Return Mail Processing
PO Box 999
Suwanee, GA 30024

1 1 119 **********SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN US 12345-6789

February 12, 2026

Dear Sample A. Sample:

On February 3, 2026, PLOS discovered it experienced a spear-phishing attack that resulted in an email containing your 2025 W-2 Form being sent to an unknown third party. We sincerely apologize for this incident and the disruption caused to you, and we assure you that we have and continue to deploy measures to avoid these kinds of incidents from happening.

What happened

A phishing email sent to PLOS on February 3, 2026 was mistakenly responded to, providing copies of US employees' 2025 W-2 tax forms. The W-2 form includes your social security number, residential address, salary and tax withholding information. The incident was reported immediately, and we began investigating the same day.

What information was involved

The personal information that was involved is your Form W-2 for 2025, which includes your name, residential address, social security number, salary and tax information. We maintain this and other employment information about you, including bank account information, to process payroll and direct deposit. However, only the information in the W-2 form was affected by this incident. Your bank account information has not been compromised.

What we are doing to protect you

Immediately upon discovering the disclosure, we commenced an investigation, including contacting appropriate law enforcement, such as the Internal Revenue Service (IRS) and the Federal Bureau of Investigations. Based on our report to the IRS, they will begin a risk assessment that may include monitoring taxpayer accounts for signs of identity theft.

We are working with our Digital team to assist us with our investigation and remediation. We are not aware of any information being used improperly, however, our research shows that following these attacks some employees may experience unauthorized use of their personal information in connection with fraudulent tax filings.

We are sending this advisory to you 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 below information concerning IRS resources that can assist you if you have experienced tax-related identity theft.

Additional steps you can take

The attached sheet describes steps you can take to protect your identity, credit and personal information.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** May 29, 2026 by 11:59 pm UTC (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/1Bcredit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by May 29, 2026 at (833) 931-7577 Monday – Friday, 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.

- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For more information

Again, we apologize for this incident. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring and we will be reviewing our systems and making improvements where we can to minimize the chances of this happening again. This includes redoubling our efforts on training to recognize these kinds of attacks.

If you have questions, please feel free to contact me at supegui@plos.org or call 1-415-624-1200.

Sincerely,

Sandra M. Upegui

Sandra M. Upegui
General Counsel & Data Privacy Officer

PLEASE SEE ATTACHED FOR ADDITIONAL INFORMATION

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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, https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft and https://www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works. **As discussed in the Taxpayer Guide, IRS Form 14039 can be filed with the IRS to report potential identity theft concerning your federal taxes (https://www.irs.gov/dmaf/form/f14039). 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 security alert to your credit report. You only need to contact one of the three agencies listed below and your request for a security alert will be shared with the other two agencies. This security alert will remain on your credit file for a year. You can also place a security freeze on your credit report but you will need to contact each agency separately for a security freeze.
   - 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, how to avoid identity theft, and 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. 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. You can also obtain such information from state attorneys general and law enforcement, including the New York Attorney General's Office which you can contact by calling (800) 771-7755, or going to https://ag.ny.gov/consumer-frauds/identity-theft.

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/