Infiltrating the Scam: A Pig Butchering Investigation

blogs.infoblox.com/threat-intelligence/telegram-tango-dancing-with-a-scammer/

Infoblox Threat Intel May 6, 2025

One gray morning this winter, a random person contacted me on Telegram and asked if I was interested in working a part-time, remote job. They said their name was Arabella and told me the job would pay US$150-$310 per day. Better yet, the job required no experience and they would train me for free! (see Figure 1). Arabella's message included an image with a logo for "Corner Office Consultants" and the domain corneroffice consultants[.]com (see Figure 2).

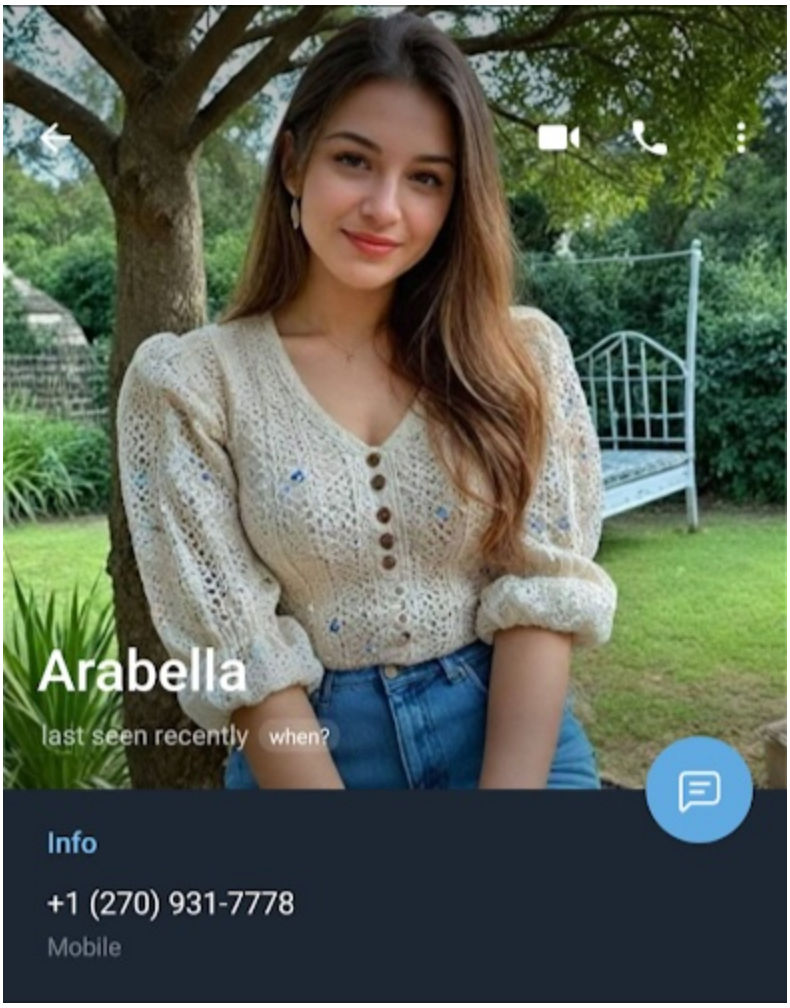
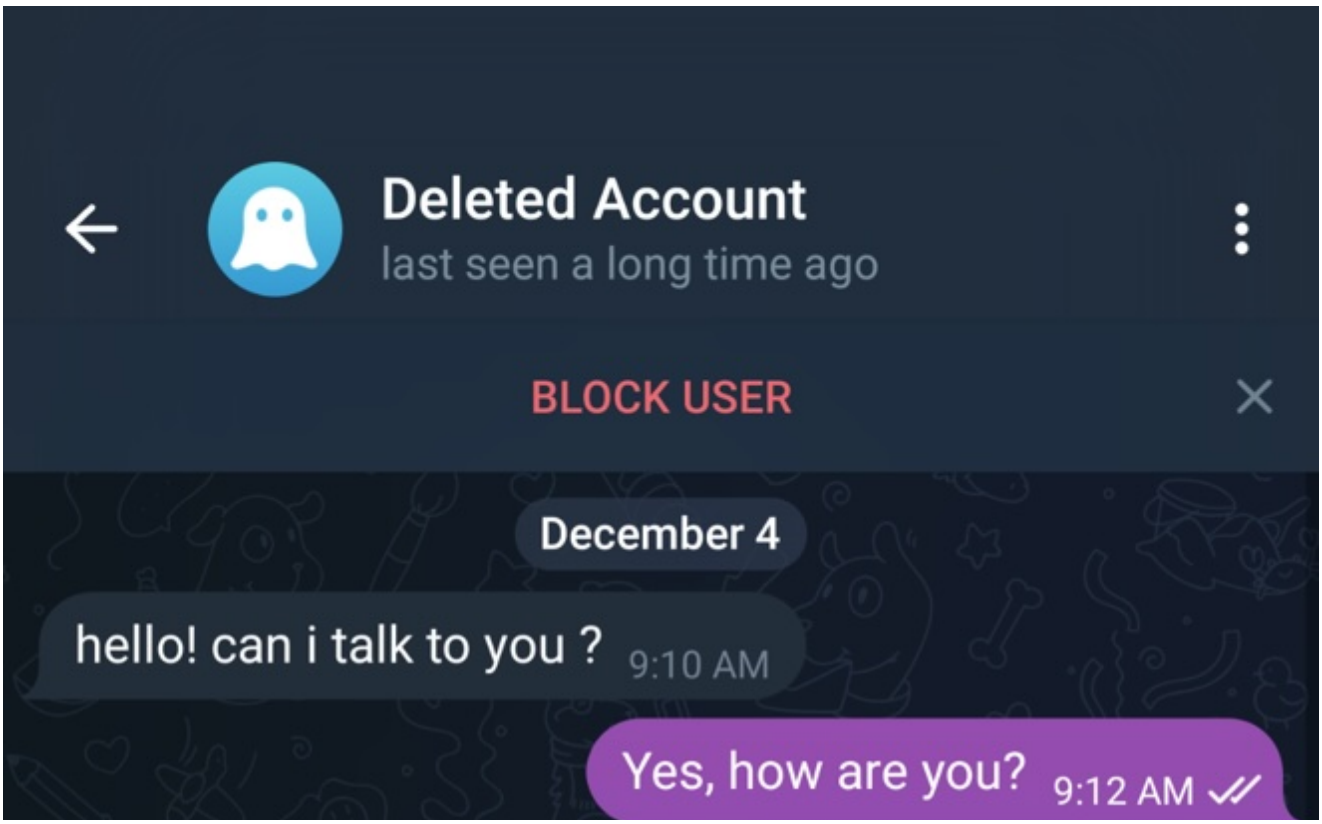


Figure 1. Arabella’s Telegram profile



Nice to meet you. My name is Arabella . from Corner-Office Consultants. 9:12 AM

Can lexplain to you a little bit about this jobremotely? 9:12 AM

Yes I would love to hear about it 9:12 AM ✓✓

Nice to meet you as well 9:13 AM ✓✓

Okay, I will send some details to you first. 9:13 AM

Delete this chat

Figure 2. Initial messages from Arabella

This business and the domain name are legitimate. But I was sure Arabella was part of an increasingly large scam industry and this was all a ruse. As a threat researcher, I know all about the concepts of these scams, but Arabella was giving me the chance to get the real experience of a victim.

I jumped at the opportunity and told her I'd love to work for Corner Office Consultants. Over the days that followed, I interacted with several different accounts, some seemingly human, some seemingly AI. I performed meaningless tasks and was asked to pay various amounts of cryptocurrency into the scammer's wallet. I tried and failed to scam the scammers and then tried again. And of course, I recorded everything along the way. This blog is a blow-by-blow account of my adventure, twists and turns included.

Soon after accepting the job offer, a different "employee" named Maria (Figure 3) contacted me. She told me that she got my contact info from Arabella and provided this job description: "Marble Media provides a work platform where users can click on and submit apps, helping them achieve better rankings and ratings in the app store, and through this process, we can earn commissions and salary." Marble Media is also a real company, but the domain Maria gave me, marblemediaseo[.]cc, is a lookalike unrelated to the marketing firm.

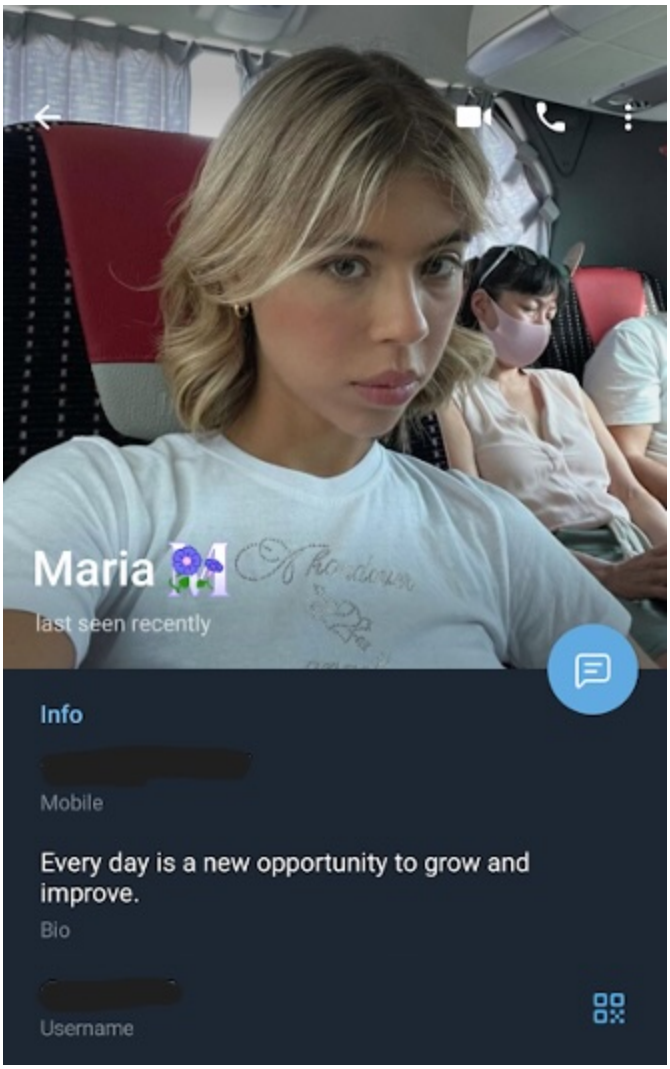


Figure 3. Maria's Telegram profile

Maria gave me credentials for a training account on the lookalike domain and then had me register an account of my own. To prevent unwanted users from signing up, she provided me with an invite code that I had to enter during the account creation process. The account keeps track of my balance and profit. The balance is used to place the orders, and the profit is how much I have earned from my work.

I started my training and quickly became proficient at my new job, which involved mindlessly clicking the same two buttons over and over and over again: "Starting" and "Submit" (see Figures 4 and 5). I was asked to fill 40 so-called "orders" for my "training" assignment, but their website was a bit slow so I had to wait a couple of seconds between each click for it to work. This quickly became very monotonous; but hey, easy money!

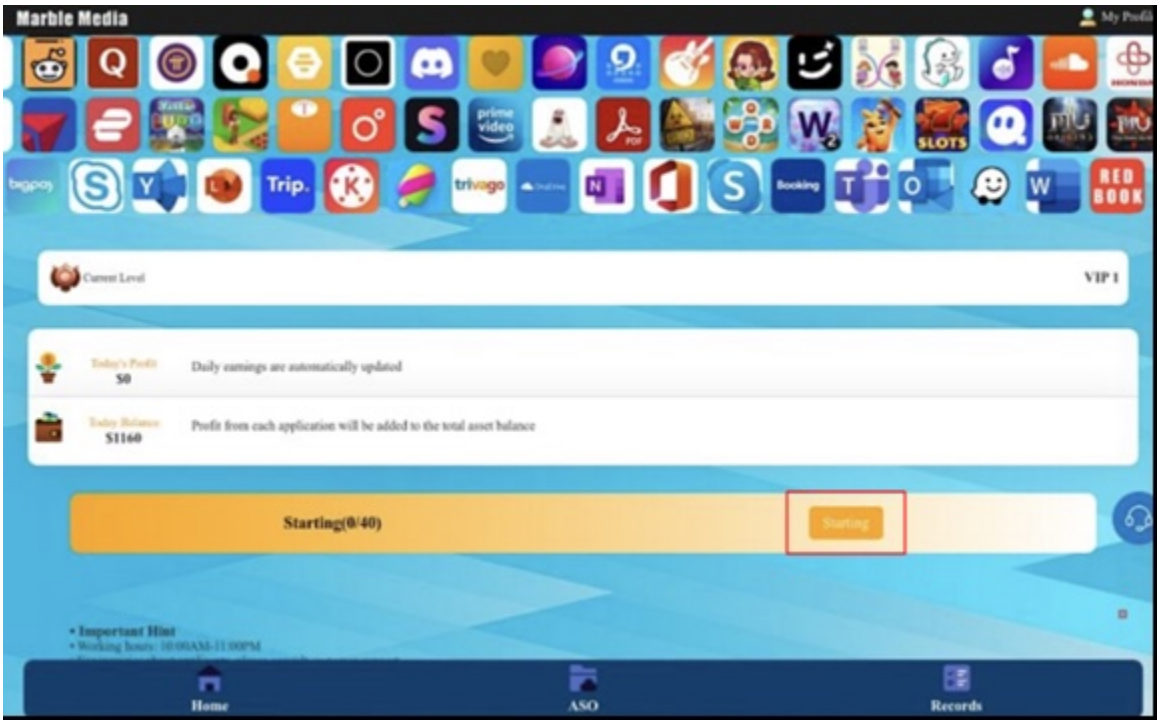


Figure 4. Screenshot of the scam task website highlighting the “Starting” button

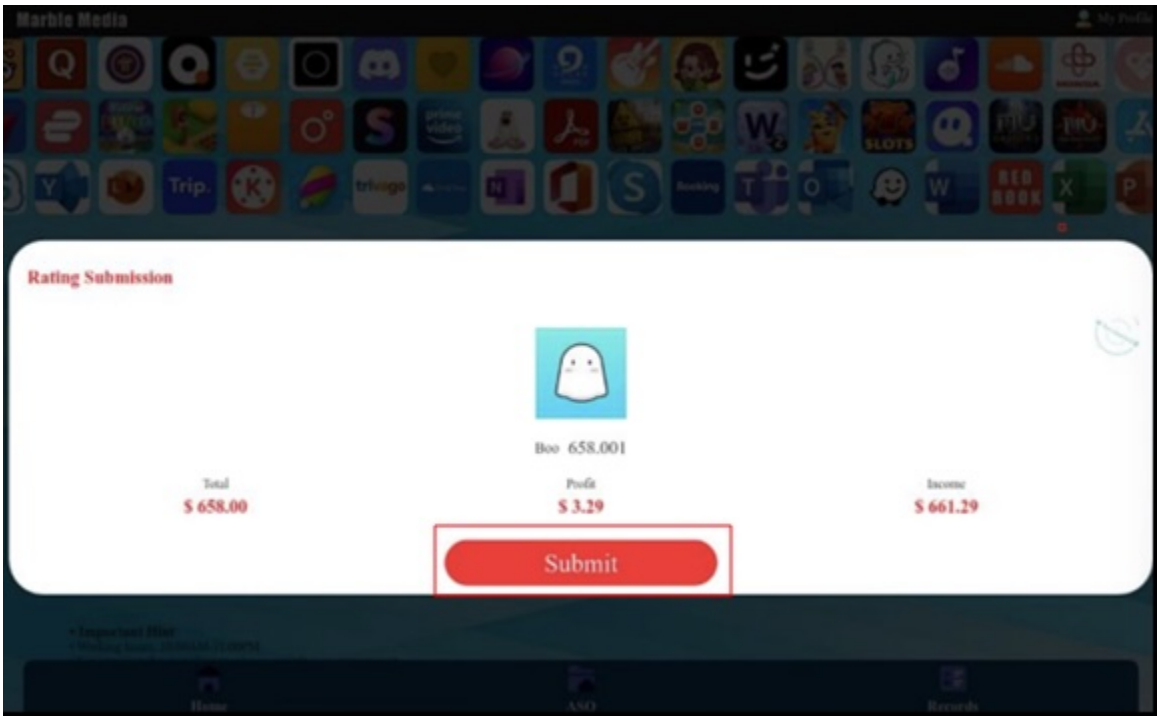


Figure 5. Screenshot of completing one of the orders, highlighting the “Submit” button

During my time working for the scammers, there was a lot of text communication. I suspect that they were using a mix of AI/large language models (LLMs) along with human interaction for the chat messages. Some of the responses from them were nearly instant, as well as

being somewhat lengthy, while others took a while longer even if the message was shorter. It seemed to me that some responses may be automated, but it was not clear whether there was some sort of process to hand off the interaction to a human in some cases.

There were other red flags. One of the orders I received was for the app “Apollo for Reddit,” which shut down in June 2023,[1] well over a year before this interaction took place. It seems the template or data they used for this domain was quite out of date.

It wasn’t clear at first, but I actually needed to pay money in order to work and earn money! While attempting to complete the rest of my 40 orders, I hit a roadblock: an error message stated, “Insufficient account available balance” and indicated that the balance was (–)$616 on the training account (Figure 6). At this point, I could not fill any more orders due to the negative balance, so I messaged Maria to ask what to do next.

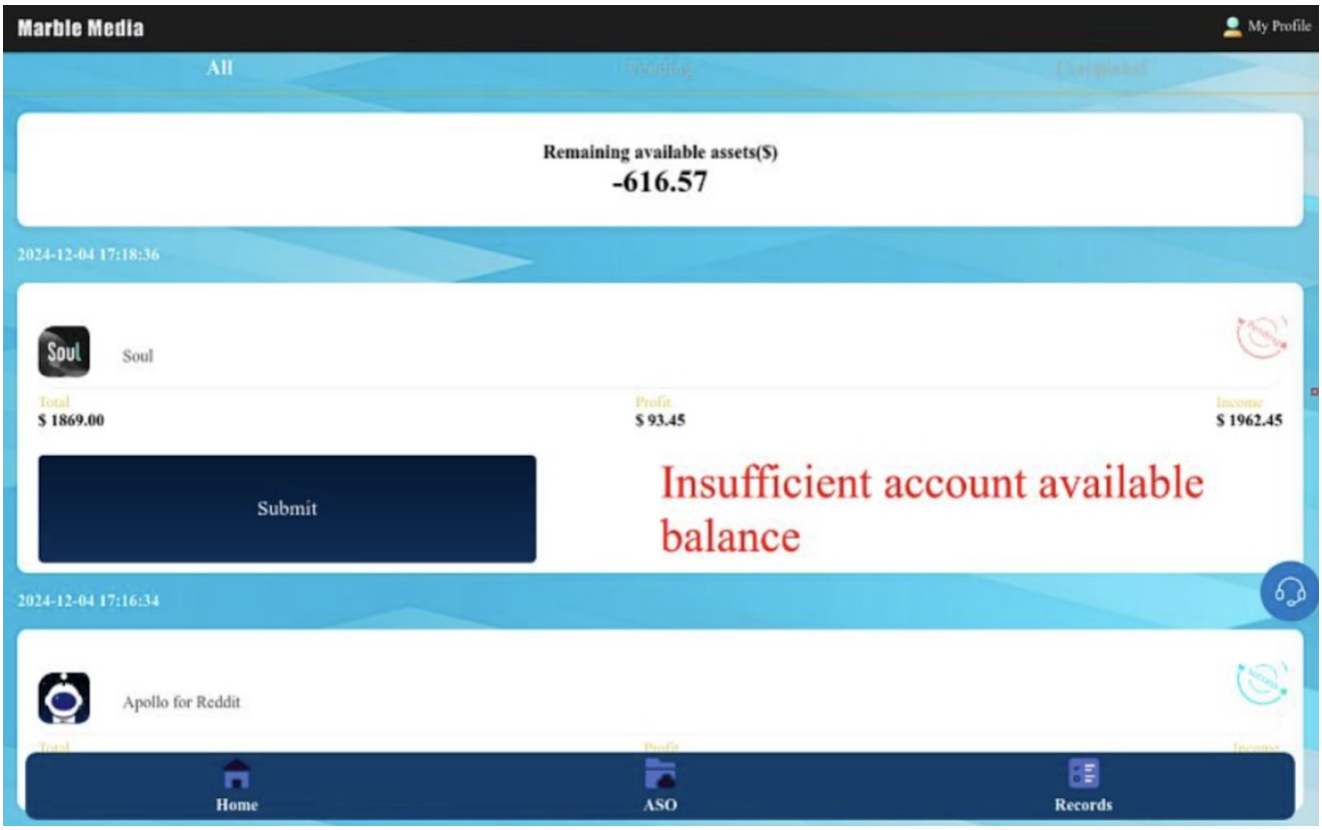


Figure 6. Screenshot of website showing “Insufficient account available balance”

Maria explained that I needed to deposit money into the account to continue, but the reasoning was a mystery. She said I was “very lucky” and got a “high-profit order,” which pays ten times the normal commission (see Figure 7 below). In order to keep me working, she would pay the balance this time. How generous! It still wasn’t clear why I had to deposit funds, but I soldiered on.

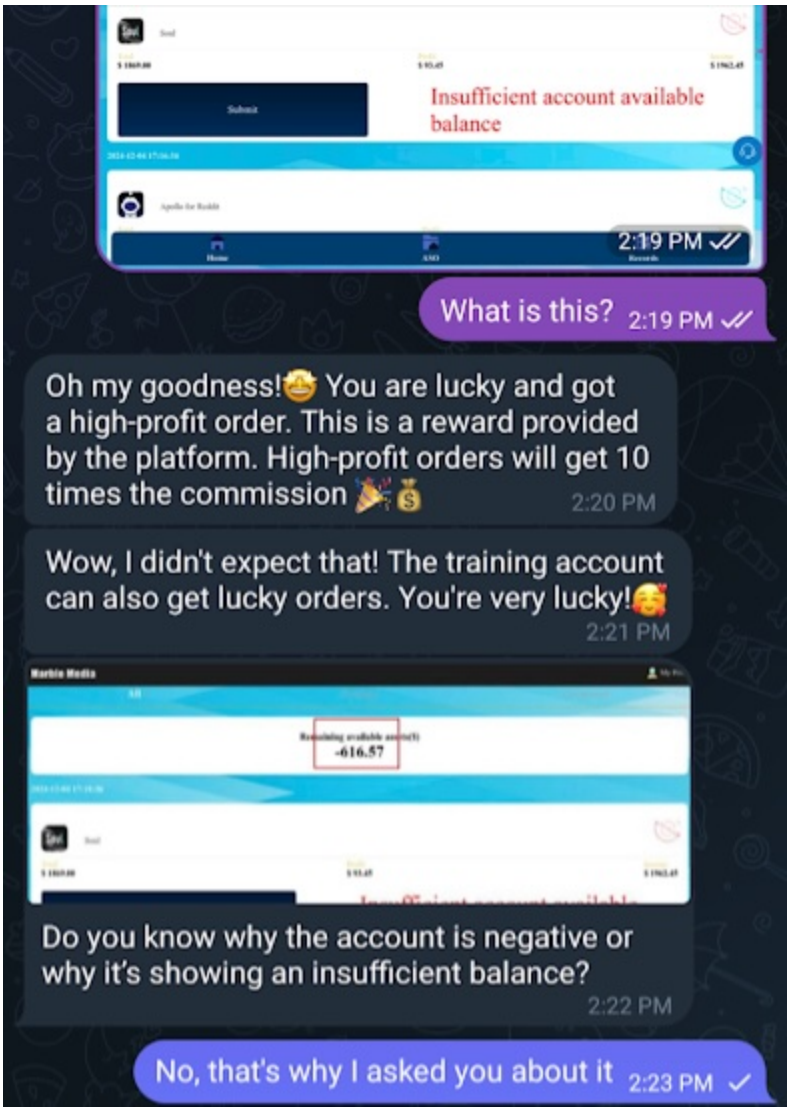


Figure 7. Asking Maria about the insufficient account balance

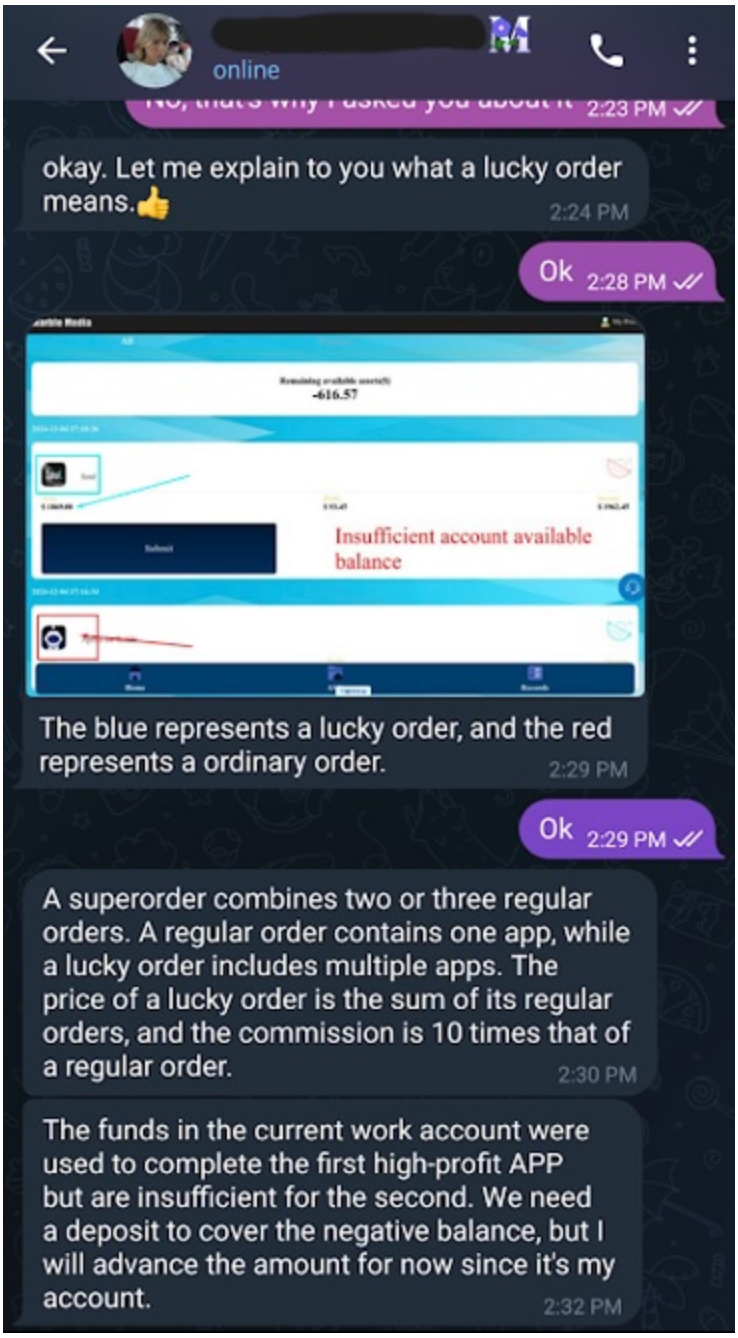


Figure 8. Maria's explanation of "lucky orders"

Maria walked me through the deposit process and introduced me to a new contact—Marble Media's Customer Support Agent—who handles the financial transactions. I reverse image searched the profile picture and found that they were using a stock photo for this account (Figure 9).

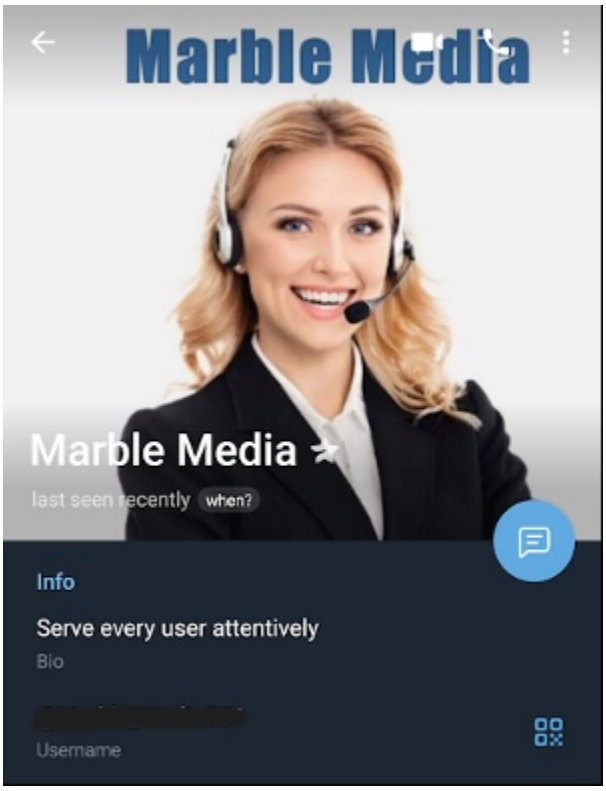


Figure 9. Customer Support Agent's Telegram profile

Maria told me to reach out to this Customer Support Agent, who gave me the address of the Ethereum wallet where Maria would make the deposit to clear my path (Figure 10). Being a threat researcher, I was curious, so I looked up the wallet and saw that it held over 18 Ethereum, worth over $70,000 at the time (Figure 11).

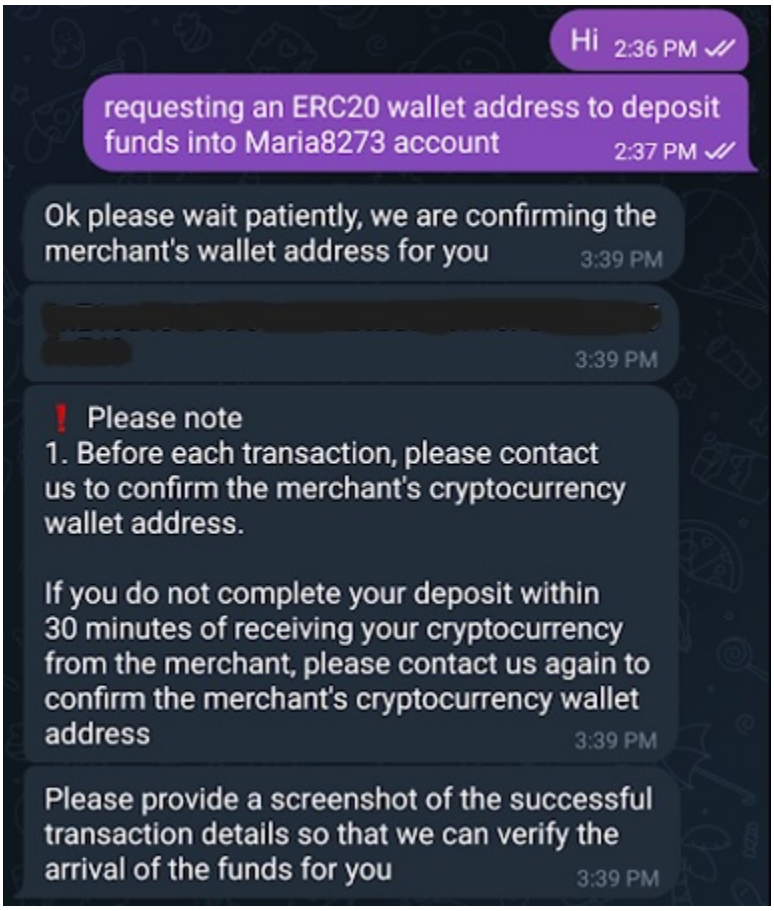


Figure 10. Customer Support Agent sending the wallet address

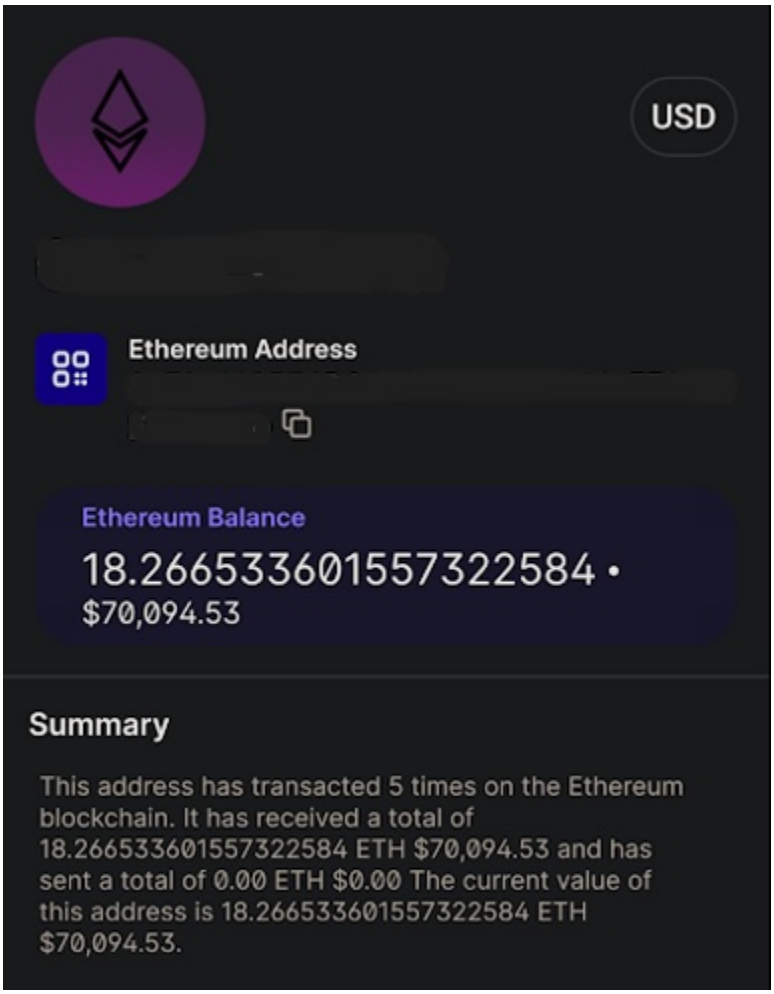


Figure 11. Screenshot of the wallet's balance

This gave me an idea and I decided to test it out. Instead of giving Maria the address that the Customer Support Agent supplied, I edited a screenshot of the chat and put in my own wallet address, then sent it to Maria. I was hoping that she would deposit the money to me. Unfortunately, Maria did not fall for this and deposited the money into the wallet that the Customer Support Agent had supplied. How did she know?! Perhaps it's some kind of standard wallet for the training phase. When Maria sent me a screenshot of the transaction with her deposit and instructed me to send it to the Customer Support Agent, I did.

At this point, I figured they wouldn't be interested in working with me anymore since I blatantly tried to scam them, so I stopped messaging them for the day. They didn't call me out for my trick though, either.

After some sleep, I devised a way to continue pushing this interaction forward. I told Maria that I think I contacted the wrong customer support agent and was actually talking to a scammer! She replied "ok" and I completed my 40 tasks, concluding my training.

Next, Maria gave me the green light to start working in my own account and "deposited" some money into my account on their website. She also dangled a carrot in front of me: during training, the account earned $243 in profit; presumably, I could be making that soon

(Figure 12).

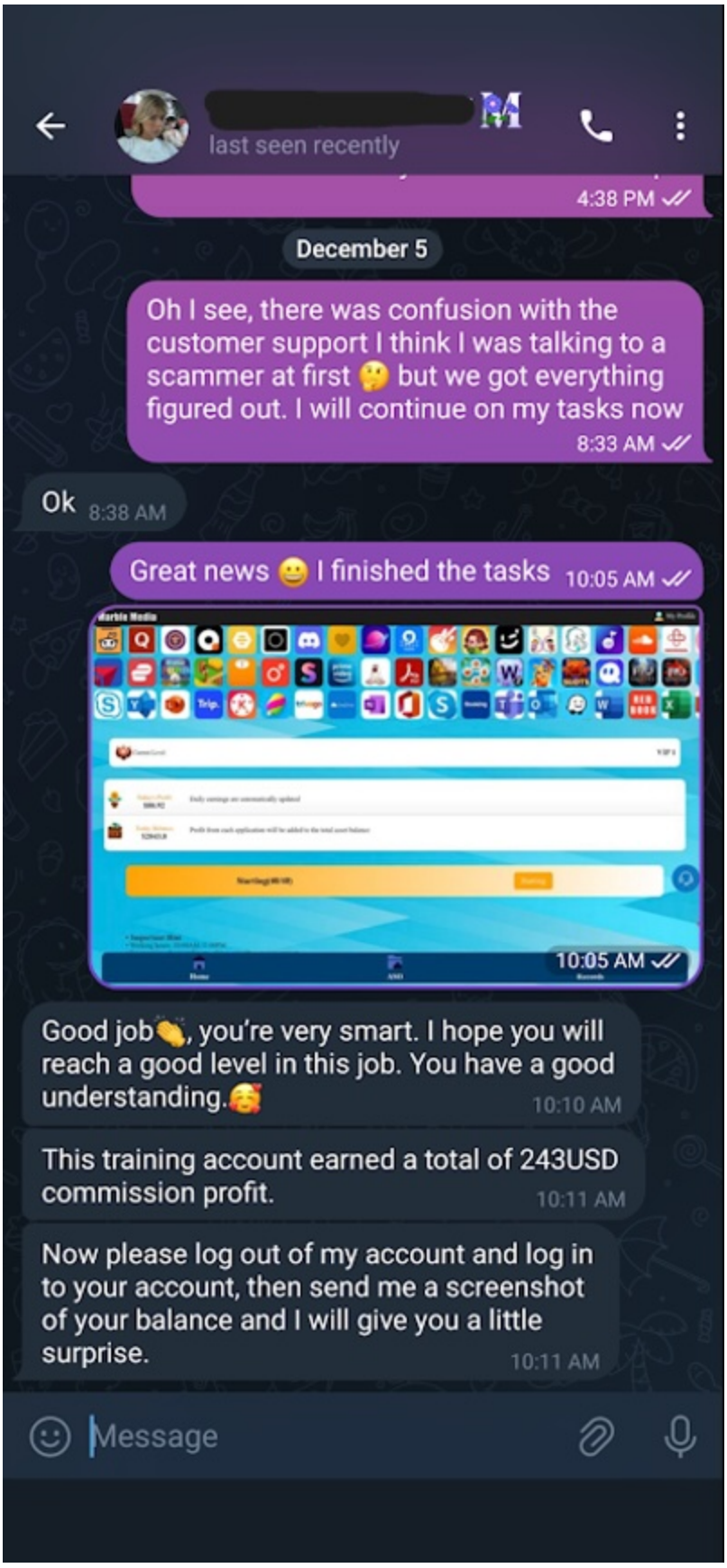


Figure 12. Maria telling me how much profit the training account made

Motivated, I got down to business working in my own account. I completed my 40 tasks and told Maria I had finished. I was looking forward to figuring out the payment process for my account when she threw me a curveball and told me that there are actually two sets of tasks to complete, and I could not start working on the second set until I “reset” my tasks. This was a new twist, so I asked her how I should do that? I was not entirely surprised when the answer was to send them cryptocurrency. Specifically, she needed $26 worth of Ethereum before I could continue (Figure 13).

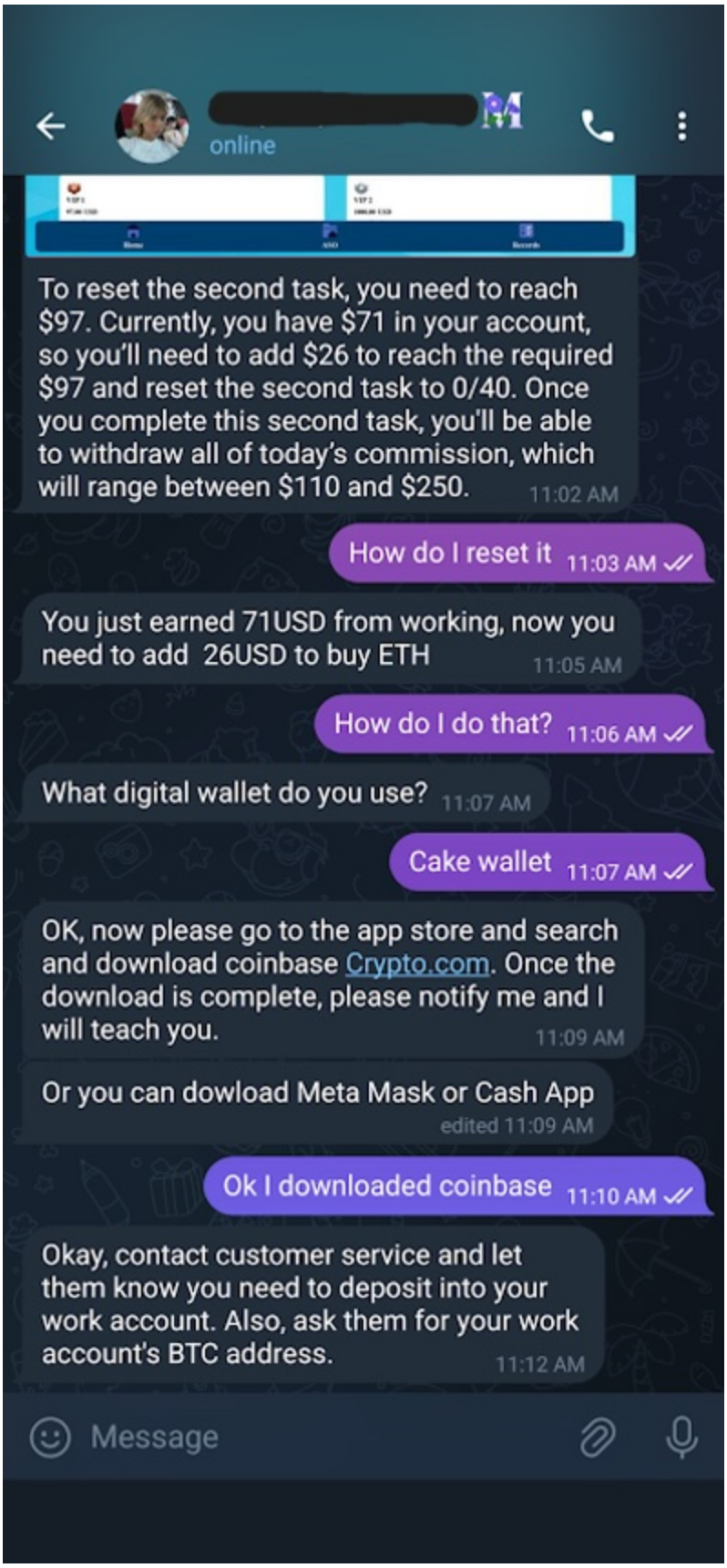


Figure 13. Maria tells me I need to send her $26 of Ethereum to continue working

Once again, I contacted the Customer Support Agent to get the address of the wallet to make my payment, theoretically (Figure 14). I wanted to see how everything worked, but I also was not going to send them any money. Luckily, one of my colleagues had a genius idea: fake a screenshot showing my “transaction.”

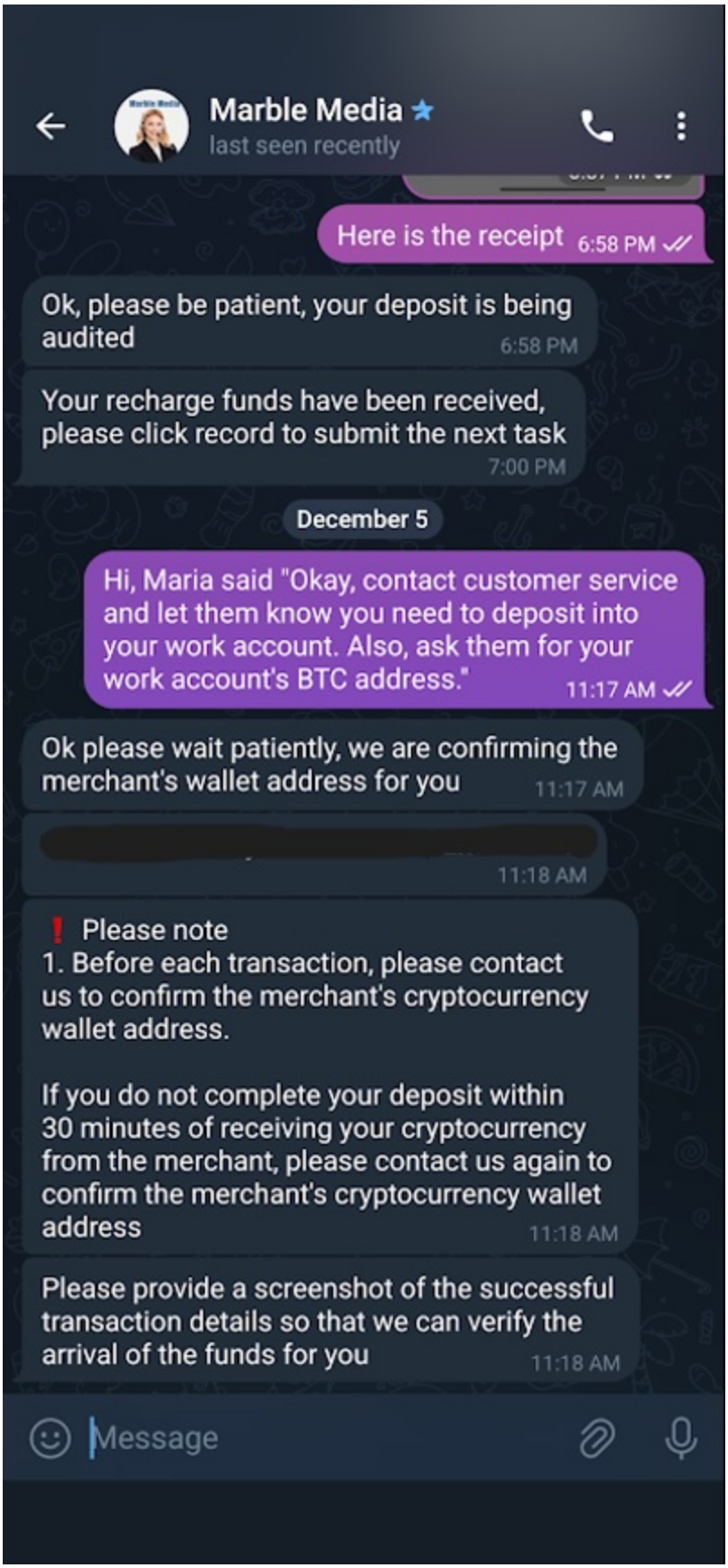


Figure 14. Customer Support Agent sending me a new wallet address

I searched online for a crypto transaction screenshot and edited it to make it look like I sent approximately the correct amount to their wallet (Figure 15). In hindsight, there were several discrepancies that could have easily been noticed, but to my delight, they did not seem to validate my claim to have made this transaction.

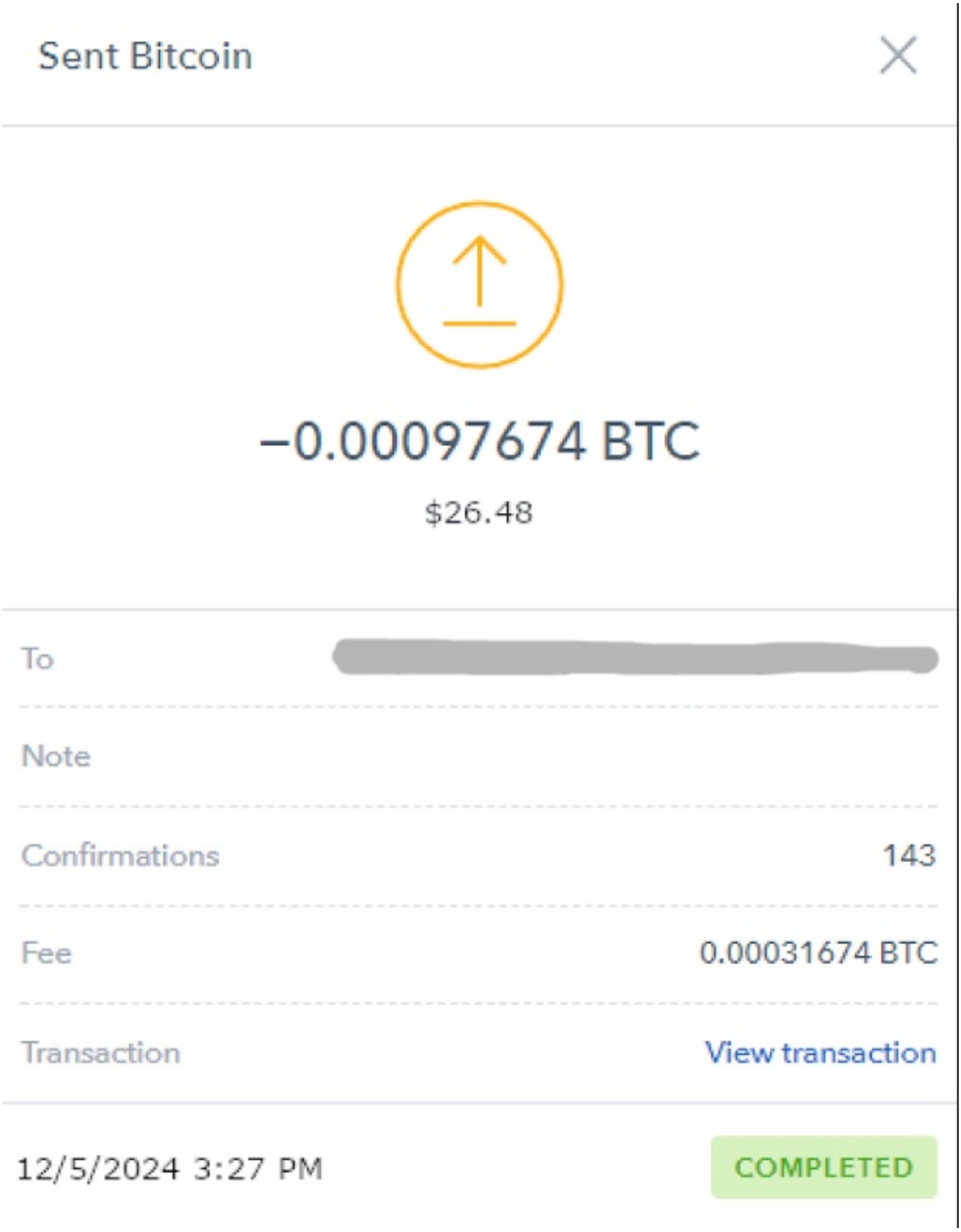


Figure 15. Edited screenshot of a cryptocurrency transaction

I wasn't in the clear yet, though. Customer Support did have a problem: they could not find my deposit and asked for the transaction ID so that they could confirm it. I had not included a transaction ID in my screenshot, so I searched through the history of their wallet and caught a lucky break. There happened to be a transaction earlier that day for an amount similar to what I claimed to have paid. I hoped they wouldn't notice the minor difference if I sent that transaction ID to them (Figure 16).

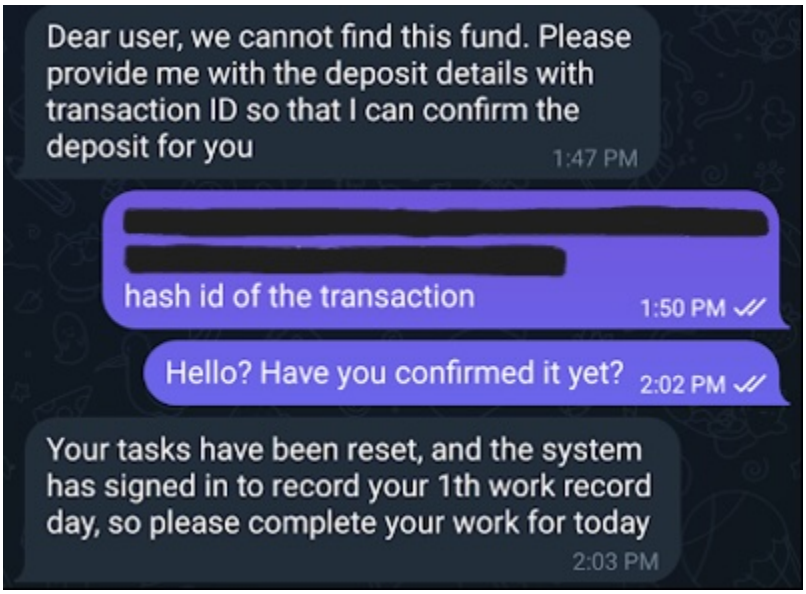


Figure 16. Sending the Customer Support Agent the transaction ID

For the next 12 minutes I waited in anticipation for a reply. Would they believe it? Was I too sloppy?

Finally, the Customer Support Agent replied, "Your tasks have been reset." I logged back into my account and saw the balance had increased. They fell for it! Newly inspired, I completed my second set of tasks for the day so that I could withdraw my hard-earned money.

Despite spending time digging around the website trying to figure out how to do so, I couldn't get past one seemingly simple roadblock. The withdrawal section allows the user to set an amount to withdraw but it did not allow a wallet address to be entered. It was impossible to type in that box. See Figure 17.

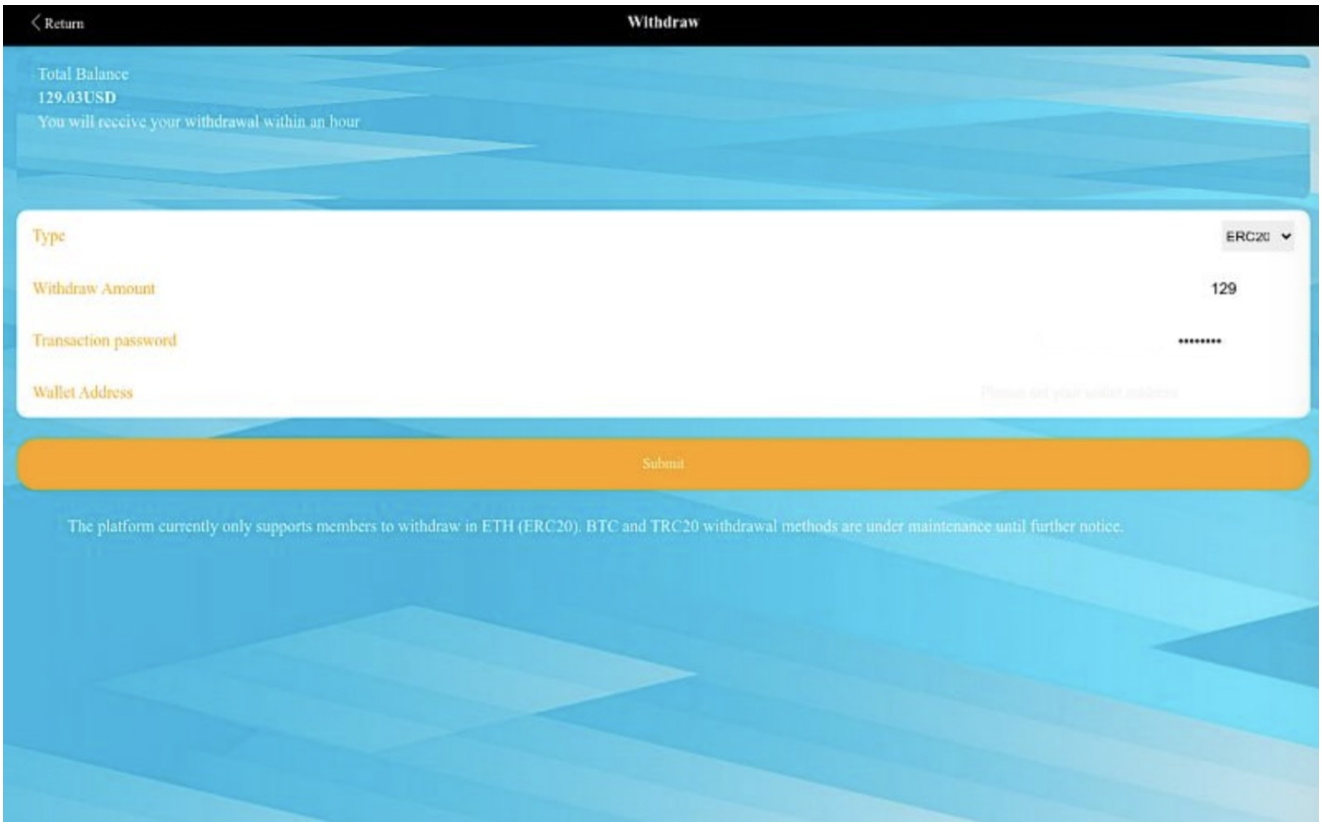


Figure 17. Scam website's withdrawal page

I was stuck and reached out to Maria for help in figuring out the withdrawal process. Figures 18 and 19 show the conversation; spoiler alert: it didn't go well.

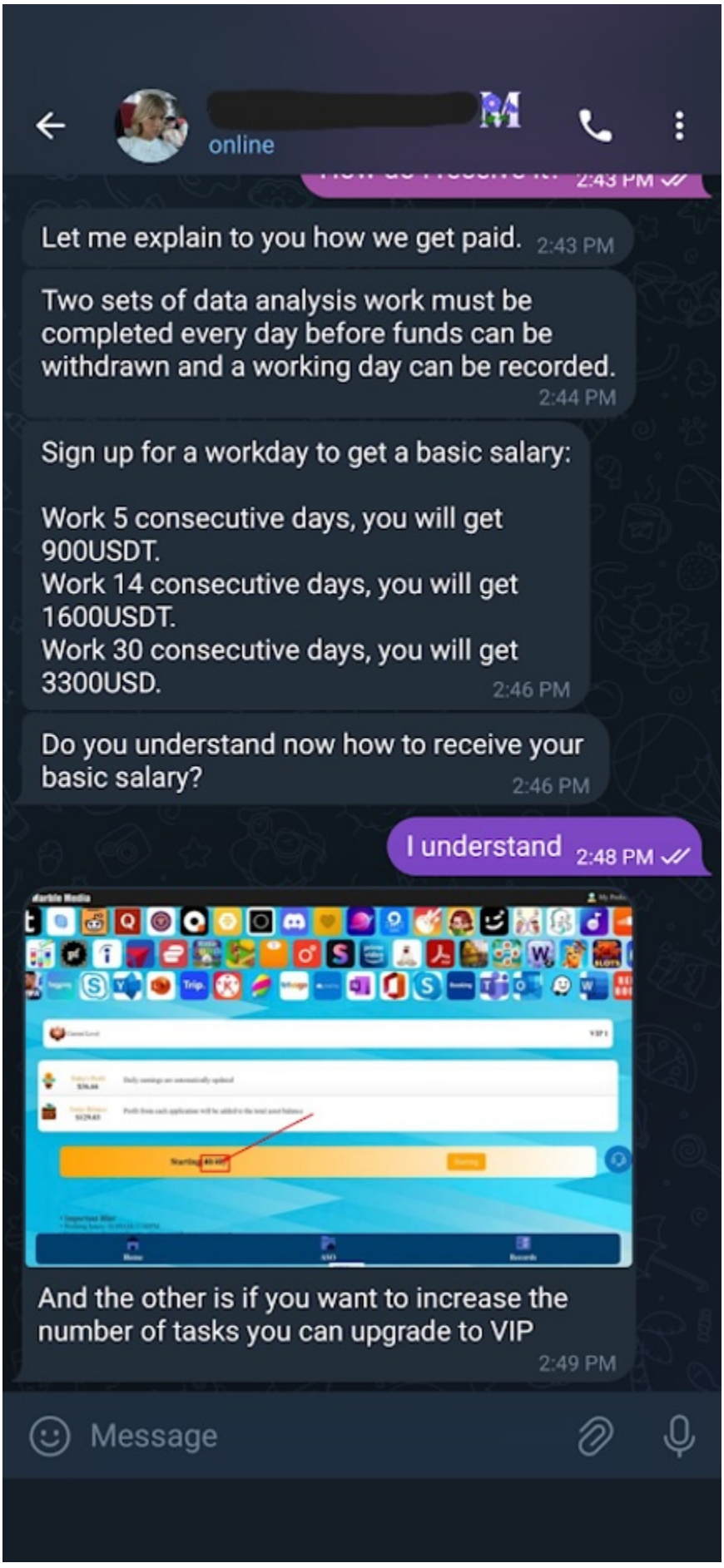

[redacted]
online
2:43 PM
Let me explain to you how we get paid. 2:43 PM
Two sets of data analysis work must be completed every day before funds can be withdrawn and a working day can be recorded. 2:44 PM
Sign up for a workday to get a basic salary:
Work 5 consecutive days, you will get 900USDT.
Work 14 consecutive days, you will get 1600USDT.
Work 30 consecutive days, you will get 3300USD. 2:46 PM
Do you understand now how to receive your basic salary? 2:46 PM
I understand 2:48 PM
And the other is if you want to increase the number of tasks you can upgrade to VIP 2:49 PM
Message

Figure 18. Maria explaining the hypothetical salary for the job

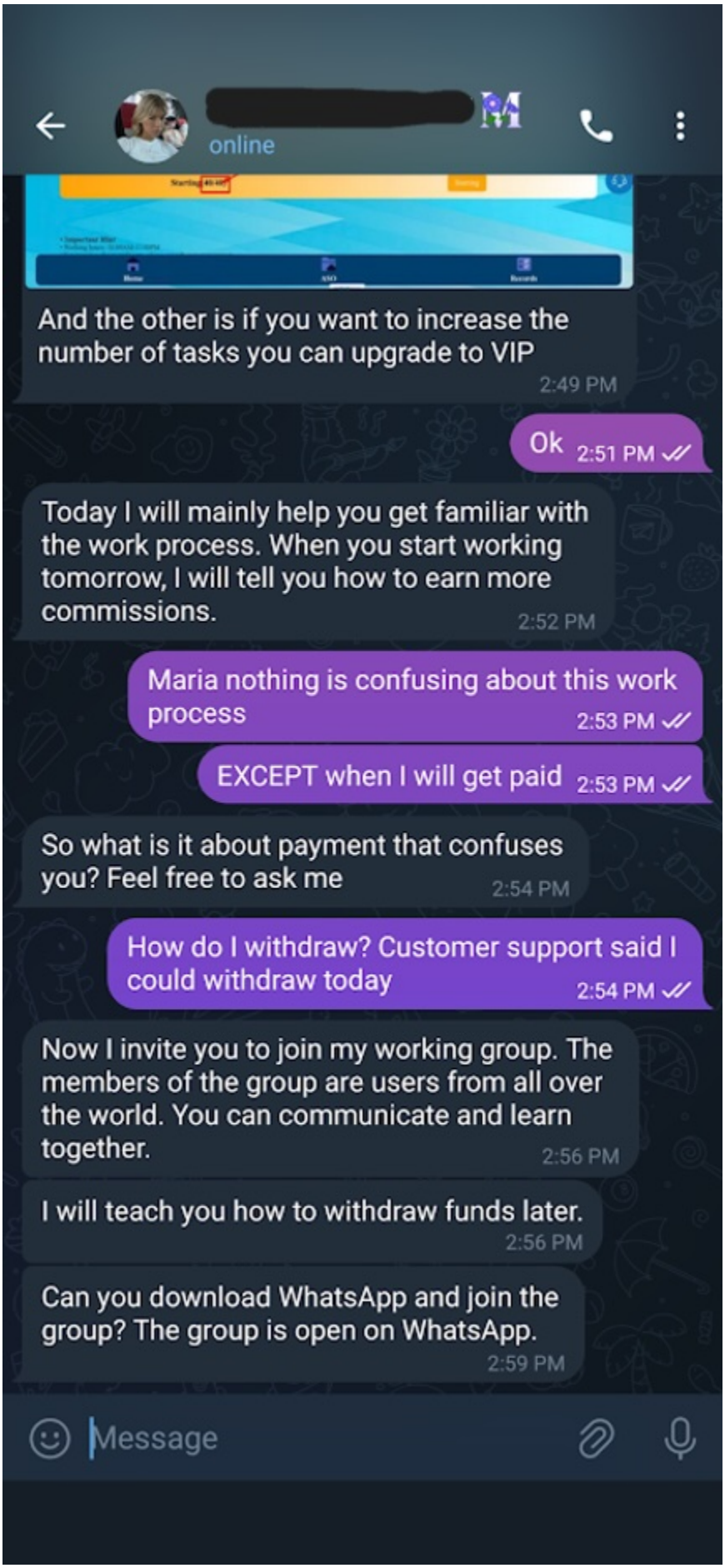

[redacted]
online
And the other is if you want to increase the number of tasks you can upgrade to VIP
2:49 PM
Ok 2:51 PM
Today I will mainly help you get familiar with the work process. When you start working tomorrow, I will tell you how to earn more commissions.
2:52 PM
Maria nothing is confusing about this work process
2:53 PM
EXCEPT when I will get paid 2:53 PM
So what is it about payment that confuses you? Feel free to ask me
2:54 PM
How do I withdraw? Customer support said I could withdraw today
2:54 PM
Now I invite you to join my working group. The members of the group are users from all over the world. You can communicate and learn together.
2:56 PM
I will teach you how to withdraw funds later.
2:56 PM
Can you download WhatsApp and join the group? The group is open on WhatsApp.
2:59 PM
Message

Figure 19. Maria dodging my questions about how to withdraw my earnings

Maria and I went back and forth for about 20 minutes, but she avoided answering my question and ultimately tried to redirect me with the messages “Now I invite you to join my working group … You can communicate and learn together. I will teach you how to withdraw funds later.” I was not interested in joining this work group though, I was focused on getting my crypto currency. Frustrated, I turned to the Customer Support Agent for answers, but they didn’t reply to me.

In the hopes that taking a different angle with Maria would lead to progress, I went back to her and asked specifically how to set the wallet address in the withdrawal screen. Success! Turns out I had to go into my account settings and set the withdrawal address from there. It would then be filled in the withdrawal page automatically. I set my address, submitted the request to cash out the $129 that I had earned and messaged Customer Support. To my surprise, the request was approved. I eagerly stared at my wallet app for several minutes and eventually I received a notification:

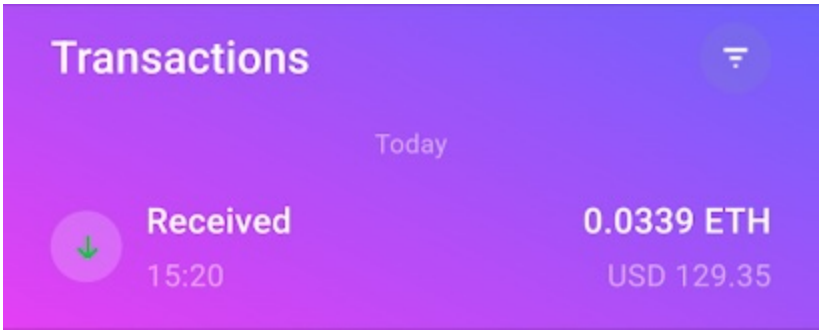


Figure 20. I finally received the 0.0339 ETH

They sent me 0.0339 ETH; thanks for the free crypto!

Naturally, the next day I wanted to do this again (minus the hiccups, of course). I had discovered these scammers had a flaw in their validation system and I wanted to continue exploiting it. Feeling highly motivated, I completed my tasks planning to pull off the same stunt.

Unfortunately, they threw a huge wrench into my plan: they sent me a different wallet address. One that hadn’t been used before. One with zero transactions associated with it.

I assumed there was no way my scheme would work this time. Their validation wasn’t great, but it wouldn’t take a genius to see that the balance of their wallet was $0.00. The transaction history is what made this plan work. A bit disappointed, I decided to just ignore them and try again later.

The next day, I woke up to a message from Maria saying that she wanted to have breakfast with me (Figure 21). This was different from our previous conversations, which were strictly business related. It felt like she was trying to go down the route of a more typical, romance-themed pig butchering scam.

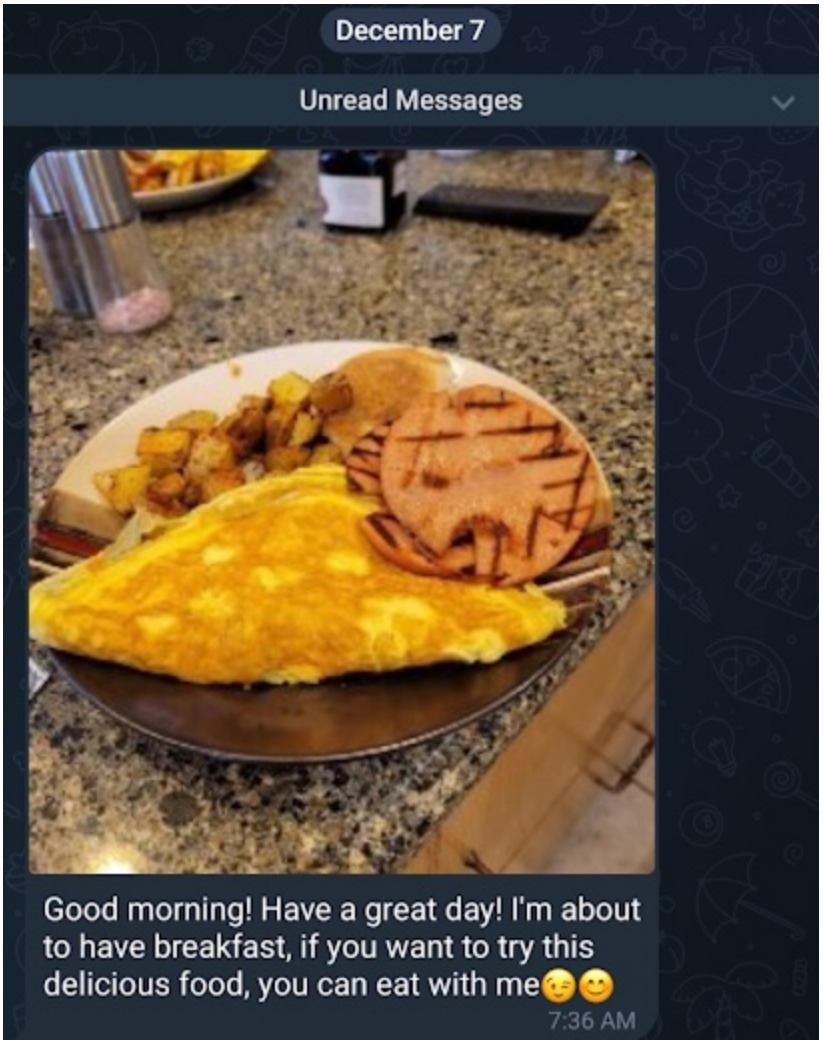


Figure 21. Maria sending me winking emojis and saying she wants to have breakfast together

She told me she really enjoys cooking and asked me what I like to do in my free time. I was not distracted by this, however— there was money to be made. Back to work.

Once I completed my first set of tasks, I needed to reset them before starting on the second set, which included depositing more money. Again, they sent me a different address, but fortunately, this time it actually had a transaction history. Time to get a little artistic. I significantly improved my Photoshop job this time around, made it look just like a recent transaction to the wallet and even included the transaction ID in the screenshot (Figure 22).

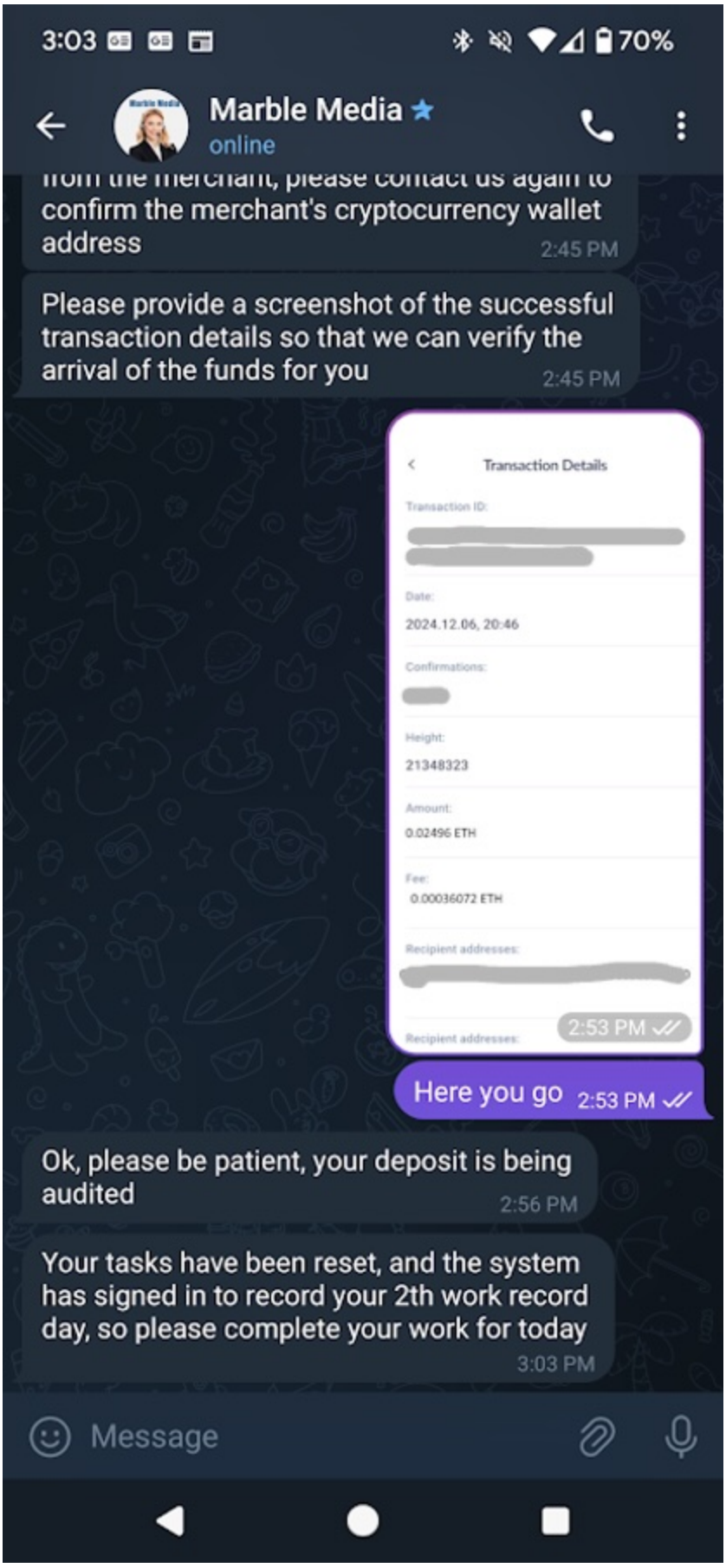


Figure 22. Customer Support Agent confirming my transaction and resetting my tasks

It worked on the first try! My tasks got reset and I could continue working for the day. This was important because I could only withdraw after completing both sets of tasks for a day.

I was nearly done with the second set when disaster struck: I hit another high-profit order. My account was in the hole again and I needed to make another deposit before I could finish my tasks for the day and be able to withdraw. I was down close to $342, which presented a couple of problems. First, it's significantly more money so I assume they may look at the transactions more closely. Second, there are not many transactions going to their wallets that are this large. The previous transactions were about $26 and $90.

I decided to wait and see if a larger transaction happened to hit one of these wallets. If so, I could swoop in with my usual trick and claim it to be mine. Until that happened, I was dead in the water.

In the meantime, I tried to stall with Maria and asked her about the VIP tiers for this job (Figure 23). For only $1,000, I can become a tier 2 VIP. Supposedly, it would increase how much I earned, but it would also increase the number of tasks per set from 40 to 50, so it actually seems like a costly downgrade to me.

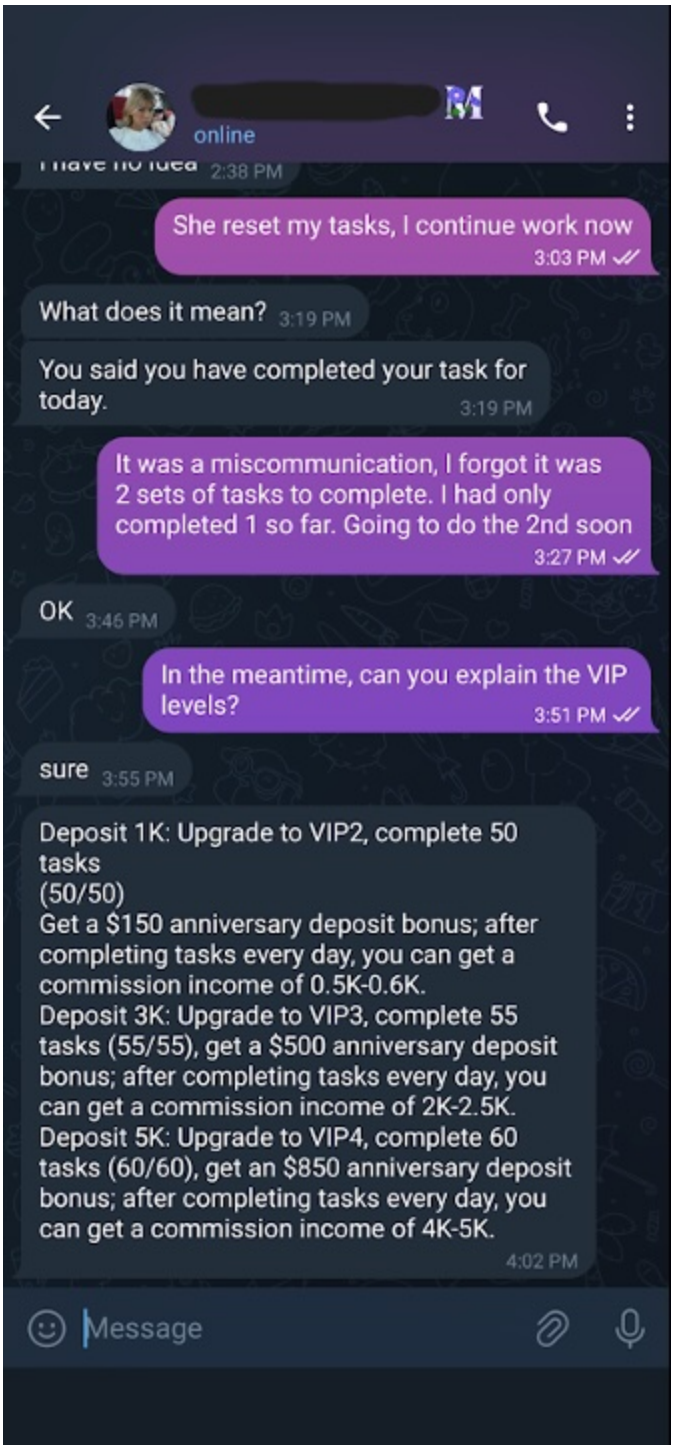


Figure 23. Maria explaining the VIP tiers

About an hour later I caught a big break: there was a large transaction to one of their wallets. It was even bigger than I had been hoping for—about $1,600. This would let me “go big.” For $1,600, I could both cover my negative balance and get the upgrade. I messaged Maria and told her I wanted to step up to the next VIP tier.

I photoshopped another transaction and sent it to Customer Support. She gave me some pushback, asking about the transaction ID (twice) even though I had already included it in the screenshot just like last time (Figure 24). It felt like something was going wrong, making me both frustrated and concerned that this may be the end of my experiment.

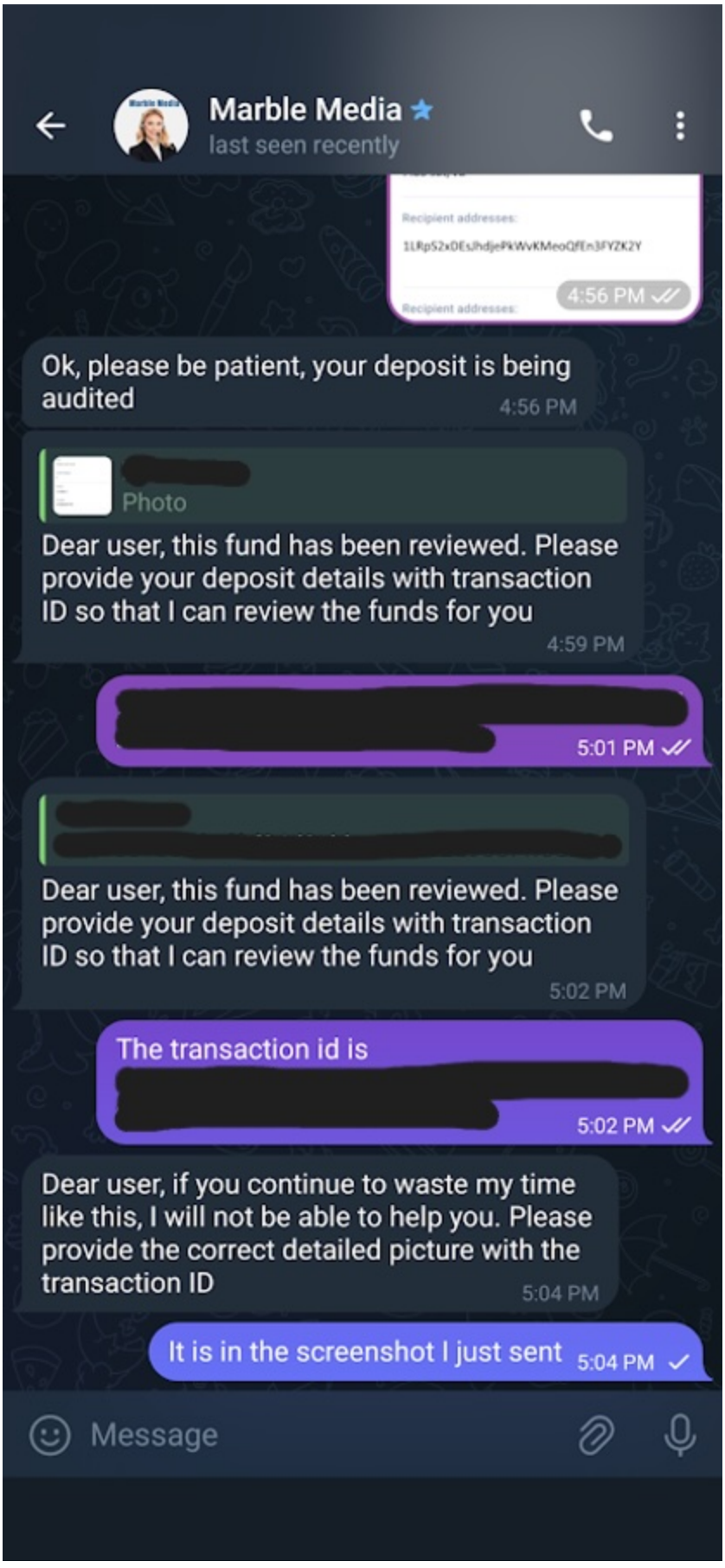


Figure 24. Customer Support has some problems with my transaction

My trick had worked the first time. It worked the second time. But it didn't work the third time. They said the money had been reviewed and deposited into another user's account half an hour ago (Figure 25). Darn, busted.

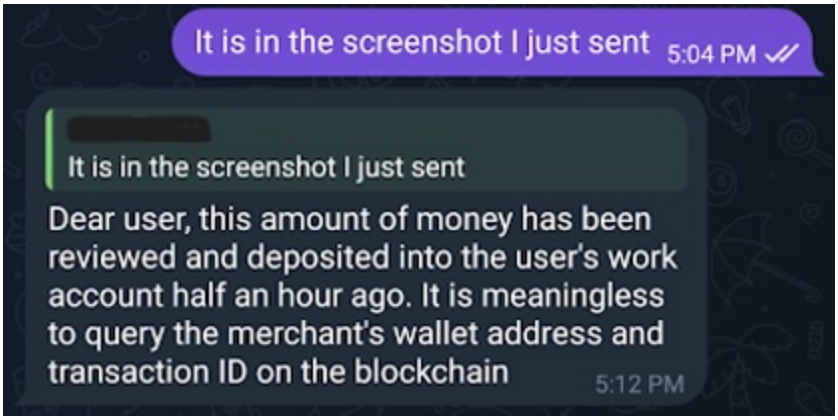


Figure 25. Customer Support figured out "my" transaction was not mine

They even had the audacity to say that it was "meaningless" to look up the transaction history of the wallet! Well, the joke's on them because it wasn't meaningless when I got $129.

Nevertheless, at this point I was grasping at straws, so I went for one last Hail Mary. I complained to Maria that the Customer Support Agent was not verifying my deposit and I claimed that someone else was carrying out my trick on me. I told her that I was the real person who made the transaction and an imposter was claiming it as their own (Figure 26).

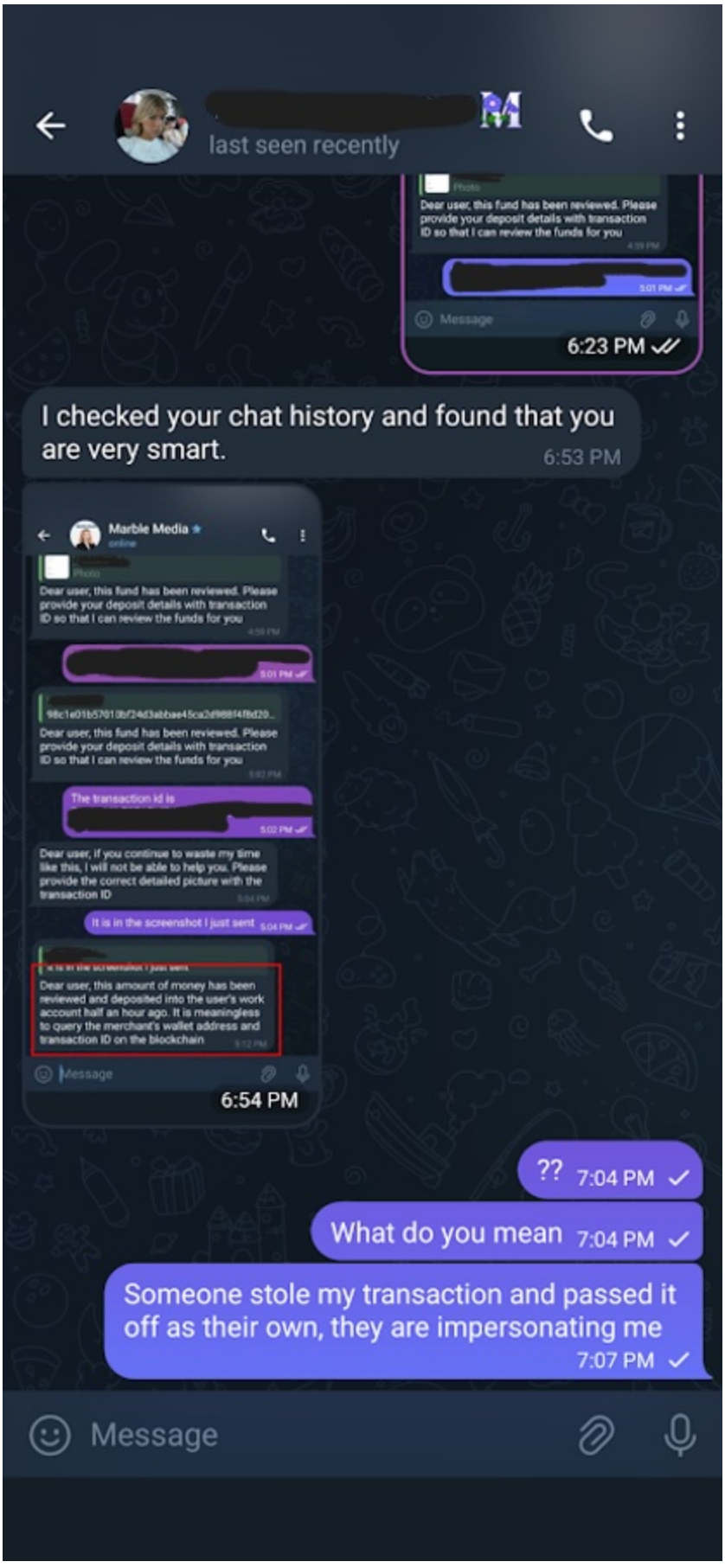


Figure 26. Telling Maria someone else claimed my transaction as their own

To my disappointment, Maria did not believe me and stopped replying.

By the next day, I had accepted that I wouldn't get any more money from this experiment, so I thought I'd throw out one last question on the off chance that I might at least get some information or insight. I thanked Maria for the Ethereum and asked her about the scam. Unfortunately, she seemed to take offense and began hurling insults at me in Chinese.

Shortly after, both Maria and the Customer Support team deleted our conversations. Arabella did not do the same to our brief conversation, but her account has been deleted.

On a more serious note, I did research the scam domain, marblemediaseo[.]cc, and found additional, related domains. marblemediaworks[.]cc is highly likely to be used by the same actor because it shares the same content on the website, similar hosting TTPs, such as the high-risk TLD ".cc," and both appear to be lookalike variations of "marblemedia." Additionally, I found dozens of other domains that seemed to be using the same "kit," as the contents on the sites were very similar. However, due to differences in the hosting and registration information, I suspect there are multiple actors, possibly affiliates using a template, operating the domains.

Crypto scams continue to be a lucrative method for bad actors to steal money. In 2024, consumers reportedly lost an estimated $9.3 billion from crypto scams.[2] This blog is part of an ongoing series of reports on our findings about groups operating scams worldwide. Stay tuned!

Indicators of Activity

A list of related indicators is available on our GitHub repo **here**.

Indicator	Description
marblemediaworks[.]cc	Domains controlled by featured scam actor
marblemediaseo[.]cc	
ukseo[.]click	Domains likely using the same kit/template
seoclick-works[.]click	
profiletree-seo[.]click	
dreamseo[.]cc	
dialektaseo[.]click	
seoclick-tasks[.]cc	
seoclick-works[.]cc	

Indicator	Description
creatorseoireland[.]cc	
creatorseo-apps[.]cc	
appradaseo[.]cc	
sdmgrowthseo[.]cc	
seoclick-tasks[.]click	
hawksearchseos[.]cc	

Footnotes

1. **https://www.theverge.com/2023/6/8/23754183/apollo-reddit-app-shutting-down-api**
2. **https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf**