RAJ FERBER
PLLC

1629 K Street NW, Suite 300
Washington, DC 20006

Scott Ferber
(202) 868-0035
scott@rajferber.com

August 15, 2024

PRIVATE & CONFIDENTIAL
EXEMPT FROM FOIL / PUBLIC RECORDS REQUESTS

BY EMAIL

The Honorable Anthony G. Brown
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notice of a Cybersecurity Incident

Dear Attorney General Brown:

We represent TCPS, Inc., headquartered at 4200 Parliament Place, Ste 600, Lanham, MD 20706, and are writing to notify your Office of an incident that may affect the security of certain personal information relating to 1,774 State residents. The investigation into this matter recently concluded. This letter is being supplied on a strictly confidential basis and is not intended for further sharing or distribution with any third party. By providing this notice, TCPS does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Nature of the Cybersecurity Incident

TCPS is a privately-owned professional services company, supporting entities that specialize in manufacturing, installing, and servicing of high-quality home remodeling products.

Based on the investigation to date, on June 10, 2024, TCPS discovered that it was a victim of a cybersecurity incident that resulted in the encryption of certain TCPS systems and data, as well as potential exfiltration of certain data. Shortly after discovering the incident, TCPS engaged an expert external cyber forensic firms to assist with a forensic investigation, containment of the incident, and system and data restoration. TCPS promptly and proactively disconnected affected systems and engaged in a secure, phased restoration of data and systems, which is now complete. The last identified instance of unauthorized activity was on June 10, 2024.

TCPS did not identify indications that the incident had spread to any third-party systems.

On August 5, 2024, TCPS completed its review of potentially affected data, which comprised HR-related information for current and certain former employees. TCPS did not identify covered personal information of customers or vendors that was affected by the incident. The information that could have been subject to unauthorized access varies by individual and may include name and one or more of the following elements: social security number, government-issued identification number, financial account number, health coverage information, telephone number, beneficiary/dependent information, and/or email address. On August 15, 2024, TCPS plans to mail notices to the identified affected current and former employees of the company – approximately 2,905 individuals. TCPS will be providing them with access to complimentary identity protection and credit monitoring services for 24 months through Experian.

Notice to Maryland Residents

TCPS plans to mail written notice of this incident to the identified individuals on August 15, 2024. A sample of that individual notice is attached here as ***Appendix A***.

Other Steps Taken and To Be Taken

Upon discovering the incident, TCPS moved quickly to investigate and identify potentially affected individuals. TCPS has taken steps to further strengthen and enhance the security of systems in its network, including updating administrative and technical safeguards, as well as providing additional cybersecurity guidance for our personnel. TCPS also notified federal law enforcement and is cooperating with their investigation of the incident.

As discussed above, TCPS is providing access to complimentary identity protection and credit monitoring services for 24 months, through Experian, to identified current and former employees whose personal information was potentially affected by this incident. Additionally, TCPS is providing these individuals with a toll-free number in the event that they have questions about the incident. The letters contain guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. TCPS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Further, TCPS is providing written notice of this incident to relevant state regulators, as well as to the nationwide consumer reporting agencies.

Contact Information

Should you have any questions regarding this notification or other aspects of the incident, please do not hesitate to contact us at (202) 868-0035.

Sincerely,

Scott Ferber

Return Mail Processing
PO Box 999
Suwanee, GA 30024

13 1 2905 ************************************SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

August 15, 2024

NOTICE OF SECURITY INCIDENT

Dear Sample A. Sample:

TCPS, Inc. is contacting you regarding a cybersecurity incident that may have resulted in exposure of some of your personal information. We take the security and privacy of your information very seriously and for that reason want you to understand what happened, what we are doing to address it, and what steps you can take to further protect yourself, should you feel it necessary to do so. While we are unaware of fraudulent misuse of your personal information, we are offering complimentary credit monitoring and identity theft protection services as a precaution. Instructions on how to enroll are provided below.

What Happened? On June 10, 2024, we identified suspicious activity in our information technology network from an unauthorized actor. After detecting the activity, we quickly implemented a series of containment and remediation measures. We launched an investigation, engaged external cybersecurity firms to assist, notified federal law enforcement, and engaged in a secure, phased restoration of data and systems, which is now complete. Once the incident was contained, we initiated a detailed review to identify affected sensitive personal information.

What Information Was Involved? Data from our HR files appears to have been accessed without authorization as part of the incident. Your information is contained in those files, including, among other data, your name and one or more of the following: social security number, government-issued identification number, financial account number, health coverage information, telephone number, beneficiary/dependent information, and/or email address.

What We Are Doing. We engaged external cybersecurity firms to assist with our investigation of the incident and analysis of the affected data. We also notified federal law enforcement and are cooperating with their investigation of the incident. In addition, we have taken steps to further strengthen and enhance the security of systems in our network, including updating administrative and technical safeguards, as well as providing additional cybersecurity guidance for our personnel.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the enclosed *Steps You Can Take To Protect Personal Information* for additional information on steps you can take to further protect your information, should you feel it necessary to do so. As an added precaution, we are offering you 24 months of complimentary credit monitoring through Experian. Please review the enrollment instructions included in the attached *Steps You Can Take To Protect Personal Information* and use Activation Code ABCDEFGHI. We encourage you to enroll in these monitoring services, as TCPS is not able to do so on your behalf. Please note the deadline to enroll is November 29, 2024. If you are interested in obtaining complimentary credit monitoring for your dependents and/or beneficiaries, please contact us at the below number.

For More Information.

We apologize for any inconvenience or concern this incident may cause. Security remains a top priority at TCPS, and we will continue to take all appropriate steps to safeguard personal information and our systems. You understandably may have questions that are not addressed in this letter. You may direct any questions you have about the incident by calling us toll-free at 1-833-918-4978, Monday - Friday, 9 am - 9 pm EST (excluding major U.S. holidays). Please be prepared to provide engagement number [Engagement Number].

Sincerely,

TCPS

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** November 29, 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 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 1-833-918-4978 by November 29, 2024. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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 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.

* 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to file a police report if they experience identity fraud. To file a crime report or incident report with law enforcement for identity theft, consumers likely will need to provide some kind of proof that they have been a victim. A police report is often required to dispute fraudulent items. Consumers can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information: full name (including middle initial as well as Jr., Sr., II, III, etc.); social security number; date of birth; addresses for the prior two to five years; proof of current address, such as a current utility bill or telephone bill; a legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 877-ID-THEFT (877-438-4338); and TTY: 866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, you may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Iowa residents, the Iowa Attorney General can be contacted at 1305 E. Walnut Street, Des Moines, Iowa 50319, www.iowaattorneygeneral.gov, 515-281-5926, or 888-777-4590.

For Kentucky residents, the Kentucky Attorney General may be contacted at 700 Capital Avenue, Suite 118, Frankfurt, KY 40601, www.ag.ky.gov, 502-696-5300.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 410-528-8662 or 888-743-0023; and https://www.marylandattorneygeneral.gov/. TCPS is headquartered at 4200 Parliament Place, Ste 600, Lanham, MD 20706.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-566-7226 or 919-716-6000; and www.ncdoj.gov.

For Oregon residents, we encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 877-877-9392 (toll-free in Oregon), 503-378-4400; or www.doj.state.or.us.

For South Carolina residents, the South Carolina Department of Consumer Affairs may be reached at 293 Greystone Blvd., Ste. 400, Columbia, SC 29210, www.consumer.sc.gov, 800-922-1594.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 401-274-4400. We first learned about a possible data security incident on June 10, 2024. Based on the investigation, personal information for approximately two Rhode Island residents was in the affected files. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.