IDAHO
DEPARTMENT OF FINANCE

BRAD LITTLE
Governor

PATRICIA R. PERKINS
Director

Contact: Celia Kinney
Consumer Affairs Officer
(208) 332-8067

NEWS RELEASE

FOR IMMEDIATE RELEASE **December 28, 2022**

CONSUMER ALERT
AVOID FALLING PREY TO EMPLOYMENT SCAMS

Boise, Idaho… The Idaho Department of Finance is warning jobseekers to be aware of the red flags of employment scams in light of a recent consumer complaint the Department received, and the continued prevalence of these scams nationwide. In the first quarter of 2022, U.S. consumers were scammed out of $68 million as a result of fake business and job opportunity schemes according to the Federal Trade Commission. Although this is not a new threat, it continues to have a devastating impact on victims resulting in monetary harm, identity theft, and even unwitting involvement in criminal schemes such as money laundering.

"Employment scams are egregious in that they target individuals intentionally seeking to improve their financial futures," said Patricia Perkins, Director of the Idaho Department of Finance. "It is particularly important that consumers take precautions to verify the identity of the job poster and position before they engage."

Employment scams occur when cyber criminals deceive jobseekers into believing they have a potential job, then leverage their role as an "employer" to elicit the desired information or action from the victim. These criminals pose as employers or recruiters online much like legitimate employers do, through employment websites, advertisements on social media channels, newspapers, or may communicate via unsolicited e-mails or text messages. They lure jobseekers with flashy descriptions or low-effort, high-reward offers.

According to a consumer advisory from the Federal Bureau of Investigation (FBI), most often cyber criminals impersonate a company's website by creating a domain name that is similar to a legitimate company, then post fake positions on popular websites that direct jobseekers to apply on the spoofed sites. Applicants are contacted by email to conduct an interview using a teleconference application. After being interviewed, victims are offered jobs, usually in a work-at-home capacity.

To appear legitimate, criminals may send victims an employment contract to physically sign, and request a copy of the victims' driver's licenses, Social Security numbers, direct deposit information, and credit card information. Criminals may request payment upfront for costs that will later be reimbursed such as background checks or start-up equipment, but once they get money, criminals cease communications.

Alternatively, in the recent consumer complaint the Department received, the victim responded to an employment advertisement on social media, securing what was described as a project management position. Several days after depositing their first earnings check, the consumer received notification from their financial institution that the check had been returned, resulting in substantial financial loss to the individual; this is also known as a fake check scam.

Fake check scams often occur in conjunction with employment scams; a consumer receives a check with direction to deposit the funds and instructed to repay excess funds by purchasing gift cards, wire transfer, or investing in cryptocurrency. Eventually the check bounces, and the consumer is liable to repay the funds. Consumers should be aware that a cleared check does not equate to a good check, financial institutions are required under law to make funds available shortly after a deposit is made, and it can take several days to determine if the instrument is false.

Before Beginning a Job Search, or Responding to an Offer, Consider These Guidelines

- **Never provide personal information upfront**. If you are being asked for your social security number, driver's license number, or financial information before the offer, the job is likely a scam. Even if the request for information occurs after a formal offer, be vigilant to confirm the employer's identity in-person or over video before sharing personal information even after an offer has occurred.
- **Be skeptical of vague communication from a potential employer**. Scammers generally avoid direct questions, and face-to-face interactions such as interviews conducted in-person or secure video call. Watch for interviews conducted via teleconference applications that use email addresses instead of phone numbers, this can be a red flag.
- **Research the company or name of the person that claims to be hiring you**. Search terms such as "scam" or "complaint" for more targeted results. Scammers often impersonate legitimate companies so examine any communication for discrepancies such as slightly altered domain names, web addresses, misspellings or grammatical errors. Try to confirm the legitimacy of a job post by cross-referencing the company's website for the same offer.
- **Beware of any job offer that requires payment.** If a potential employer is requesting payment as a condition of employment, it's a scam.
- **Discuss the job offer or business opportunity with a trusted third party before proceeding.**

If You Suspect You Are a Victim of An Employment Scam

- Immediately contact your financial institution, or the holder of the account that was used to transfer payment (wire transfer, crypto platform, etc.) and report the fraudulent or suspicious activity. Ask that any transactions be stopped or reversed but be mindful that it can be difficult if not impossible to recover funds lost as a result of a scam.
- Keep copies of all communications with scammers and report them to the Federal Bureau of Investigation's Internet Crime Complaint Center at https://www.ic3.gov/Home/ComplaintChoice and the Federal Trade Commission at https://reportfraud.ftc.gov/.
- If applicable, report the activity to the website in which the job posting was listed, and to the company the cybercriminal impersonated.
- Visit IdentityTheft.gov for a personalized recovery plan, including how to monitor your credit.
- Update personal passwords, enable multifactor authentication when possible, and update your computer's security software if a scammer has remotely accessed your computer.

****

Consumers can obtain information about financial firms, professionals or products, as well as view more Department press releases and other information on the Internet at http://finance.idaho.gov or by contacting the Department at (208) 332-8000 or Idaho toll-free at 1-888-346-3378.