose Futchko at 202-822-7535 between 9:00 a.m. – 5:00 p.m. EST, Monday through Friday.

You may also write to us at:

Rose Futchko
Director, Information Technology Services
National Education Association
1201 16th Street, N.W., Suite 511
Washington, D.C. 20036

Sincerely,

Rose Futchko
Director, Information Technology Services

Steps You Can Take to Protect Against Identity Theft and Fraud

Take Advantage of Free Credit Monitoring Services. NEA has arranged with CyberScout offer credit monitoring services for 18 months at no cost to you. This service includes Single Bureau Credit Monitoring, a Single Bureau Credit Report, and Cyber Monitoring.

To take advantage of this offer, log on to https://www.myidmanager.com within 12 months from receipt of this letter and follow the instructions provided. You will need to provide the following unique code to receive services: <CODE HERE.> For further guidance with the CyberScout services, please call the CyberScout help line 1-800-405-6108 and supply the fraud specialist with your unique code.

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. We recommend that you remain vigilant by reviewing your account statements. 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.identitytheft.gov, or call 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. 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.

Monitor Your Free Credit Reports. You should also remain vigilant about monitoring your 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 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.

Contact information for the three national credit reporting agencies is provided below:

Equifax	Experian	TransUnion
(888) 766-0008	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19106

Place a Fraud Alert and/or Security Freeze. We recommend placing a fraud alert on your credit report. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. The initial fraud alert stays on your credit report for one year, and you can renew it after one year. To place a fraud alert on your credit report, contact any one of the three credit reporting agencies listed above. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts.

You may also want to consider placing a "security freeze" on your credit report, which will prevent potential creditors from obtaining your credit report. That makes it less likely that an identify thief can open new accounts in your name. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Should you wish to place a security freeze, please contact each of the major consumer reporting agencies listed above.

File Your Taxes Early. File your taxes before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.

Be Alert for Telephone Scams. Do not believe anyone who calls and says you will be arrested unless you pay for taxes or debt—even if they have part or all of your Social Security number, or they say they are from the IRS.

Further Educate Yourself on Avoiding Identity Theft. You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, the Internal Revenue Service, or your state Attorney General. For example, you may wish to review *Identity Theft: A Recovery Plan*, a comprehensive guide from the FTC to help you guard against and deal with identity theft, along with other tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit www.identitytheft.gov, or call 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The IRS also has guidance concerning identify protection at https://www.irs.gov/identity-theft-fraud-scams.