



## Recruitment Fraud Alert

At S&P Global, the integrity of our hiring process is a top priority. It has come to our attention that fraudulent individuals and organizations are posing as S&P Global recruiters or hiring managers—often through fake job postings or emails—to deceive job seekers. These scams sometimes involve demands for payment in exchange for job applications, interviews, offer letters, “pre-employment training” fees, payments for equipment and delivery of equipment.

**Please be aware: S&P Global never requires any candidate to pay money for job applications, interviews, offer letters, “pre-employment training” or for equipment/delivery of equipment.**

### What You Should Know:

- Be cautious of the domain names from which you are receiving emails and reach out to [reportfraud@spglobal.com](mailto:reportfraud@spglobal.com) and verify the source of your emails.
- We do not extend job offers without a formal interview process conducted by S&P Global representatives.

### How to Protect Yourself:

- Do not share sensitive personal information (passport, Social Security number, banking information) with unverified contacts.
- Be sceptical of requests to pay for training, equipment, or onboarding.
- Verify job postings through our official channels before taking action.
- Examples of fraudulent domain names include, but are not limited to, [spglobalind.com](http://spglobalind.com).

### Report Suspicious Activity:

If you suspect recruitment fraud using the S&P Global name, please report it to us at [reportfraud@spglobal.com](mailto:reportfraud@spglobal.com). Include any relevant emails or documents you've received so we can investigate promptly.

We are committed to safeguarding the candidate experience and ensuring that your interaction with S&P Global is professional, transparent, and trustworthy.