



RECRUITMENT FRAUD WARNING

It has come to our attention that various individuals and organizations have contacted people offering false employment opportunities with Hill International. Such scams are fraudulent and intended to steal from the victims.

We have taken this matter seriously and notified appropriate legal authorities in an effort to stop such fraudulent schemes. By making you aware of this, we hope to avoid and ultimately stop victims from falling for this scam. Please do not provide any personal or financial information and do not send any money to anyone you suspect of recruitment fraud. Please do not accept any payment or deposit it into your account prior to beginning employment with Hill International. Hill International supplies its employees with equipment and systems necessary to perform their services and will not send you a check in advance of employment or request that you buy your own.

If you are contacted by someone whom you suspect may not be appropriately representing Hill International, please email: ReportRecruitmentFraud@hillintl.com.

Do not send CVs, resumes or vacancy applications to that email address as it will not be reviewed or considered. If you wish to apply for a job, please submit your application for an open position to <https://hillintl.com/careers/>.

What is Recruitment Fraud?

Recruitment fraud is a sophisticated scheme that offers fictitious job opportunities to people. This type of fraud is normally done through online services such as bogus websites, or through unsolicited emails claiming to be from Hill International. These emails request recipients to provide personal information, sign bogus letters of employment, organize visas and ultimately request payments to submit false applications.

How to Identify Recruitment Fraud

- The email does not come from an official hillintl.com email address and instead uses an address from a free email service such as: Gmail, Outlook.com, Live.com, Yahoo, AOL or a combination of these.
- You are asked to interview over an Instant Messenger type program.
- You are guaranteed a work-from-home position.

- You are offered a check to process before being interviewed or following your interview and being offered a position and told to purchase computer or other business equipment. The perpetrators will often ask recipients to complete bogus recruitment documentation, such as application forms, terms and conditions of employment or visa forms. The Hill International name and logo is sometimes featured on the documentation without authority.
- There is an early request for personal information such as address details, date of birth, resume (CV), passport details, etc.
- Candidates are requested to contact other companies/individuals such as lawyers, bank officials, travel agencies, courier companies, visa/immigration processing agencies, etc.
- The perpetrators frequently use mobile or landline telephone numbers beginning with 44(0)70 instead of official company numbers.
- The perpetrators may even offer to pay a large percentage of the fees requested and ask the candidate to pay the remaining amount.
- There is an insistence on urgency.

Hill International employment policies and processes involve personal interviews in most cases and candidates who seek employment with us are never required to pay any sum of money in advance. To do so would be contrary to our business conduct guidelines and ethical practices.

What Should I Do?

- Please report all perceived SCAMS to local authorities.
- Please contact the FBI at this link to report the Internet scam: <https://www.ic3.gov/complaint/default.aspx>

Please Do Not

- Respond to unsolicited business propositions and/or offers of employment from people with whom you are unfamiliar.
- Disclose your personal or financial details to anyone you do not know.
- Send any money. Hill International does not ask for money transfers or payments from applicants to secure a job as an employee or as a contractor.
- Deposit any check sent to you in advance of beginning employment.
- Engage in further communication if you believe the communication may be fraudulent.