



PIERSON FERDINAND

MARC A. LINDEMANN
PARTNER

1270 Avenue of the Americas
7th Floor
New York, NY 10020

Direct: 1.646.347.7952
Email: marc.lindemann@pierferd.com

January 30, 2025

Via Email (idtheft@oag.state.md.us)

Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Data Incident Notice

Pierson Ferdinand LLP represents The Partners Group, LLC (“TPGRP”), located at 11850 SW 67th Avenue, Suite 100, Portland, Oregon, 97223, in connection with a data security incident outlined below. The protection and proper use of information in its possession is a top priority for TPGRP, and TPGRP has taken steps to prevent a similar incident from occurring again in the future.

1. Incident Description

TPGRP detected a compromise of its email environment on May 11, 2024. TPGRP secured and remediated the compromise, engaged additional third-party experts, enhanced its data security, and commenced an investigation. The investigation determined that certain personal information was included in an email mailbox that could have been compromised.

TPGRP then conducted an extensive third-party data mining process to identify and notify potentially impacted individuals. Impacted data elements vary for each individual – the following personal information for your state’s residents could have been impacted by this incident: date of birth and social security number.

2. Steps Taken

TPGRP is committed to ensuring the security and proper use of all information in its control. TPGRP worked with experts to investigate how the compromise occurred and take appropriate hardening steps to enhance email security and data privacy, including retraining employees on phishing and information governance. TPGRP notified law enforcement regarding this incident.

Incident notification letters were mailed to residents of your state on January 30, 2025. A sample copy of the notification letter is attached as Exhibit A. This notification included complimentary credit monitoring, identity protection services, and identity theft insurance for twelve (12) months through Experian, a company specializing in fraud assistance and remediation services. At this time, TPGRP is not aware of anyone experiencing fraud as a result of this incident.



3. Contact information

TPGRP remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at marc.lindemann@pierferd.com or +1 646-347-7952.

Sincerely,

Marc A. Lindemann

Partner

Pierson Ferdinand LLP

Enclosure (1)



PIERSON FERDINAND

EXHIBIT A



The Partners Group, LLC
Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 30, 2025



M6340-L01-0000001 P001 T00001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 NON-MA

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



Notice of Data [Breach/Incident]

Dear Sample A. Sample,

The Partners Group, LLC (“The Partners Group”) has detected a compromise to its email environment that could have impacted your personal information. We have no indication that your information has been or will be misused. The Partners Group is an insurance brokerage that processes personal information directly and on behalf of our client policyholders. We want to make you aware of the incident and the measures we have taken in response, as well as provide details on steps you can take – should you deem it appropriate – to help protect your information. The protection, privacy, and proper use of personal information is paramount, and we are working to prevent this type of incident from occurring again.

What Happened

The Partners Group identified unauthorized activity in an email account on May 11, 2024. We secured and remediated the compromise, engaged additional third-party experts, hardened and enhanced our data security, and commenced an investigation. We have worked diligently to determine what happened and what information could have been compromised, including an extensive third-party process to review impacted email mailboxes to gather information sufficient to notify potentially impacted individuals. Unfortunately, these types of incidents have become commonplace and impact organizations of all sizes.

What Information Was Involved

The third-party digital forensic investigation determined that your personal information could have been compromised. Specifically, an email account that was subject to unauthorized activity contained your personal information. While the impacted data elements vary, this compromise could have included your [data elements]. Please note that we have no evidence at this time that any of your personal information has been misused as a result of the incident.

What We Are Doing

We take this incident seriously and are committed to the strength of our data security, including additional employee training on phishing and cybersecurity. We have notified law enforcement regarding this incident.

Additionally, out of an abundance of caution, we have arranged for you to activate complimentary credit monitoring for ## months through Experian. This service will be provided by Experian, a company specializing in fraud assistance and remediation services. To enroll in this service, please follow the instructions provided within ninety (90) days of the date of this letter. You can enroll by using enrollment code ABCDEFGHI and visiting <https://www.experianidworks.com/credit>.

0000001



Please note that to activate monitoring services, you will need an internet connection and e-mail account. Additionally, you may be required to provide your name, date of birth, and Social Security number to confirm your identity. Due to privacy laws, we cannot register you directly. Certain services might not be available for individuals who do not have a credit file with the credit bureaus or an address in the United States (or its territories) and a valid Social Security number. Activating this service will not affect your credit score.

What You Can Do

We are not aware of anyone experiencing fraud as a result of this incident. As data incidents are increasingly common, we encourage you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. We encourage you to review the Additional Important Information located on the following pages, which includes further steps to safeguard your personal information, such as implementing a fraud alert or security freeze.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for ## 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 ## 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 ##-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 **March 31, 2025**. Enrollments must occur by no later than 5:59 p.m. CT on this last day. (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 **866-530-9923** by March 31, 2025. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-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.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call **866-530-9923** toll-free Monday through Friday from 8 am – 8 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number **ENGAGE#**.

The Partners Group values the protection of our network and the privacy of personal information, and we understand the concern that these incidents cause.

Sincerely,

Jakob Lutkavage-Dvorscak
General Counsel
The Partners Group
11850 SW 67th Ave, Suite 100
Portland, OR 97223

* 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 Important Information

Monitoring: You should always remain vigilant and monitor your accounts for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for suspicious or unusual activity. You can report suspicious activity to financial institutions or law enforcement.

Fraud Alert: You can place fraud alerts with the three major credit bureaus by phone and online as set forth below with Equifax, TransUnion, or Experian. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can get an extended fraud alert for seven years.

Credit Report: Consumers are also entitled to one free credit report annually from each of the three credit reporting bureaus. To order your free credit report: visit www.annualcreditreport.com; call, toll-free, 1-877-322-8228; or mail a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information may need to be included when requesting a security freeze: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current and addresses for the past five years; (5) proof of address; (6) Social Security Card, pay stub, or W2; or (7) government-issued identification card. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

<u>TransUnion</u>	<u>Experian</u>	<u>Equifax</u>
1-888-909-8872	1-888-397-3742	1-800-349-9960
www.transunion.com/credit-help	www.experian.com/help/	www.equifax.com/personal/credit-report-services/
<u>Fraud Alert</u> P.O. Box 2000 Chester, PA 19016	<u>Fraud Alert</u> P.O. Box 9554 Allen, TX 75013	<u>Fraud Alert</u> P.O. Box 105069 Atlanta, GA 30348-5069
<u>Credit Freeze</u> P.O. Box 160, Woodlyn, PA 19094	<u>Credit Freeze</u> P.O. Box 9554, Allen, TX 75013	<u>Credit Freeze</u> P.O. Box 105788 Atlanta, GA 30348-5788

Implementing an Identity Protection PIN (IP PIN) with the IRS: To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register and validate your identity. Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. Some items to consider when obtaining an IP PIN with the IRS: (1) an IP PIN is valid for one calendar year; (2) a new IP PIN is generated each year for your account; (3) logging back into the Get an IP PIN tool, will display your current IP PIN; and (4) an IP PIN must be used when filing any federal tax returns during the year including prior year returns.

Fair Credit Reporting Act: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Federal Trade Commission: More information can be obtained by contacting the Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft.

For Massachusetts residents: You can obtain a police report if you are a victim of identity theft.

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

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

For Vermont residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Residents of the below states can obtain additional information regarding identify theft and more at:

- **District of Columbia Attorney General:** 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and <https://oag.dc.gov>.
- **Maryland Office of the Attorney General:** Consumer Protection Division, 200 St. Paul Place, 16th Fl, Baltimore, MD 21202; 1-888-743-0023; <https://www.marylandattorneygeneral.gov>.
- **New York Attorney General:** Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.
- **North Carolina Attorney General:** 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and <https://www.ncdoj.gov>.



