

Morgan Lewis

Kristin M. Hadgis

Partner
215.963.5563
Kristin.hadgis@morganlewis.com

January 11, 2024

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

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

Re: Notice of Data Security Incident

Dear Office of the Attorney General:

This Firm represents Carnegie Mellon University ("CMU") and we are writing to notify your office regarding the nature and circumstances of a data security incident. On August 25, 2023, CMU detected suspicious activity on a CMU computer system and immediately launched an investigation. The investigation revealed that an unauthorized third party gained access to a CMU computer system and may have copied files. CMU worked to quickly disable access to the copied files, in collaboration with law enforcement, and secured the impacted computer system. Through the investigation, CMU determined that some of the files may have contained personal information. This was determined over the subsequent months as CMU worked to identify the impacted files with the assistance of law enforcement, conducted a comprehensive review of the files to determine whose information may have been involved, and worked diligently to confirm current contact information for notification purposes. That process was completed on December 4, 2023.

During the investigation, CMU determined that the impacted files may have included name, social security number and/or date of birth of Maryland residents. Although there is no indication that the disclosed personal information has been used for any fraudulent purpose, CMU is sending notifications by mail to the affected individuals to explain what happened, what information was involved, what CMU has done, and how affected individuals can contact CMU with questions. CMU is offering two years of credit monitoring to affected individuals.

CMU is committed to maintaining the privacy and security of information and has taken this data security incident very seriously. It also has taken, and continues to take, steps to prevent this type of incident from occurring in the future, including to deploy additional security tools.

Further information about what CMU has done and is recommending to the individuals in question can be found in the enclosed notification that CMU is sending to 341 Maryland residents via mail on January 12, 2024.

Morgan, Lewis & Bockius LLP

2222 Market Street
Philadelphia, PA 19103-3007
United States

T +1.215.963.5000
F +1.215.963.5001

State of Maryland
Office of the Attorney General
January 11, 2024
Page 2

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

Regards,



Kristin M. Hadgis

Enclosure

January 12, 2024



K6458-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



Re: Notice of Data Security Incident

Dear Sample A. Sample:

The Information Security Office at Carnegie Mellon University (CMU) recently discovered a data security incident that might involve some of your personal information. At this time, we have no reason to believe that your personal information has been used inappropriately, but we are sending this letter out of an abundance of caution to share with you what we know about what happened, what information was involved, what we have done, and what you can do to protect your continued privacy.

What Happened

On August 25, 2023, we detected suspicious activity on a CMU computer system. We immediately launched an investigation and recovery effort. Our investigation revealed that an unauthorized third party gained access to a CMU computer system and may have copied files which included your personal information. This was determined over the subsequent months as CMU worked to identify the impacted files with the assistance of law enforcement, conducted a comprehensive review of the files to determine whose information may have been involved, and worked diligently to confirm current contact information for notification purposes. That process was completed on December 4, 2023, and you are receiving this notice because your information was identified as potentially involved.

What Information Was Involved

While we have no indication that your personal information was used inappropriately, the information that was accessed may have contained your name, social security number and/or date of birth.

What We Are Doing

CMU is committed to maintaining the privacy and security of your information and has taken this data security incident very seriously. Immediately upon learning of this incident, CMU launched an investigation and recovery effort, ultimately disabling access to the copied files, in collaboration with law enforcement. We also have taken, and continue to take, steps to prevent this type of incident from occurring in the future.

To help protect your identity, we are offering you a complimentary 24-month membership in Experian® IdentityWorksSM. This product provides you with credit monitoring, identity fraud detection and resolution of identity theft.

To activate your membership and start monitoring your personal information, please follow the steps below:

- Enroll by: **April 30, 2024** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your activation code: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **1-833-918-3456** by **April 30, 2024**. Be prepared to provide engagement number **B114001** as proof of eligibility for the identity restoration services by Experian.



What You Can Do

To help protect your personal information, we strongly recommend you take the following steps:

- 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 personal information to establish credit and to block that credit from being established if you were not the one who initiated it.
- Carefully review statements sent to you by your bank, credit card company or other financial institutions, as well as government institutions such as 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 more information. We encourage you to read and follow these steps as well.

Experian IdentityWorks Membership Details

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

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

* 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.

If you believe there was fraudulent use of your information, please contact Experian at 1-833-918-3456. If it is determined that identity restoration support is needed, an Experian identity restoration agent will work with you to investigate and resolve each incident of fraud (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 this identity restoration support 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. You will also find self-help tips and information about identity protection at this site.

For More Information

We apologize and regret the inconvenience associated with this incident. If you have questions or concerns, please call 1-833-918-3456 toll-free, Monday through Friday from 9 a.m. - 9 p.m. EST (excluding major U.S. holidays). Please be prepared to provide engagement number **B114001**.

Sincerely,

John K. Lerchey
Incident Response Coordinator
Information Security Office
Carnegie Mellon University

REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, 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 in the event 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 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	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

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 at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	www.transunion.com

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 District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

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 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.

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

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. 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

For 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.