



**FINANCIAL
CRIMES**
VICTIM ADVOCACY

Hiring/Job Scams

Hiring/Job Scams

In an uncertain economy and job market, the LAST THING we need are bad actors targeting people trying to re-enter or enter the workforce. But, unfortunately, there are no safe places from scammers. I've learned quickly over the last few weeks when I re-entered the job market, it's definitely something job seekers have to pay close attention to.

It's clear that scammers are targeting apps like LinkedIn, using AI, to trick job-seekers into providing their information.

True to my style of dealing with pieces of shit, I'm taking the bull by the horns. So, if you hit me up with a job scam, I'm going to put you on blast. You're welcome.

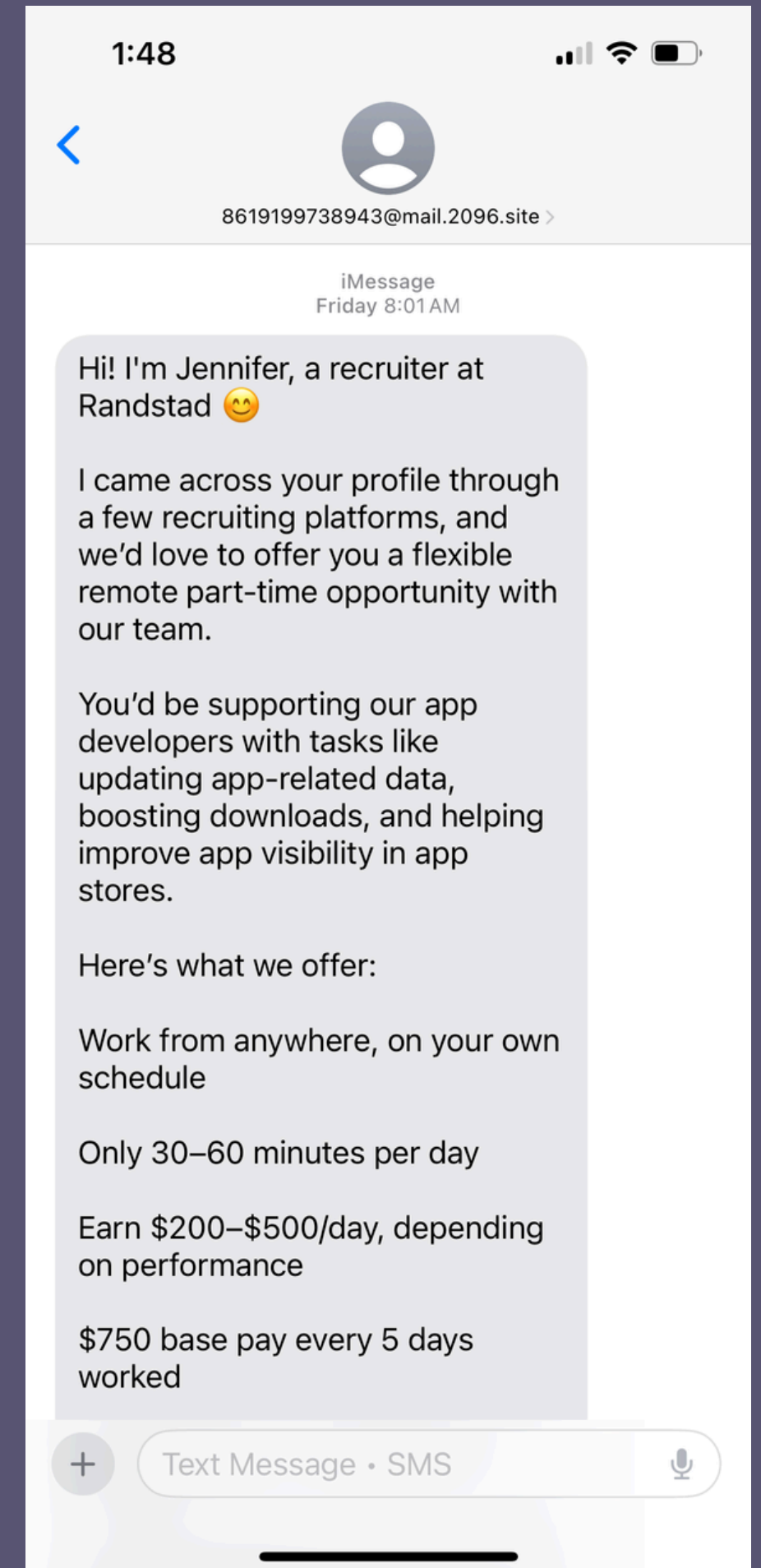
I'm learning quickly, but wanted to share just a few of the "offers" I've received over the last few weeks, so that you hopefully won't have to deal with this non-sense, and more importantly, that you protect your information from getting in the hands of a bad actor.

Ready, Set, Go!!

Hiring/Job Scams - Red Flags

What are some of the tell-tale signs of fraudulent recruiting?

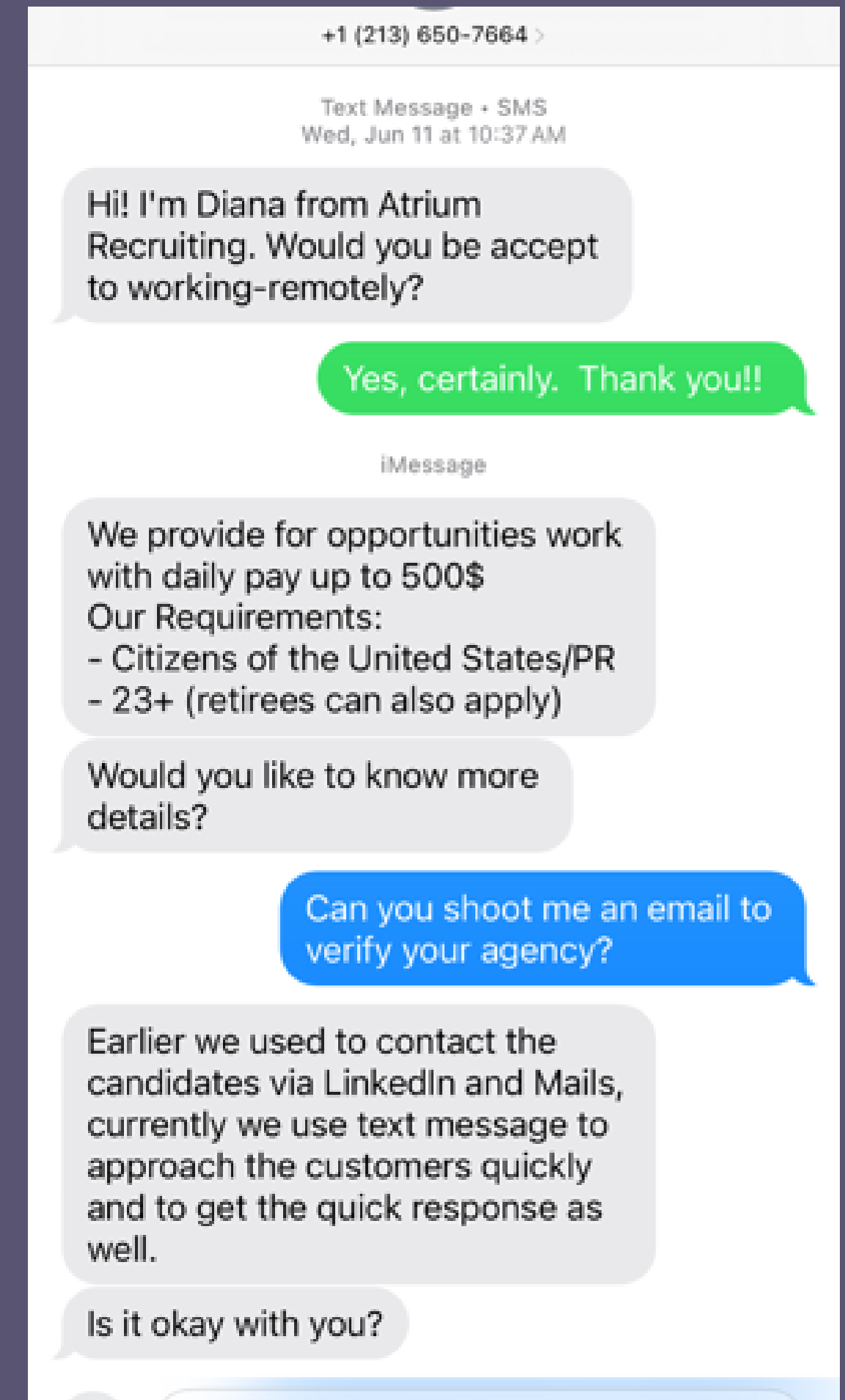
- If it sounds too good to be true, it probably is!
- Initial contact by text message, not through LinkedIn or email, with insistence that communications be maintained outside of email. (Remember - legitimate emails will have a domain name, and would not come from a gmail account). They may try to push to communicate through WhatsApp, or other anonymized email communications.



Hiring/Job Scams - Red Flags

What are some of the tell-tale signs of fraudulent recruiting?

- Language barriers - See the first sentence with broken English
- Check the phone number - conduct an online search to see if it matches the business.



LinkedIn Scams - Red Flags

What are some of the tell-tale signs of fraudulent recruiting on LinkedIn?

- If you have changed your LinkedIn profile to “OpenToWork”, watch for fraudulent recruiters.
 - Look at the recruiter’s profile in LinkedIn - if they have less than ten followers, that is a HUGE RED FLAG!! Avoid giving them ANY information!

Activity

0 followers

Posts

Comments



Cassandra Hlenn • 3rd+

Executive Director of Recruiting Operatio...

1h •

...

Hello, I have a fantastic job opening at our company that matches your expertise. I'd love to discuss it with you! Please send me a connection request or [...more](#)



Cassandra Hlenn • 1:40 PM

This sender appears to be trying to move the conversation off LinkedIn. We recommend you review these [safety tips](#) before proceeding. [View message anyway](#)

Hiring/Job Scams - Protecting Yourself

What Steps Can I Take to Protect Myself?

- Contact them directly through the contact information on their website.
- Verify employment of the Employer's through their HR representative. If using a recruiting or contract agency, verify the recruiter information.
- Never pay a fee to get a job, unless you initiated the contact through your own recruiter. No legitimate business will charge you to be hired.
- NEVER provide your Social Security number, or bank account account details to anyone you are interviewing with!
- Never click any links in messages from a hiring manager, without verifying.

What Is It That They Want?

- **Bottom line - your information!**
- They may also ask you for a deposit or upfront fee to secure a job - you should never have to pay to get a job!

What To Do If You Become a Victim

- Cease all communications with the fraudster
- Contact your bank and immediately place holds on any compromised accounts and/or bank cards
- Change passwords to any compromised accounts
- Immediately report the fraud to the Federal Trade Commission ([ReportFraud.FTC.gov](https://www.ftc.gov/report-fraud))
- Report the fraud to Internet Crime Complaint Center, IC3 ([IC3.gov](https://www.ic3.gov))
- Report the fraud to local police and/or Sheriff's office in your jurisdiction.
- Make sure your home computer and mobile devices have been restored with the latest virus protection software
- Contact your mobile phone provider to ensure your phone is clean and has not been compromised.

What To Do If You Become a Victim

Other entities you may need to contact:

If your personal identification information (e.g., name, social security number and date of birth) has potentially been compromised, monitor your credit through [identitytheft.gov](https://www.identitytheft.gov).

Need Help?
**If you have questions or are a fraud victim
needing assistance, contact us.**



Email: support@fcvadvocacy.com

Phone: 888-264-2010

