# Recruitment scams

## Guidance for hotels to recognise and mitigate the risks to their employees and job seekers of recruitment scams

There are many recruitment frauds that will have an impact on the hotel industry. Recruitment fraud is also known as a recruitment scam, this is when a fraudster claims to be an employer, brand recruiter or hiring agency and creates a fake job in hope of collecting money or personal data.

Recruitment frauds can happen at various levels for example within large criminal networks or business enterprises. Increasing use of technology including social media and messaging services by scammers can often deceive prospective workers, especially those who are vulnerable.[1]

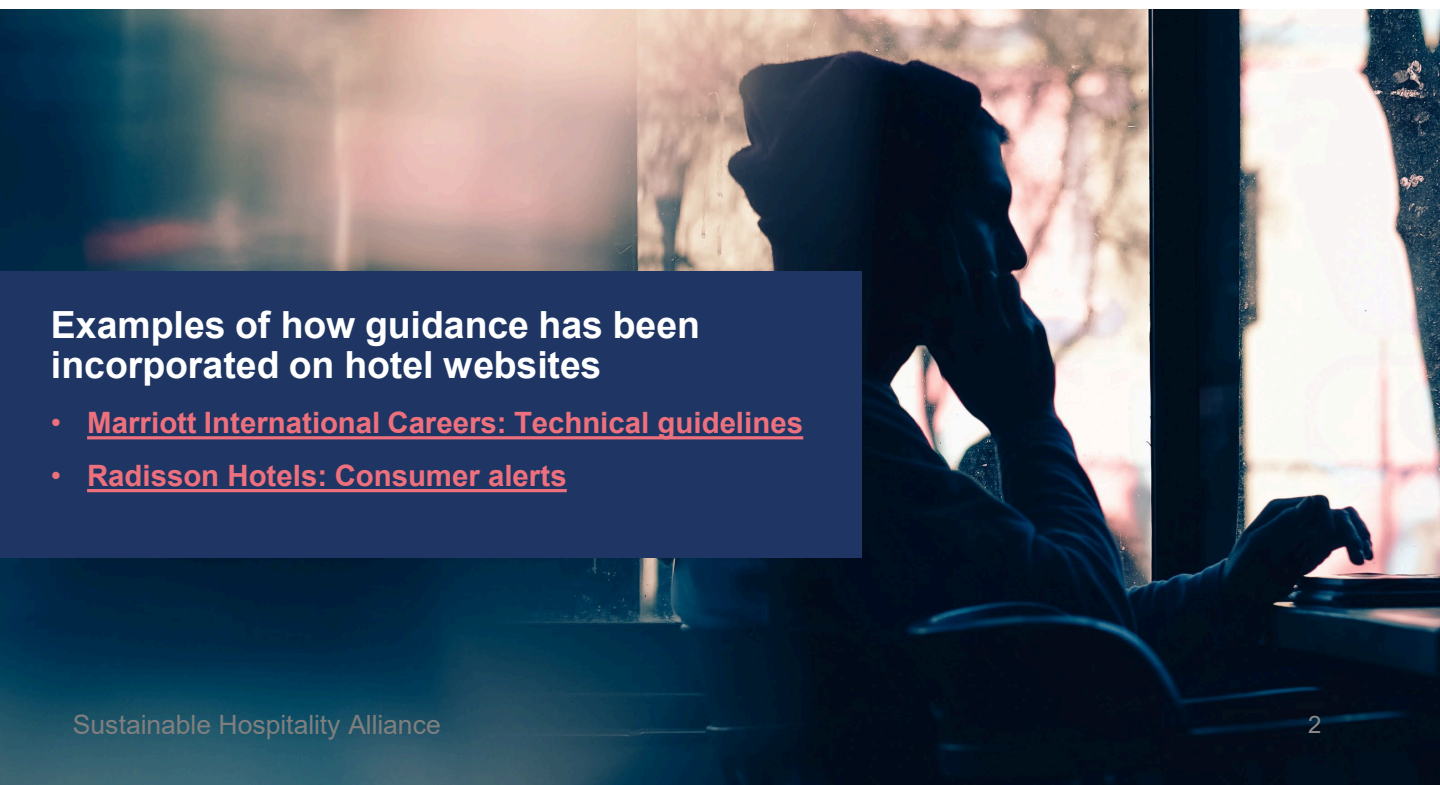
## Common recruitment scams

- **Fake brand websites** designed to fool job seekers into believing that they are applying for a position on the official brand website.
- **Unsolicited emails** from a free account offering amazing job opportunities.
- **False jobs** posted on job boards and on social media.
- Applicants asked to send their application/CV to **fake email addresses or fax numbers**.
- People circulating scams while **posing as representatives for hotels**, agencies/recruiters/recruitment brokers.
- **Contract substitution** where unscrupulous recruiters falsify contracts or deceive workers about their employer.
- Scams on **job-finding public groups** such as Facebook.
- Applicants being asked to **send personal data**, such as national identification number, date of birth, social security number, national insurance number, bank account details, passport information, or any number appearing on identity documents.
- **Advance-fee scams** where a job seeker can be asked to pay for work visas, application fees, travel expenses in advance.
- **Using local newspapers**, or other print materials to advertise fake job openings.
- **Premium-rate phone scams** where job seekers will be asked to call a number that has an extremely high call charge rate. Use of mobile/cellphone numbers rather than a company office number.

[1] ILO, '*Use of digital technology in the recruitment of migrant workers*'

## Suggestions of some preventative measures for the hotel industry

- **Check your job vacancies are not being copied**. For example, set up a Google Alert with your brand's name and words typically used in a job description. HR can monitor the results to ensure that only legitimate results show up.
- **Check for recruitment scams** on Facebook and other social media using your brand.
- **Circulate information on scams among your properties** and communities at a local level in local languages.
- **Alert employees and job seekers** on how to avoid recruitment scams (see guidance on p3).
- **Add a statement or page to your career site** that addresses recruitment scams and provides guidance for job seekers.
- **Make a recruitment scam pack** for agencies and recruiters. This could include information on how to advertise job vacancies and what recruitment fraud looks like.
- **Create a verification site or process** for prospective workers to validate contracts and offers of employment.
- **Create alert system** so employees and job seekers can make you aware of possible recruitment scams occurring in your brand's name. This can take the form of an email address or contact number that can be used if a fraud has been identified.



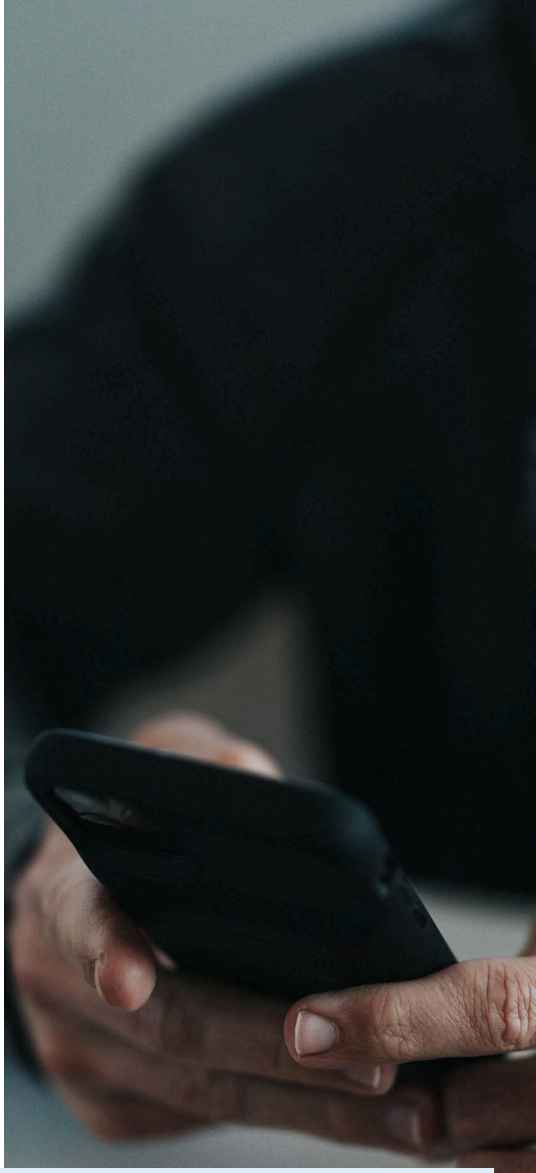
### Examples of how guidance has been incorporated on hotel websites

- Marriott International Careers: Technical guidelines
- Radisson Hotels: Consumer alerts

## What to do if you are informed that a job seeker has been scammed

If you have been informed that a job seeker has been the victim of a scam, you can advise the applicants to undertake the following:

- Contact their **local police department** and advise them that they have been the victim of a recruitment scam.
- Contact their **bank** and make them aware that they have been scammed.
- **Save all messages** they have received from the fraudsters as this will help the police with the investigation.
- **Monitor their bank accounts** for unusual activity if they have given out personal information.
- Contact **local data protection authorities** in their country or region if there are concerns of identity fraud.
- **Monitor call and emails** and if they receive calls from suspicious phone numbers these should be blocked, and any suspicious email should be deleted.
- **Share the job advert** so the brand is aware of fraudulent activity happening in their name.



## Information to circulate amongst employees and job seekers on how to avoid being scammed

- **Carry out research** when applying for positions.
- **Check email addresses** – Professional companies do not use Hotmail, Yahoo or Gmail accounts. Look for misspellings of emails or anything ending in a non-traditional site address. Also, be careful when opening attachments or clicking on links from unfamiliar email addresses.
- **Check company addresses** – Professional companies will not use a PO Box in place of a permanent physical address.
- **Make no upfront payments** and avoid calls or emails requesting personal information.
- **Always interview** – Professional companies will not offer positions without interviewing job seekers.
- **Check company reviews**.
- **Ask around**.
- **Call the company directly**.
- **Do not give out personal information** during or before an interview.
- **Beware of job postings on social media** sites such as Facebook or Instagram, these are not the 'usual' advertisement platforms.
- Do not to engage with **unsolicited offers** of employment from companies, emails or websites they are unfamiliar with.