Return Mail Processing
PO Box 999
Suwanee, GA 30024

April 15, 2026

Re: Notice of Data Security Incident

Dear [redacted],

We are writing to notify you of a data security incident at the University of Pennsylvania ("Penn" or "University") that involved some of your personal information. We are sending this letter to tell you what happened, what information was involved, what we are doing in response, and what you can do should you feel it is appropriate to do so. Penn takes this incident very seriously. Protecting our community is of utmost importance, and we are committed to maintaining the privacy and security of your information.

What Happened?

On October 31, 2025, Penn became aware of unauthorized access to certain University systems through a user account. We immediately terminated the unauthorized access. An investigation was launched with the assistance of cybersecurity experts. We also notified law enforcement. Based on our investigation, we determined that certain files had been downloaded as part of the unauthorized activity. Some of these files included contact and demographic information about alumni, donors, students, and employees. We conducted a multi-stage review of those files to identify personal information and to whom it belonged. Our review is now complete.

What Personal Information Was Involved?

Based on our review of the data, on March 6, 2026, we determined that your [redacted] was included in the files that were downloaded. Although [redacted] are often publicly available from government sources and ancestry and genealogy websites, some state laws require you to be notified when [redacted] are downloaded. The files did **NOT** contain any other data requiring notification. They did **NOT** contain your bank account numbers, credit card numbers, Social Security Number, Driver's License Number, or other government identifiers.

What We Are Doing.

As detailed above, we notified law enforcement and an investigation was launched with the assistance of cybersecurity experts. Please be assured that we are taking steps to improve our information security program and systems.

What You Can Do.

To help protect your personal information, you may wish to take the following steps, all of which are good ideas in any event:

- Carefully review statements sent to you by your bank, credit card company, or other financial institutions as well as government institutions like the Internal Revenue Service. Notify the sender of these statements immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.

- The attached **Reference Guide** describes additional steps that you can take in certain situations and provides resources for additional information. We encourage you to read and follow these steps as well.

For More Information.

We sincerely regret that this incident occurred and any concern this may cause you. If you have any questions regarding this incident, please feel free to call the following dedicated number [redacted] Monday through Friday from 8 am - 8 pm Central Time. Be prepared to provide engagement number [redacted]

Sincerely,

The University of Pennsylvania
3451 Walnut Street
Philadelphia, PA 19104

REFERENCE GUIDE

If you suspect that you are a victim of identity theft or credit fraud, we encourage you to remain vigilant and consider taking the following steps.

1. Obtain and Monitor Your Free Credit Report.

U.S. residents are entitled under U.S. law to one free credit report annually from each of the 3 major credit bureaus. You can obtain a free copy of your credit report by calling 1-877-322-8228, visiting www.annualcreditreport.com, or by completing an Annual Credit Report Request Form on the FTC's website at www.ftc.gov and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/index.action. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the 3 national credit reporting agencies. Do not contact the 3 credit bureaus individually; they provide your free report only through the website or toll-free number. When you receive your credit report, review the entire report carefully for discrepancies. Verify all information is correct. Look for any inaccuracies and/or accounts you don't recognize, or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting company.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer credit reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumerfinance.gov or www.ftc.gov.

2. Implementing a Fraud Alert or Security Freeze on Your Credit File.

We recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any new accounts in your name. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name. To place a fraud alert, you can contact the 3 major credit bureaus at the addresses below to place a fraud alert on your credit report.

You have the right to place a "security freeze" on your credit file. A security freeze generally prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must contact the 3 credit bureaus below:

Equifax	**Experian**	**TransUnion**
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
(888) 766-0008	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following identifying information: (1) Your full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security Number; (3) Date of birth; (4) If you have moved in the past five (5) years, the addresses where you have lived over those prior five years; (5) Proof of current address such as a current utility bill or telephone bill; and (6) A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft. After receiving your freeze

request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

3. Additional Helpful Resources.

If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe you identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly. You may also contact the FTC for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 600 Pennsylvania Avenue, NW, Washington, DC 20580; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.