

Warning Regarding Web Fraud and Phishing

TPG is a leading global alternative asset management firm founded in San Francisco in 1992 with over \$100 billion of assets under management and investment and operational teams in 12 offices globally.

We are proud of our success. But an unfortunate consequence of our size and global reputation is the misuse of our name, brands and reputation by cyber criminals and fraudsters seeking to make illicit financial gains or to steal sensitive information.

Fraudsters may pose as TPG employees using fake web sites, "phishing" e-mails from lookalike e-mail addresses, phone calls, or even impostor accounts on popular instant messaging services.

TPG does not engage in telephone, email, or social media solicitation of individual retail investors. Any such solicitation should be considered an immediate red flag and an indication of fraud.

In particular, beware of scams purportedly affiliated with TPG soliciting financial investments with promises of extraordinary returns at little to no risk. These "high yield investment programs" are frauds and are unfortunately quite common.

When communicating with TPG through digital media, please:

- Confirm you are visiting a TPG authorized web site. TPG's only authorized web sites are posted through the below listed domains. No other web site domains are authorized.
 - tpg.com
 - healthcare.tpg.com
 - pace.tpg.com
 - shareholders.tpg.com
 - software.tpg.com
 - therisefund.com
 - tpgrefinance.com
 - tpgexecutivenetwork.com
 - yanalytics.org
- Do not share your password and login ID with anyone, including anyone from TPG. Certain TPG on-line environments are private, available only to investors through secure log-in procedures. Apart from allowing you to use your password and log-in to enter an authorized site, TPG will never ask you for your password or log in information. (If you forget your password or login, we will issue you new ones.)
- Do not communicate or deal with personnel who are not affiliated with an authorized office. All authorized office locations are listed on our contact page. No other office locations are authorized offices of TPG.
- TPG does not use social media to solicit investors or offer securities. Although TPG maintains a legitimate social media presence, it does not directly communicate with individuals over any social media about potential investments. Any social media postings about investment opportunities with TPG should be considered red flags.

- Do not send e-mails about TPG matters to anyone with an address other than an authorized TPG e-mail address. TPG only uses the below listed domains for e-mail addresses. TPG does not permit our employees and authorized representatives to send or receive work related e-mails from personal accounts or any other address.
 - @tpg.com
 - @advisorstherisefund.com
 - @advisorstpg.com
 - @advisorsyanalytics.org
 - @texpac.com
 - @texpacdev.com
 - @therisefund.com
 - @tpgglobal.onmicrosoft.com
 - @tpgrefinance.com
 - @tpgriseclimate.com
 - @yanalytics.org
- If you are concerned about a potential fraudulent use of TPG’s name and want to verify a communication from TPG, please contact us at Inquiries@tpg.com.

For further information on staying safe from cyber criminals and fraudsters, please refer to the following resources. TPG provides links to these resources for informational purposes only and is not responsible for their content.

United States

U.S. Securities and Exchange Commission webpage on high-yield investment program fraud: <http://www.sec.gov/answers/highyield.htm>.

U.S. Securities and Exchange Commission webpage on avoiding fraud: <http://investor.gov/investing-basics/avoiding-fraud>

FBI webpage on common fraud schemes: <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud>

If you think you have been the victim of internet crime, you may file a complaint with the FBI’s Internet Crime Complaint Center (IC3) <https://www.ic3.gov/> or the Federal Trade Commission <https://reportfraud.ftc.gov/>

United Kingdom

UK Finance Take Five to Stop Fraud website: <https://takefive-stopfraud.org.uk/>

Financial Conduct Authority's ScamSmart webpage: <https://www.fca.org.uk/scamsmart>

Money & Pensions Service's MoneyHelper website on how to spot an investment scam: <https://www.moneyhelper.org.uk/en/money-troubles/scams/how-to-spot-an-investment-scam>

CIFAS – UK's Fraud Prevention Community: <https://www.cifas.org.uk/>

If you think you have been the victim of internet crime, you may file a report with the UK Police and National Fraud Intelligence Bureau at: <https://www.actionfraud.police.uk/>

Hong Kong

Hong Kong Police Force's Anti-Deception Coordination Center: <https://www.adcc.gov.hk/en-hk/home.html>

Hong Kong Monetary Authority webpage on Financial Fraud: <https://www.hkma.gov.hk/eng/smart-consumers/beware-of-fraudsters/>

Singapore

Singapore National Crime Prevention Council ScamAlert: <https://www.scamalert.sg/>

If you have any questions about the above, the security of any TPG communication, or have concerns about a web site or e-mail communication that you suspect may be fraudulent, please contact us at Inquiries@tpg.com.