

August 17, 2023

BY EMAIL

Office of the Attorney General
200 St. Paul Plaza
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

On behalf of Proskauer Rose LLP (“Proskauer”), and pursuant to Md. Code Ann., Com. Law § 14-3504(h), this letter provides notice of a cybersecurity incident involving Maryland residents. Proskauer is a law firm headquartered in New York, NY.

On April 4, 2023, Proskauer learned that an unauthorized third party named GrayHatWarfare had unlawfully accessed a Microsoft Azure cloud storage site maintained by Proskauer (the “Portal”) and posted an index of all files stored on the Portal on their website behind a paywall. The Portal is used by Proskauer to store certain files relating to transactions for which our services were retained.

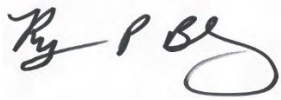
Upon discovering this unauthorized access, Proskauer promptly initiated a privileged investigation, directed by outside counsel, with the assistance of leading outside cybersecurity experts. That investigation determined that the earliest unauthorized access to the Portal occurred in November 2022, and evidence indicates there were several instances of anomalous download activity from the Portal between late January 2023 and mid-March 2023. There is no evidence of unauthorized access to Proskauer’s network or other systems, and we are confident those were not affected. We have also seen no evidence of unauthorized access to the Portal after Proskauer took steps to secure it on March 15, 2023. Proskauer’s investigation has determined that the access vector into the Portal was likely a misconfiguration that rendered it vulnerable to a hacking technique developed subsequent to the Portal’s creation. While the Portal was subject to routine penetration testing, these tests did not detect the issue that was exploited here. As soon as Proskauer became aware of the misconfiguration, its security team reconfigured the Portal and took additional steps to secure its data, including enabling an additional firewall to block all access from outside of the Proskauer IP space. Proskauer also reported the unauthorized and unlawful access to the Portal to law enforcement.

On July 21, 2023, Proskauer completed a manual review of thousands of affected files and determined that the personal information of 65 Maryland residents was affected. The types of personally identifiable information that were affected, depending on the individual, included name, included name, address, Social Security number, date of birth,

driver's license number, financial account number, other government issued ID number, signature, and health or medical information. Proskauer will be notifying all individuals whose personally identifiable information was affected. We anticipate beginning to notify individuals via U.S. mail by no later than August 18, 2023. The notice to individuals will not have been delayed as a result of a law enforcement investigation. As stated in the enclosed sample notification letter, we will be offering individuals whose personal information may have been exposed two years of complimentary identity theft and credit monitoring services through Experian. We will also be establishing a call center to respond to individuals' questions.

Proskauer takes this matter very seriously and we are committed to answering any questions you may have. If you have any questions regarding this submission, please do not hesitate to contact us at RBlaney@proskauer.com or 202.416.6815.

Sincerely,

A handwritten signature in black ink, appearing to read "Ry P Blaney", with a large, stylized loop at the end.

Ryan P. Blaney
Partner

Enclosure



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 18, 2023

J8821-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L02 GENERAL



APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY



Notice of Security Incident

Dear Sample:

We at Proskauer Rose LLP (“Proskauer”) are contacting you to provide important information about a data security incident that affected your personal information. The personal data was contained within documents in Proskauer’s possession relating to a transaction for a Proskauer client and was unlawfully acquired by an unauthorized third party as a result of the security incident as set out below. Although we have no indication of identity theft or fraud in relation to this incident at this time, we are providing you with information about the incident, our response, and additional measures you can take to help protect your personal information.

What Happened? On or about April 8, 2023, we uncovered evidence that an unauthorized third party had illegally downloaded data from a cloud-hosted Proskauer Portal. Upon learning this, we immediately began an investigation and conducted a manual review of the affected data to confirm the individuals affected and identify their contact information to provide notifications. We recently completed this review and have concluded that your personal information was involved in the incident. We have not delayed this notification as a result of any law enforcement investigation.

What Information Was Involved? Our investigation determined that your personal information was affected and included your: name, address, [Extra1].

What We Have Done/Are Doing. Proskauer takes this incident and the security of the information we receive very seriously. We engaged leading cybersecurity and forensic experts to carry out a full investigation and review all compromised data in order to notify affected individuals. We immediately reconfigured the Portal and took additional steps to secure its data, including enabling an additional firewall. We conducted a full review of our on-premises environment and found no evidence of unrelated compromise.



While we are unaware of any identity theft or fraud as a result of this event, Proskauer is offering you access to 24 months of complimentary credit monitoring and identity restoration services through Experian. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: November 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- 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 **888-397-0073** by **November 30, 2023**. Be prepared to provide engagement number **B101917** as proof of eligibility for the identity restoration services by Experian.

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, Equifax and Transunion files 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.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-397-0073. 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 (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.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, monitoring your free credit reports for suspicious activity and to detect errors, and reporting any unusual activity to your financial institution. Please also review the enclosed *Additional Resources* page, which contains information on what you can do to help safeguard against possible misuse of your information. You can also enroll in the credit monitoring and identity restoration services that we are offering.

For More Information. If you have additional questions, you may contact us at 888-397-0073, toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B101917.

Sincerely,

Proskauer Rose LLP

* 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.



Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

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

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at <https://www.annualcreditreport.com/manualRequestForm.action>. Credit reporting agency contact details are provided below.

Equifax:

equifax.com
equifax.com/personal/credit-report-services
P.O. Box 740241
Atlanta, GA 30374
866-349-5191

Experian:

experian.com
experian.com/help
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion:

transunion.com
transunion.com/credit-help
P.O. Box 1000
Chester, PA 19016
888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado, Delaware, and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, <http://www.marylandattorneygeneral.gov>, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, <http://www.ncdoj.gov>, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Georgia, Maryland, New Jersey, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

For New York residents: You may contact the New York Office of the Attorney General at: The Capitol, Albany, NY 12244-0341, <http://www.ag.ny.gov/home.html>, 1-800-771-7755, and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, <http://www.dos.ny.gov/consumerprotection>, 1-800-697-1220.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington, D.C. 20001, <https://www.oag.dc.gov/>, 202-727-3400.



