

18636



THE PLANNING GROUP  
WEALTH MANAGEMENT

Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<MailID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>>

<<Date>>

## NOTICE OF DATA BREACH

Dear <<Name 1>>:

TPG Advisors, LLC d/b/a The Planning Group ("The Planning Group") understands the importance of protecting your information and is writing to inform you that The Planning Group recently identified and addressed a security incident involving its email systems that may have involved your personal information. This notice describes the incident, outlines the measures that The Planning Group has taken in response, and advises you on steps you can take to further protect your information.

**What Happened?** On or about October 21, 2020, The Planning Group became aware of a potential data security incident involving unauthorized access to one of its employees' email accounts. The Planning Group immediately changed all passwords associated with the account, thereby terminating any potential unauthorized access, and implemented additional security measures to further enhance its already robust data security platform. The Planning Group simultaneously retained a forensic investigation firm to determine the nature of the security incident and identify any individuals whose personal information may have been compromised.

**What Information Was Involved?** The forensic investigation concluded that the data security incident was limited to a brief period of unauthorized access to a single account occurring between October 13, 2020 and October 21, 2020. The forensic investigation was unable to confirm any specific files contained within the impacted account that may have been accessed and/or acquired without authorization.

Nonetheless, in continuing its thorough investigation, The Planning Group undertook a comprehensive manual review process to identify the specific individuals with personal information contained in the impacted mailbox, if any. In an abundance of caution, The Planning Group is providing this notification to you as your personal information was contained within the impacted account. Specifically, the data security incident *may have* resulted in unauthorized access to and/or acquisition of information including <<Data Elements>>. As indicated above, the forensic investigation was unable to confirm that any specific files contained within the impacted account were accessed and/or acquired, and it is entirely possible that your specific personal information *was not compromised* as a result of the incident.

**What We Are Doing** As stated above, immediately upon learning of potential unauthorized access, The Planning Group undertook efforts to eliminate any potential unauthorized access by changing all passwords associated with the impacted account and implemented additional security measures to further enhance its already robust data security platform. The Planning Group is continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of their systems to help prevent this from happening in the future.

Additionally, we are offering you a free <<12-month or 24-month>> membership to TransUnion myTrueIdentity credit monitoring service. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This product also includes various features such as up to \$1,000,000 in identity theft insurance with no deductible, subject to policy limitations and exclusions. TransUnion myTrueIdentity is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft protection and TransUnion myTrueIdentity, including instructions on how to activate your complimentary <<12-month or 24-month>> membership, please see the additional information attached to this letter. ***To take advantage of this offer, you must enroll by <<deadline>>.***

**What You Can Do** We are aware of how important your personal information is to you. To protect yourself from potential harm associated with this incident, we encourage you to enroll in the complimentary credit monitoring service, to closely monitor all mail or other contact from individuals not known to you personally, and to avoid answering questions or providing additional information to such unknown individuals. We also remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements, explanation of benefit statements, and credit reports for unauthorized activity, and to report any such activity or any suspicious contact whatsoever to law enforcement if warranted.

**For More Information** For further information on steps you can take to prevent against possible fraud or identity theft, please see the attachments to this letter. The Planning Group understands the importance of protecting your information, and deeply regrets any concern this may have caused to you. **Should you have any questions and would like further information regarding the information contained in this letter, please do not hesitate to contact me at (847) 446-9534.**

Sincerely,

A handwritten signature in black ink, appearing to read "Michael D. Brown", with a stylized, flowing script.

Michael D. Brown, CFA, CPA  
Chief Investment Officer  
TPG Advisors, LLC d/b/a The Planning Group

## Attachment 1: Protecting Yourself

We remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements and credit reports for unauthorized activity. **Residents of the United States are entitled to one free credit report annually from each of the three major credit reporting agencies.** To order your free credit reports, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll-free (877) 322-8228. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

**You may want to consider placing a fraud alert on your credit report.** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert.

- **Initial Alert:** You may ask that an initial alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. A fraud alert does not impact your ability to get a loan or credit, but rather alerts a business that your personal information may have been compromised and requires the business to verify your identity before issuing you credit. Although this may cause some delay if you are applying for credit, it may protect against someone else obtaining credit in your name. An initial fraud alert stays on your credit report for at least 90 days
- **Extended Alert:** You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies. The agency that you contacted must notify the other two agencies.

Additionally, you have the right to put a **credit freeze**, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. However, unlike a fraud alert, you must separately place a security freeze on your credit file at each of the three national credit reporting agencies. In order to request a security freeze, you may 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.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Below are the toll-free numbers and addresses for the three largest credit reporting agencies:

Equifax  
P.O. Box 74021  
Atlanta, GA 30374  
1-800-685-1111  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 1000  
Chester, PA 19016  
1-800-916-8800  
[www.transunion.com](http://www.transunion.com)

Below is the toll-free number, address and website address for the Federal Trade Commission, which you may contact to obtain further information on how to protect yourself from identity theft and how to repair identity theft:

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

*For residents of Hawaii, Michigan, Missouri, Virginia, Vermont and North Carolina:* It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

*For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon and West Virginia:* It is required by state law to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report using the contact information listed above.

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

*For residents of Oregon:* State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

*For residents of Maryland, Rhode Island, Illinois and North Carolina:* You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

Rhode Island Office of the Attorney General  
Consumer Protection  
150 South Main Street  
Providence, RI 02903  
1-401-274-4400  
[www.riag.ri.gov](http://www.riag.ri.gov)

Office of the Illinois Attorney General  
Identity Theft Hotline  
100 W Randolph St, Fl. 12  
Chicago, IL 60601  
1-866-999-5630  
[www.illinoisattorneygeneral.gov](http://www.illinoisattorneygeneral.gov)

North Carolina Office of the Attorney General  
Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-566-7226  
[www.ncdoj.com](http://www.ncdoj.com)

*For residents of Massachusetts and Rhode Island:* It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

*For residents of Connecticut, Massachusetts, Rhode Island and West Virginia:* You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed above.

*For residents of Texas:* We believe that this incident may have affected one Texas resident.

**FAIR CREDIT REPORTING ACT.** You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit [www.ftc.gov/credit](http://www.ftc.gov/credit). The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also

entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Note - Identity theft victims and active duty military personnel have additional rights.