



Freeman
Mathis & Gary LLP

1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009

www.fmglaw.com

Nicholas Jajko
Partner
D: 215.279.8070
nicholas.jajko@fmglaw.com

August 4, 2022

Via E-Mail Reporting

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

RE: The Preston Partnership, LLC - Notice of Data Event

Dear Sir or Madam:

We represent The Preston Partnership, LLC ("The Preston Partnership"), which is an Architecture and Interior Design firm based in Atlanta, Georgia. This submission is provided pursuant to the Maryland Personal Information Protection Act, MD CODE ANN. COM. LAW § 14-3501, *et seq*, which requires notice to your office in the event of a breach in the security of personal information affecting residents of the State of Maryland.

The Preston Partnership was recently the victim of a computer malware attack. Upon discovery of the incident, The Preston Partnership immediately shut down its network and commenced an investigation that included partnering with cyber security incident specialists to secure its systems and restore data safely. During the restoration, the investigation determined The Preston Partnership's systems were accessed by someone outside the organization between July 5, 2022, and July 9, 2022. On July 22, 2022, the Preston Partnership confirmed that certain files on its server were accessed and taken from the network that contained sensitive personal information. As a result, The Preston Partnership conducted a review of its records and notified all potentially impacted current and former employees of this incident. The information impacted for Maryland residents included their name and Social Security number.

www.fmglaw.com



Maryland Office of the Attorney General

August 4, 2022

Page 2

On or about August 4, 2022, The Preston Partnership provided notice via U.S. regular mail of the incident to the potentially affected individuals. A sample copy of the notice is attached as Exhibit "A" for your records. The Preston Partnership provided this notification to a total of 195 individuals, four (4) of which are residents of the State of Maryland.

As an added precaution, The Preston Partnership offered the affected Maryland residents twelve (12) months of credit monitoring and identity restoration "IdentityWorks" services through Experian. The notice to the affected individuals includes instructions on the use of this product as well as encouragement to remain vigilant for incidents of fraud or misuse, by reviewing and monitoring account statements and credit reports, immediately reporting errors or suspicious activity to the financial institution or issuing creditor, and filing a report with law enforcement, their state attorney general, and/or the Federal Trade Commission in the event fraud or misuse is discovered. The Preston Partnership also included contact information for the major consumer reporting bureaus, state-specific regulators, and additional steps individuals may take to protect the impacted information from misuse, should they find it appropriate to do so.

After discovering the incident, The Preston Partnership reset account and system passwords across the entire organization. The Preston Partnership continues to use and expand implementation of multi-factor authentication throughout its environment. The Preston Partnership reported the incident to Federal law enforcement and will cooperate with any investigation. The Preston Partnership also partnered with industry leading professionals to thoroughly investigate the incident, notify potentially affected individuals, and implement additional security solutions to enhance the existing security protections on its network going forward. The Preston Partnership is also notifying other state regulators as necessary.

I believe this provides you with all information necessary for your purposes and to comply with Maryland law. However, if anything further is needed, please contact me directly.

Respectfully,

FREEMAN MATHIS & GARY, LLP

/s/ Nicholas Jajko

Nicholas Jajko

Exhibit “A”



The Preston Partnership, LLC
115 Perimeter Center Place, Suite 950
Atlanta, Georgia 30346
T. 770 396 7248
theprestonpartnership.com

August 4, 2022



Re: Notice of Data Event

Dear [REDACTED]:

We at The Preston Partnership take data privacy and information security seriously. As part of that commitment, we write to notify you of an incident that may impact the security of your personal information. The Preston Partnership has an obligation to maintain this information in connection with your, or your family member's, current or prior employment with our firm.

What Happened?

The Preston Partnership was recently the victim of a computer malware attack. Upon discovery of the incident, we immediately shut down our network and commenced an investigation that included partnering with cyber security incident specialists to secure our systems and restore our data safely. During the restoration, our investigation determined our systems were accessed by someone outside our organization between July 5, 2022, and July 9, 2022. On July 22, 2022, we confirmed that certain files on our server were accessed and taken from our network that contained sensitive personal information. As a result, we conducted a review of our records and are notifying all potentially impacted current and former employees, and family members of this incident.

What Information Was Involved?

You are receiving this notice because, based on our review, your personal information including name and Social Security number were present in files on certain server data that was accessed and taken from our network. While we have no reports of fraud or misuse of your data at this time, we encourage you to review the information contained within this notice carefully and to take advantage of the resources we are offering you.

What We are Doing

We take this event and the security of personal information entrusted to us seriously and have taken steps to help mitigate the potential for harm and to prevent this from happening again. After discovering the incident, we reset account and system passwords across the entire organization. We continue to use and expand implementation of multi-factor authentication throughout our environment. We reported the incident to Federal law enforcement and will cooperate with any investigation. We

also partnered with industry leading professionals to thoroughly investigate the incident, notify potentially affected individuals, and implement additional security solutions to enhance our existing security protections on our network going forward.

What You Can Do

We encourage you to remain vigilant for incidents of fraud or misuse, from any source, by reviewing and monitoring your account statements and credit reports. We recommend you report errors or suspicious activity to your financial institution or the issuing creditor immediately. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. Please refer to the enclosed documentation which contains additional steps you may take to protect your information from misuse, should you find it appropriate to do so.

As an added precaution to help protect your identity, we are offering a complimentary twelve (12) month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by November 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/credit>
- **Select** "All other members" Get Started Option
- Provide your **activation code:** [REDACTED]

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 (877) 890-9332 by November 30, 2022. Please be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

For More Information

If you have any other questions or concerns, you may contact Bob Preston at [REDACTED] for further information and assistance. We are very sorry for any concern or inconvenience this incident has caused or may cause you, and we encourage you to take advantage of the resources we are offering you. The Preston Partnership remains committed to safeguarding the information in our care.

Sincerely,

Robert Preston

Robert Preston, AIA, RIBA
Principal & Vision Keeper
The Preston Partnership LLC

Additional Steps to Help Protect Your Information

Review personal account statements and credit reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax
1-866-766-0008
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com

Experian
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion
1-800-680-7289
P.O. Box 2000
Chester, PA 19022
www.transunion.com

Report suspected fraud. You may contact law enforcement and have the right to file a police report to report suspected identity fraud or theft. Please note that to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. For more information, visit <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.marylandattorneygeneral.gov, (888) 743-0023.
- **New York Residents:** Office of Attorney General, The Capitol, Albany, NY 12224, 1-800-771-7755 (toll-free), <https://ag.ny.gov/>; and the Bureau of Internet and

Technology (BIT), 28 Liberty Street, New York, NY 10005, (212) 416-8433, <https://ag.ny.gov/internet/resource-center>

- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338). This notification was not delayed by a law enforcement investigation.

Additional details regarding your 12-month Experian IdentityWorks Membership:

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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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 (877) 890-9332. 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 12 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.

* 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.