By: *Susan Grant*, *Director of Consumer Protection and Privacy, Consumer Federation of America, and Nick Roper, Administrative & Advocacy Associate, Consumer Federation of America*

When you visit sites like Indeed, ZipRecruiter, LinkedIn, or GlassDoor, you're likely to find many different companies seeking workers. Unfortunately, it can be difficult to distinguish legitimate online job offers from those placed by people who are out to scam you, especially when it comes to work-from-home jobs. Even worse, these scams have become very sophisticated. What may seem like a lucrative job that allows schedule flexibility may actually be a scheme designed to steal your money, time, and even your identity.

Georgia Attorney General Chris Carr recently warned consumers about a rising tide of fake employers who post on job websites and forums to exploit their victims. The alert described a complaint to the Georgia Consumer Protection Division:

[A] scammer sent an email posing as a manager from a company called Huawei Technologies. In an email, the scammer claimed that after reviewing the applicant's resume, they were offering her a job working from home that involved price comparing products online and entering that information into a Google spreadsheet. The scammer told the victim she would receive $4,000 a month for this work. Once the victim accepted the job, the scammer sent another email asking her to fill out a W-4, a direct deposit authorization form, a photo of the front and back sides of her driver's license, a current photo of herself, and a utility bill (as "proof of residency"). The victim emailed back this information and began work as described. She did not realize she had been scammed until a month went by and she never received a paycheck as promised. By then, she was unable to reach the scammer, who now had all the information needed to access her bank account, create fake IDs, commit tax identity fraud, and apply for credit cards in the victim's name.

How can you protect yourself? The Georgia Consumer Protection Division suggests that

consumers should watch out for these “red flags of a job scam”:

· **Requests for payment.** Real placement agents or employers do not require payment from job applicants, whether it’s for training materials, certification, background and credit checks, or the recruiter’s expenses for placing you with a company.

· **Requests for sensitive financial or personal information.** You should be suspicious of any company that requests via phone or email your Social Security number, driver’s license, bank account, PayPal, or credit card information as part of the initial application process.

· **Offers high salary for simple tasks or minimal experience.** A legitimate employer will evaluate your experience and abilities before deciding on what to pay you. Scammers commonly advertise high-paying jobs that state “no experience necessary” or “will train.” Remember, if it sounds too good to be true, it could be!

· **Immediately offers job.** Actual employers take their time to research and get to know potential job candidates before offering a position. Be skeptical of a job offer that has come via email, when you’ve never had a telephone or in-person interview.

· **Communicates via non-business address.** If a company communicates from a free email account such as Yahoo or Gmail, this could signify a scam. Legitimate job-related emails usually come from corporate email accounts.

· **Know the common scams.** Ads for envelope stuffing, at-home craft or assembly work, medical or claims processing, and refund recovery, are often placed by scammers. Additionally, be on the lookout for jobs that ask you to accept payment to your own bank account and then wire money on behalf of the company. Almost always, the money the victims are transferring is stolen, and therefore, you would be committing theft and wire fraud.

· **Do your homework.** If you’ve never heard of the company, research it on the Better Business Bureau’s website. You might also do a search for the company name and the word “complaints” or “scam.” If you recognize the company name, contact it through the phone

number listed on the legitimate website and verify whether it is actually seeking to hire for the position in question, and if so, what the hiring process consists of.

"Job scammers often take advantage of young adults who are new to the workforce and retirees trying to supplement their income," says Susan Grant, CFA Director of Consumer Protection and Privacy. "People looking for work they can do from home because they are disabled or have young children are also targets." Grant offers some additional tips for recognizing fraudulent job listings:

· **Use the "lack of info" test.** Real job postings from real companies usually have contact details such as website links, an email to reach the hiring manager, or a phone number for the business. If a job posting doesn't have one of these, do a little more digging before sending your personal information. A simple online search will often reveal a lot about a company. Because scammers may use the names of real businesses, however, contact the company directly to verify the job posting.

· **Be wary of vague descriptions and sloppy language.** While these scams are becoming more sophisticated, many bogus job ads may have vague language, misspelled words, grammatical errors, or may be written in all caps. These should ring alarm bells for anyone on the hunt for a job.

· **Limit your personal information.** With scammers out to steal job applicants' identities, it's a good idea to limit the information you provide on a resume and CV. Never include your date of birth, driver's license number, social security number, bank account number, or credit card numbers.

· **Keep a list of where you've applied.** Scammers know that hunting for a job is tough and requires people to send out countless resumes and CVs to potential jobs. They may take advantage of this by emailing you posing as a hiring manager from a well-known company. Keep a list of where you've applied and where your resume is posted so you can catch these scams early.

· **Report fake posts.** If you've stumbled onto a fake job post and recognize it as such, don't let others fall victim. Job board sites often offer a report feature to flag these scams

(usually located at the bottom of the job posting). Report the post and be as descriptive as you can so the job board can remove it and block future postings by that scammer.

· **Warn your friends and family.** If they're also looking for work, pass the information along so they'll be aware of phony job postings and how to avoid falling for them.

· **Remember, there are real jobs out there.** Job searching can be stressful and time consuming. Always trust your gut, though. If you think the job is too good to be true, it is. Don't waste your time (and potentially lose your identity) by applying for something you suspect is a scam.

For tips about how to avoid another type of work-at-home job scam, this one involving phony checks, go to https://consumerfed.org/consumer_info/consumer-tips-fake-check-scams/ .