CME Group

Recruitment fraud often occurs through online media, including fake recruitment emails, SMS texts, URLs, social media accounts, messaging apps such as WhatsApp and Signal, and online recruitment services. Scammers may use actual employee names and company logos to convey legitimacy.

Please familiarize yourself with the following information to protect yourself against recruitment fraud:

- **CME Group colleagues and recruiters will never solicit money at any point in the recruitment process.**
- **CME Group will never make an offer of employment without conducting a formal interview process.**
- **CME Group will never initiate contact via non-CME Group or personal email, or via encrypted messaging apps such as WhatsApp.** Emails will only come from the cmegroup.com domain.
- **CME Group will not ask you to purchase start-up equipment directly from the company.**
- **CME Group will not request sensitive personal information** such as copies of passports, drivers licenses, credit cards, national identification number, social security number or date of birth during the application process or interview.
- **CME Group will not refer you to a third party to process job applications**. If an offer of employment is extended and accepted, CME Group will utilize a third party to conduct a background check. However, your point of contact at CME Group will explain this process and identify the vendor before you are contacted.

Help us identify fraud:

If you believe that a communication or job offer you received from CME Group may not be legitimate, please contact us at SecurityConcern@cmegroup.com.