

Morgan Lewis

Gregory T. Parks

Partner
215.963.5170
gregory.parks@morganlewis.com

March 1, 2023

VIA EMAIL TO IDTHEFT@OAG.STATE.MD.US

State of Maryland
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
Attn: Security Breach Notification

Re: Notice of Data Security Incident

Dear Office of the Attorney General:

This Firm represents the University of Pennsylvania ("Penn") and we are writing to notify your office and provide details regarding the nature and circumstances of a recent data security incident.

Penn detected suspicious activity within an email account of one of its employees and immediately initiated an investigation in consultation with third-party cybersecurity experts to investigate what happened and make sure its system was secure. Penn determined that only one employee's email account was compromised and the incident did not extend to any other Penn system.

Penn also worked with experts to review the affected email account to determine whether the unauthorized individual may have accessed any personal information. On January 30, 2023, Penn confirmed that personal information of one Maryland resident may have been exposed to the unauthorized individual, including name, address, and social security number.

Since learning of this incident, Penn has consulted with cybersecurity experts to better understand what happened and to prevent a similar incident in the future. Penn has also taken steps to further protect and strengthen the security of its systems to prevent a similar incident in the future, including password reset and continuing to implement additional safeguards. Penn will continue with these efforts.

Penn sent notifications by mail to the affected individual to explain what happened, what information was involved, what Penn has done and how the affected individual can contact Penn with questions. Penn is also making an offer of one year of credit monitoring to the affected individual. Further information about what Penn has done and is recommending to the individual in question can be found in the enclosed notice that Penn will send to one Maryland resident via mail on March 1, 2023.

Morgan, Lewis & Bockius LLP

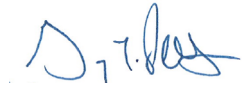
1701 Market Street
Philadelphia, PA 19103-2921
United States

 +1.215.963.5000
 +1.215.963.5001

State of Maryland
Office of the Attorney General
March 1, 2023
Page 2

If you have any questions, please feel free to contact me.

Regards,

A handwritten signature in blue ink, appearing to read "G. T. Parks", is positioned above the printed name.

Gregory T. Parks

Enclosure



Office of Audit, Compliance and Privacy

March 1, 2023

[ADDRESS]

Re: Notice of Data Security Incident

Dear [NAME]:

We are writing to notify you of the potential exposure of your personal information in a recent data security incident.

What Happened?

We detected suspicious activity within an email account of one of our employees and we immediately initiated an investigation and consulted with cybersecurity experts to investigate what happened and make sure our system was secure. Working with experts, we determined that only one employee's email account was compromised and the incident did not extend to any other Penn system.

What Information Was Involved?

After review of the affected email account, on January 30, 2023, we determined that certain personal information may have been exposed to an unauthorized individual between August 13, 2022 and October 24, 2022, including your name, address, and social security number.

What We Are Doing

We are committed to maintaining the privacy and security of your information and we are taking this incident very seriously. Since learning of the incident, we have consulted with third-party cyber experts to better understand what happened and to prevent a similar incident in the future. We have also taken steps to further protect and strengthen the security of our systems to prevent a similar incident in the future, including password reset and implementing additional safeguards. We will continue with these efforts.

To help protect your identity, we want to provide you with tools to help protect your information, and we are offering you a 12-month membership of credit monitoring services at no cost to you.

How to Activate Your Identity Monitoring Services

We have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring

services¹ include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

1. You must activate your identity monitoring services by **06-6-2023**. Your Activation Code will not work after this date.
2. Visit **[Enroll.krollmonitoring.com/redeem](https://enroll.krollmonitoring.com/redeem)** to activate your identity monitoring services. Provide Your Activation Code: **CODE** and Your Verification ID: **ID NUMBER**

What You Can Do

We encourage you to enroll in the credit monitoring services offered above, which will alert you to any attempt to establish a new line of credit using your name and social security number.

There are several additional steps you can take to protect your privacy and ensure that your personal information is not used improperly, all of which are best practices individuals should regularly implement.

Carefully review financial statements sent to you by your bank, credit card company, other financial institutions, and government entities, like the IRS, and immediately notify them by phone or email of any suspicious transactions or activity and follow up in writing if you make the notification by phone.

The attached reference guide provides more information and resources.

For More Information

If you have questions or concerns not answered by this letter, please call 215-573-4492.

Please know that we take this matter very seriously, and we apologize for any concern and inconvenience this may cause you.

Sincerely,

Scott D. Schafer
Chief University Privacy Officer and Institutional Compliance Officer
Office of Audit, Compliance and Privacy
University of Pennsylvania

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three 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. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible if there are any.

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.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov

Place a Fraud Alert on Your Credit File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	Experian	TransUnion
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 740241 Atlanta, Georgia 30374-0241	P.O. Box 9532 Allen, Texas 75013	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus using the same contact information noted above.

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following 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, provide the addresses where you have lived over the prior five years.
5. Proof of current address, such as a current utility bill or telephone bill

6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
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

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. 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 your 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.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For 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, 888-743-0023, www.oag.state.md.us

For 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/internet/resource-center>

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

For North Carolina Residents: You can obtain information from the Federal Trade Commission 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.

Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.