LEARN. TEACH. LEAD.

1703 North Beauregard Street
Alexandria, VA 22311–1714 USA
1-703-578-9600 or 1-800-933-2723
1-703-575-5400 (fax)
www.ascd.org

**February 22, 2018: Notice of Data Breach**

Please be advised that on February 21, 2018, ASCD discovered it experienced an electronic/email communications scam intended to steal data, otherwise known as a "spear-phishing attack". This scam resulted in your W-2 form being acquired by an unknown third party. The personal information on a W-2 includes your name, address, and social security number.

We are sending this notice to inform you as to ASCD's actions and provide information so that you can take steps to protect yourself and minimize the possibility that your information will be misused. We are taking this breach very seriously, knowing the impact it may have on our team. We are aggressively working to protect you and enacting additional measures to ensure similar incidents will not happen in the future.

**What Information Was Involved**

The personal information that may have been acquired (as we cannot verify that it was received- only that it was accessed) includes your name, address, and social security number. While we maintain other employment information, including bank account information to process payroll and direct deposit, this information was not affected by this incident.

**What We Are Doing to Protect You**

Immediately upon discovering the disclosure, we commenced an investigation, including contacting appropriate law enforcement, including the Internal Revenue Service. We are working with our IT department to assist with our investigation and remediation and have retained the services of an attorney who specializes in cyber-attacks.

We are not aware of any information being used improperly at this point in time. However, our research shows that, following such attacks, some employees may experience unauthorized use of their personal information in connection with fraudulent tax filings. This notification has not been delayed because of any law enforcement investigation.

We are sending this advisory to make you aware of this incident so that you can take steps to protect yourself and minimize the possibility of misuse of your information. The attached sheet describes steps you can take to protect your identity, credit and personal information. In particular, we include information concerning IRS resources that can assist if you experience tax-related identity theft.

LEARN. TEACH. LEAD.

1703 North Beauregard Street
Alexandria, VA 22311–1714 USA
1-703-578-9600 or 1-800-933-2723
1-703-575-5400 (fax)
www.ascd.org

In addition to notifying the IRS and FBI, we are required to inform each of the states in which you reside. This is in the process of being completed.

To further protect you, we are arranging to provide credit monitoring and related services for two years at no cost to you. Details will be provided shortly.

**What You Can Do**

There is a series of steps below this letter that you can take to protect your identity, credit, and personal information. We have also provided a Question and Answer attachment to provide detailed information to you about this unfortunate incident as well as steps and processes available to protect your identity. Please review this important information.

ASCD values your privacy and, as a company, we take the requisite precautionary measures to treat all employee information in a confidential manner and are proactive in the careful handling of such information. We will continue to assess and modify our privacy and data security policies and procedures. While we cannot guarantee that theft of data and similar incidents will never occur, we are committed to continuously review our systems and make improvements, as needed, to minimize the chances of this happening again.

If you have questions please contact Doug Parks (doug.parks@ascd.org) or Dana Williams (d_williams@ascd.org).

Sincerely,

Deb Delisle
CEO and Executive Director

Noah Raskin
Chief Financial Officer

**PLEASE READ BELOW FOR ADDITIONAL INFORMATION**
**PLEASE READ the Q/A ATTACHMENT FOR ADDITIONAL DETAILS**

## What You Should Do to Protect Your Personal Information

We recommend you remain vigilant and strongly 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. As discussed in the Taxpayer Guide to Identity Theft, IRS Form 14039 can be filed with the IRS to report potential identity theft concerning your federal taxes. You also may want to check with the state(s) in which you file.

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 can also obtain information from the FTC about fraud alerts and security freezes. You may contact the FTC by visiting www.ftc.gov or www.consumer.gov/idtheft, calling (877) 438-4338, or writing to the FTC at the address below. If you suspect or know that you are the victim of identity theft, you should contact local police. You can also report such activity to the Fraud

Department of the FTC, which will collect all relevant information and make it available to law-enforcement agencies. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

5. North Carolina Residents: To obtain additional information about avoiding identity theft, please contact the North Carolina Attorney General's Office at: Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001. Phone: (919) 716-6400. Website: http://www.ncdoj.gov/Home/ContactNCDOJ.aspx.

6. Maryland Residents: To obtain additional information about avoiding identity theft, please contact the North Carolina Attorney General's Office at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, Phone: (410) 576-6300, Toll-Free (in Maryland): (888) 743-0023, Website: https://www.oag.state.md.us/contact.htm.