Personal Data Security Incident Frequently Asked Questions
revised May 10, 2016

1. What happened? On April 12, 2016, W-2 information for 2015 was forwarded to a fraudulent e-mail address by a Washington Elementary School District (WESD) employee. Current and former employees who received a W-2 for 2015 from the WESD were impacted.

2. How did this happen? The release of information was the result of a phishing scam in which a District employee received an e-mail request from what appeared to be the valid e-mail address of the superintendent. The message requested the employee to send W-2 information for all District employees via e-mail. The District employee unknowingly replied to the fraudulent e-mail address and attached a report with calendar year 2015 W-2 information for current and former District employees. The employee received a second request for information, became suspicious and alerted a supervisor.

3: What is a spoofing e-mail?/What is a phishing e-mail? E-mail spoofing is the creation of e-mail messages with a forged sender address. E-mail phishing is the attempt to acquire sensitive information, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

4. What information about me was compromised? If you received a 2015 W-2 from the WESD, then your name, mailing address, Social Security number (SSN), wages and withholding information that appears on the W-2 was compromised.

5. Was my Social Security number compromised? Yes, If you received a 2015 W-2 from the WESD, then your Social Security number was included on the W-2 document that was forwarded to a fraudulent e-mail address.

6. Were Social Security numbers of dependents released? No

7. Was banking information released? No

8. Was my date of birth released? No

9. **Am I the only one this happened to?** No, other people were also affected and the District has notified them as well. Current and former employees who received a W-2 for 2015 from the WESD were impacted.

10: How do I know if my information was one of those released? You received the notification because the WESD has confirmed that your 2015 W-2 information was inadvertently released.

11. **There are fraudulent charges on my credit/debit card. What do I do?** Contact the financial institution that issued the credit/debit card right away and let them know of the fraudulent charges. They will provide you with the instructions to have the fraudulent charges disputed and how to have a new account issued to avoid any further unauthorized activity. Activate your ProtectMyID membership. Information on this service was mailed on April 22 to employees and former employees affected by this incident.

12. What if I have not received a notification? All current employees were informed via e-mail on Wednesday, April 13. Letters were mailed via USPS on April 14 to all current and former employees impacted by this incident. If you were an employee of the WESD in 2015 and your address is current with the WESD, you should have received a letter.

If you are a current employee and have moved but not updated your address, please go to the WESD Web site (wesdschools.org), click on “staff” and update your information on the Employee Self Service section so you can receive any future notifications.

If you were employed by the WESD in 2015 but are no longer an employee of the District and have moved, please e-mail your name, current address and phone number to finance.announcements@wesdschools.org.

13: Have there been any reports of misuse? WESD is aware of a limited number of affected employees who informed us that they had an issue with the electronic filing of their 2015 tax returns**.**

14. How has the District responded to the incident?
The WESD took immediate action on April 12, the day of the release, by informing the IRS and Phoenix Police. Initial correspondence from the District was sent to current employees via e-mail on April 13. Principals communicated the information during professional learning community (PLC) meetings Wednesday afternoon, April 13. Principals and department supervisors were asked to make certain that employees checked their e-mail Wednesday afternoon. A letter was mailed to current and former employees impacted by the incident on April 14. An e-mail was sent to current employees on April 15. Additional information is being sent out as well. Please visit the WESD Web site at wesdschools.org. There you will see a link called "Personal Data Security Incident" under the heading "quick links." Updated information will be posted there.

15. What steps has the District taken in response to the incident? Upon realizing the e-mail address was fraudulent, WESD immediately began to take corrective actions. The District has notified the Internal Revenue Service (IRS), the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center, Phoenix Police Department, Arizona Attorney General's Office and the Arizona State Retirement System (ASRS) to report this incident. The computer involved was quarantined and a detailed search of the computer was conducted. The fraudulent e-mail address was blocked and MIS checked for other fraudulent requests. Administration is reviewing policies and procedures, including focused, annual training for employees, and evaluating additional security controls to prevent this type of event from occurring again.

16. What steps should I consider taking?

- **PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE**

An **initial 90 day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should takes steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax	**Experian**	**TransUnion**
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

- **REGARDING YOUR 2015 TAXES**

The IRS Web site states: "If you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov.
- complete IRS form 14039, identity theft affidavit, if your efiled return is rejected because of a duplicate filing under your Social Security number or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions.
- continue to pay your taxes and file your tax return, even if you must do so by paper.

If you previously contacted the IRS and did not have a resolution, contact them for specialized assistance at 1-800-908-4490."

- **SOCIAL SECURITY ADMINISTRATION (SSA):**

If you have not already created an account with SSA, WESD encourages you to register online at SSA.gov or call 1-800-772-1213.

- **ARIZONA DEPARTMENT OF REVENUE:**

The Department of Revenue Web site has an extensive section on identity theft, including information on what to do if you suspect you are a victim of identity theft and resources available to you: https://azdor.gov/IdentityTheft.aspx.

If you know you have been the victim of identity theft, contact the Arizona Department of Revenue at 602-255-2060 to report it.

- **ARIZONA STATE RETIREMENT SYSTEM (ASRS)**

If you have not already created an account with ASRS, WESD encourages you to register online for an ASRS account at azasrs.gov or call 602-240-2000. This will allow you to review your ASRS account information and monitor your ASRS activity.

- **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE**

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

Visit www.annualcreditreport.com or call 877-322-8228.
Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

- **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

- **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**
  - Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.
  - The Federal Trade Commission has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

17. What can I do to protect myself from identity theft? The Federal Trade Commission has compiled helpful information on steps you can take to avoid or detect identity theft. Visit their Web site at www.ftc.gov/bcp/edu/microsites/idtheft/ or you can call their hotline at 1-877-IDTHEFT (438-4338). (*This information is located in the letter that the caller received)* In addition, you should regularly review statements from your accounts and you may obtain a free copy of your credit report once every 12 months from any of the three national credit reporting agencies.

18. Will Washington Elementary School District pay for a credit monitoring service for me? Yes, the WESD has insurance coverage for this type of event. That coverage includes one year of credit monitoring service that you can activate if you are one of the affected parties. To help protect your identity, the WESD is offering a one-year membership of Experian's® ProtectMyID® Alert. This service helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft.

19: What happens after my credit monitoring service expires? WESD's insurance company is covering the cost for one year of credit monitoring. After the year of service is over, you may choose to continue service at your own expense.

20. Should I add a fraud alert to my credit file? Because this event included the release of personally identifiable information (like Social Security numbers), WESD recommends you contact one of the three major credit bureaus and ask them to place a "fraud alert" on your file if you are one of the affected parties:

Equifax at 1-877-478-7625 or www.equifax.com
Experian at 1-888-397-3742 or www.experian.com
TransUnion at 1-800-680-7289 or www.transunion.com

21. What is the purpose of a fraud alert? A fraud alert tells creditors to contact you before they open a new credit account under your Social Security number.

22. Should I check my credit report? Yes. It is advisable for people to regularly monitor their credit reports. Every consumer can receive one free credit report every 12 months by contacting one of the three national credit bureaus or through the Annual Credit Report Service by visiting http://www.annualcreditreport.com or calling them at 877-322-8228.

23. How will placing a fraud alert on my credit file affect my ability to apply for credit? The lender may attempt to contact you and may request additional identifying documentation to verify you are who you claim to be. That could slow the lending process, but should not prevent it from being completed.

24. Does this mean I am a victim of identity theft? No. The fact that someone may have had access to personal information does not mean that you are a victim of identity theft, or that the personal information will be used to commit fraud. The WESD wants you to know about the incident so that you can take appropriate steps to protect yourself, such as reviewing your account statements and credit reports closely for unauthorized activity and reporting any unauthorized activity to your credit card company.

25. With regard to my 2015 taxes, what actions should I take?
If you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov.
- Complete IRS Form 14039, Identity Theft Affidavit, if your efiled return is rejected because of a duplicate filing under your Social Security number or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.

If you previously contacted the IRS and did not have a resolution, contact them for specialized assistance at 1-800-908-4490.

26. I received a letter from the IRS saying a "transcript" was requested; however, I did not make such a request. What does that mean and what should I do? Tax transcripts are often used to validate your income and tax filing status for things such as mortgage applications, student loans and small business loan applications. There are several types of transcripts. Two common types of transcripts are tax return transcripts and tax account transcripts.
Tax Return Transcript – shows most line items from your tax return as it was originally filed, including any accompanying forms and schedules. A return transcript usually meets the requirements of lending institutions offering mortgages and student loans.
Tax Account Transcript – shows basic data including return type, marital status, adjusted gross income, taxable income, credits and payments. It also shows adjustments made by you or the IRS after you filed the return.
The IRS Web site provides information on tax transcripts. We suggest you review that information and, if necessary, act according to your specific circumstances.
To request a transcript and FAQs about transcripts: https://www.irs.gov/Individuals/Get-Transcript
(See answer 16 concerning filing IRS form 14039, Identity Theft Affidavit)

27. I received the letter with information about ProtectMyID and my engagement number, but I misplaced it. What do I do? Please send an e-mail with your name and address to finance.announcements@wesdschools.org. We will forward

your information to the Trust, so that you can be mailed a new letter with your personalized engagement number.

28. I did not receive the letter with information about ProtectMyID and my engagement number. What do I do? Please send an e-mail with your name and address to finance.announcements@wesdschools.org. We will forward your information to the Trust, so that you can be mailed a letter with your personalized engagement number.

For further information, contact David Velazquez at 602-347-3506 or

finance.announcements@wesdschools.org