Morgan Lewis

Kristin M. Hadgis
Partner
+1.215.963.5563
kristin.hadgis@morganlewis.com

December 1, 2025

VIA EMAIL TO CONSUMER@AG.IOWA.GOV

Attorney General Brenna Bird
Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: The University of Pennsylvania – Notice of Security Incident

Dear Office of the Attorney General:

Morgan, Lewis & Bockius LLP represents the University of Pennsylvania ("Penn" or "University"). I am writing to notify your office of a data security incident in a third-party Oracle software application at Penn that impacted the information belonging to Iowa residents.

Penn uses a third-party software tool called Oracle E-Business Suite ("Oracle EBS") from Oracle, a third-party technology provider. Oracle EBS is a financial application used to process supplier payments, reimbursements, general ledger entries, and to conduct other University business. Oracle recently announced a previously unknown security vulnerability that could allow unauthorized access to Oracle EBS and data stored in it. This issue impacted hundreds of organizations worldwide that also use Oracle EBS. Upon learning of potential unauthorized access to Oracle EBS, Penn immediately launched an investigation with the assistance of cybersecurity experts and outside counsel. Penn also notified law enforcement and is cooperating with an ongoing federal law enforcement investigation. In the course of Penn's own investigation, Penn discovered that some data from Penn's Oracle EBS had been obtained without authorization. Penn then initiated a detailed review to determine whether any personal information was involved and to identify the affected individuals.

On November 11, 2025, Penn determined that the data from Penn's Oracle EBS contained certain personal information belonging to 752 Iowa residents. The types of personal information varied among affected residents including variations of full name, address, Social Security Number, and/or banking information. Penn is not aware of any evidence that personal information has been publicly disclosed or misused for fraudulent purposes as a result of this incident. Nonetheless, Penn began notifying the residents on December 1, 2025, via U.S. First Class Mail and is offering the residents two years of free credit monitoring and identity-theft protection services via Experian. A sample notice is attached as Attachment A to this letter.

Prior to the incident, Penn had a number of cybersecurity measures in place across its environment. Penn has taken steps to further reinforce its systems and cybersecurity controls, and it will continue with these efforts. If your office requires any further information in this matter, please feel free to contact me.

Regards,

Kristin M. Hadgis

Kristin M. Hadgis

ATTACHMENT A

Penn
University of Pennsylvania

Return Mail Processing
PO Box 999
Suwanee, GA 30024

[redacted]

December 1, 2025

Re: [redacted]

Dear [redacted]:

We are writing to notify you of a data security incident in a third-party Oracle software application at the University of Pennsylvania ("Penn" or "University") that involved some of your personal information. This letter is being sent to provide you with additional information and to advise you of services Penn is offering at no charge to you. **It is important to note that we have no evidence at this time that your information has been used for any purpose that could cause you any harm as a result of this incident.** Nonetheless, we are sending this letter to tell you what happened, what information was involved, what we have done, and what you can do should you feel it is appropriate to do so.

Penn takes this incident very seriously and sincerely apologizes to everyone affected. Protecting our community is of utmost importance, and we are committed to maintaining the privacy and security of your information.

What Happened?

Penn uses a third-party software tool called Oracle E-Business Suite ("Oracle EBS") from Oracle, a third-party technology provider. Oracle EBS is a financial application used to process supplier payments, reimbursements, general ledger entries, and to conduct other University business. Oracle recently announced a previously unknown security vulnerability that could allow unauthorized access to Oracle EBS and data stored in it. This issue impacted hundreds of organizations worldwide that also use Oracle EBS. Upon learning of potential unauthorized access to Oracle EBS, Penn immediately launched an investigation with the assistance of cybersecurity experts. We also notified law enforcement and are cooperating with an ongoing federal law enforcement investigation. In the course of Penn's own investigation, we discovered that some data from Penn's Oracle EBS had been obtained without authorization. We then initiated a detailed review to determine whether any personal information was involved and to identify the affected individuals. On November 11, 2025, Penn determined that your personal information was among the information obtained from Oracle EBS.

What Information Was Involved?

Based on our review of the data, we have determined that the impacted information included [redacted] We have found no evidence that any of this information has been or is likely to be publicly disclosed or misused for fraudulent purposes, or otherwise used in a way that could harm you as a result of this incident.

What We Are Doing.

Immediately upon learning of this incident, Penn launched an investigation with the assistance of outside cybersecurity experts, and in cooperation with law enforcement. We also promptly applied all security patches released by Oracle to address the vulnerability. Please be assured that we are working with cybersecurity experts to reinforce our systems to mitigate the risk of future unauthorized access to information.

[redacted]

We are also making resources available to those individuals whose information was involved. While we have no reason to believe that your information was misused for any fraudulent purposes as a result of this incident, we are providing you with access to complimentary Experian credit monitoring and remediation services for 24 months at no charge to you.

- **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.

To activate your membership and start monitoring your personal information, please follow these simple steps:

1) ENROLL by: [redacted] (Your code will not work after this date.)
2) VISIT the Experian IdentityWorks website to enroll: [redacted]
3) PROVIDE the Activation Code: [redacted]

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 at [redacted] by [redacted]. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity-restoration services by Experian. A credit card is not required for enrollment. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do.

To help protect your personal information, we strongly recommend you take the following steps, all of which are good ideas in any event:

- Enroll in the credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and social security number to establish credit and restoration assistance if you were not the one who initiated it. **To receive these complimentary services, you must enroll by** [redacted]
- 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 (IRS). 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 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 are committed to providing you with the necessary support and assistance. **If you have questions, please contact the dedicated call center toll-free at** [redacted] **Monday through Friday from 9 am - 9 pm Eastern Time (excluding major U.S. holidays).**

Sincerely,

The University of Pennsylvania
3451 Walnut Street
Philadelphia, PA 19104

* 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.

[redacted]

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.

Whether or not you choose to use the complimentary credit monitoring services, 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:

[redacted]

- 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.

District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the D.C. about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov.

Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5926.

Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, https://www.marylandattorneygeneral.gov.

Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

New Mexico Residents: Consumers have rights pursuant to the Fair Credit Reporting Act ("FCRA"), such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage consumers to review their rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
https://ag.ny.gov

NYS Department of State's Division of Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

North Carolina Residents: You can obtain information from the FTC and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the FTC. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge but note that consumer reporting agencies may charge fees for other services. Approximately [redacted] Rhode Island residents were impacted by this incident.

[redacted]