A Warning About Recruiting Scams

Thank you for your interest in Ricoh! We are delighted that you are considering us for your next career opportunity and invite you to peruse our current open positions to explore a potential fit with our organization.

Unfortunately, among the multitude of reputable companies like Ricoh that seek to attract and engage top talent, there are a fair number of bad actors seeking to take advantage of job seekers using fraudulent recruitment tactics. Given this rise in illicit activities, it is more important than ever to be aware of the threat of recruiting scams that prey on job seekers – both what they can look like, and what protections you can take as you conduct your search.

Fraudulent recruitment activity can take different forms:

1. **Dummy Company Websites:** Always verify the website's authenticity by checking for clear contact information, cross-referencing the company details with reputable sources, and conducting online research to ensure its existence.

2. **Errors and Tone in Job Postings and Communication.** Similar to other types of scams, spelling and grammar errors, unprofessional language, or generic templates are possible indicators of fraudulent activity. Authentic job postings almost always provide specifics about the company, job responsibilities, and qualifications in a professional manner.

3. **Correspondence from free/personal e-mail account (yahoo.com, gmail.com, etc.).** A genuine Ricoh recruiter or hiring manager will never solicit candidates through a non-Ricoh email address or phone number, but always communicate from a Ricoh account or via our recruitment portal.

4. **Requests for Personal Information (PI).** A recruiter or employer asking for sensitive personal information like your social security number, bank account details, or copies of your identification documents early in the recruitment process is a red flag. Reputable companies typically conduct these checks at a later stage and through secure channels.

5. **Requests for Monies/Financial Information.** NEVER make payments or provide financial information to secure a job. Legitimate employers do not ask job seekers to pay for application fees, background checks, or training expenses.

6. **Job Offers Without an Interview.** Legitimate employers like Ricoh invest time in screening and assessing candidates before extending an offer – and so be critical of offers that are extended in the absence of any formal interview process or evaluation of qualifications.

7. **Unsolicited/Unexpected Job Offers.** Be cautious of unsolicited job offers that are extended via email, text message, or social media platforms -- especially if you haven't completed a formal application or heard of the company. Legitimate employers like Ricoh will typically communicate with candidates via our official website or a reputable job portal.

8. **Job Offers Where the Compensation Appears Inconsistent with Responsibilities and Qualifications.** Offers promising high salaries with few requirements can be indicative of a scam, and appropriate research should be done to ensure their validity.

Taking the following steps can help protect you during your job search:

- **Do your research on the potential employer and its representatives**. Use reputable job search platforms, review company websites, and look for online content about the organization to confirm a reputable presence. Ask for names and contact information and verify their credentials, and conduct an online search to confirm

their affiliation with the company.

- **Protect your PI**. Do not offer or provide sensitive/personal information upfront, and only provide personal data when you have verified the legitimacy of the employer and the rationale for the request.

- **Trust your gut**. Paying close attention and being informed as to potential dangers will allow you to develop a sense of legitimacy around the potential opportunity. Listen to your instincts and be cautious when dealing with unfamiliar companies or individuals.

- **Report suspicious activities**. If you suspect fraudulent recruitment activity or believe you have been targeted by a scammer, report the incident to your local law enforcement agency and any relevant job seeker platforms.

We hope this information helps you to stay vigilant and enables you to avoid falling victim to recruiting scams. If you feel you have received an offer from Ricoh -- or any recruitment-related communication -- that may not be legitimate, please reach out to us at RicohCareerOpportunities@ricoh-usa.com.

Thanks again for your interest in Ricoh, and we wish you the best with your search!