

# Beware of scams involving

## fake job postings

The Pason logo is located in the top right corner of the header image. It features the word "pason" in a lowercase, italicized, sans-serif font, enclosed within a white, curved swoosh that resembles a stylized 'P' or a protective shield.

Pason has become aware of fraudulent job offers being made by scammers pretending to represent our company. We take this issue very seriously. By informing you of this, we aim to help prevent unsuspecting individuals from becoming victims of these scams. To verify the legitimacy of Pason job listings found on third-party websites (ex. LinkedIn, Indeed, Monster, ZipRecruiter, Facebook, Craigslist, Kijiji, CareerBuilder, or any other social media platform), please visit [www.pason.com/careers](http://www.pason.com/careers). Job listings posted on Pason's official job board are legitimate.

### What is Recruitment Fraud?

Recruitment fraud is a sophisticated scam that involves offering fake job opportunities. This fraud is often carried out through fake websites or unsolicited emails that appear to come from legitimate companies. Scammers use advanced tactics to look authentic, including creating fake company websites and bank websites, as well as official-looking employment documents such as offer letters, tax forms, personal information forms, and banking deposit forms. While online job sites can be safe places to post your resume and apply for jobs, it is crucial to take the time to research any job offers you receive.

### How to identify Recruitment Fraud?

1. If it sounds too good to be true, it typically is. Confirm market wages through an internet search.
2. If the job posting isn't on Pason's job page ([www.pason.com/careers](http://www.pason.com/careers)), it is not legitimate.
3. Scammers may ask you to complete fake employment documents like offer letters, tax forms, personal information forms, and banking deposit forms. They may use Pason's name and logo on these documents without Pason's permission.
4. Scammers may require you to provide personal information early in the process or during an interview, such as your address, date of birth, driver's licence, passport, Social Insurance Number, credit card or bank information. Pason will not request this type of information until later during the background check process.
5. You may be requested to send information to other companies or individuals, such as lawyers, bank officials, travel agencies, courier companies, visa/immigration processing agencies, etc. Pason will not ask you to do that without speaking to you first and explaining what is required.
6. Email correspondence may appear to be sent from an officer or senior executive of Pason (often from Legal or Human Resources) but is sent from a free web-based email account such as Gmail, Yahoo or Hotmail. If the email address doesn't end with "@pason.com" it is unlikely to be legitimate.
7. The interview may be conducted through Google Hangouts, Telegram App, WhatsApp, texting apps (ex. TextFree app, TextNow app), or no interview may be conducted at all.
8. The scammers may ask for payment to process the job application. They may even offer to pay a large percentage of the fees requested and ask you to pay the remaining amount. Pason never charges a fee in connection with a job application.
9. There is an insistence on urgency.

### What should YOU do if you receive such an email or if an acquaintance forwards such an email to you?

#### Dos

- Send a note with details on the fraudulent message to [careers@pason.com](mailto:careers@pason.com), but do NOT forward the email itself.
- Hold onto the fraudulent message for further investigation.

#### Don'ts

- Do not engage with the original sender.
- Do not forward the fraudulent email to Pason or others.

### Remember

Pason cannot stop scammers from impersonating our business or our employees because information and images on the internet can be stolen regardless of what website they are on. Our hope is that by making you aware of these fraudulent schemes, you will be able to take measures to protect yourself against becoming a victim of these scammers.