Unsplash © Kevin Ku

What you need to know to stop fake trader fraud in Forex

It’s the great mystery of the social media age: This person makes that much money doing what?

A mental step back, maybe a cup of tea, and a few moments of collected thought will probably lead you to some obvious if annoying truths:

1. *That* one is extremely good-looking and is a 7-out-of-10 dancer.
2. *This* one knows how to change their personality so that it connects with small children.
3. The one over *there* is really good at a particular video game.

That’s all pretty reasonable in today’s influencer economy.

But there are still some inexplicable outliers. Why, at the bottom of your friend requests, are there so many people who apparently made their fortunes from *forex trading*? And why are they wearing the same aviator sunglasses, posed against the same expensive but tasteless cars, looking out over the same sunset vistas? And who carries around a briefcase full of cash, really?

Forex is a portmanteau derived from foreign exchange. As a financial vertical, foreign exchange investment is traditionally in the form of arbitrage opportunities. Sums of money are moved between different currencies to take advantage of small discrepancies in exchange rates, turning a profit.

Forex fraudsters, that’s who. And their lavish insta-lifestyles are as fake as the opportunities they offer.

What are Forex scams?

A typical example might look like this: a forex investor exchanges USD to euros, then euros to Hungarian forints, forints to RMB, then back into USD, perhaps ending up with a profit of 0.2% of their initial investment. With a 0.2% ROI, huge sums of money have to be wielded to make a worthwhile profit – 0.2% of one million dollars is $2000.

Forex fraud, thus, is any sort of malicious activity within the forex vertical. In a general sense, any activity where information was misrepresented, and that information led to a foreign exchange investment that never had a realistic chance of developing returns, could be considered forex fraud.

While there are undoubtedly enterprise-level scams within the forex exchange community, the most common example of forex fraud for most people will happen in their social media channels.

What do Forex scams look like?

Many forex scams du jour will generally be promoted by a network of “affiliate marketers”.

These accounts will be fine-tuned to capture the imaginations of the vulnerable, touting designer brands, imported cars, exotic vacations, and of course, inexplicable wads of cash. The lifestyle shown will be presented as something easily achievable or as an as-yet-undiscovered secret. With true marketing team savvy, the text will be optimised to be eye-catching, with exciting statistics and evocative emojis.

In August 2022, a BBC special recounted how unlicensed traders stole £3.8M from legitimate forex customers by manipulating them with false signals and not letting them access their funds.

At this point, many people might notice the strangely empty, movie-set-like quality of the posted photos. There may even be a small, instinctual voice that says, “something’s not quite right here”.

But maybe not.

If this at-a-glance marketing ploy is successful, a potential victim may start reading the content of the fraudulent forex trader. Their posts will promise huge returns on relatively small investments, taking advantage of newbie enthusiasm and pitfalls in *trading psychology.* They might be willing to share the secrets of their success, provided you join their investment group –

membership payable via BTC only.

From here, even without knowing that a significant return on a small investment is *impossible* in forex trading, all but the most impressionable will turn back. But the impressionable, the never-before-scammed, make up a significant number of people and a significant potential return for fraudsters.

After converting their fiat currency to Bitcoin and sending the initial investment, the victim will be invited to a group on a messenger app like WhatsApp. There, the fraudster will assure them that their money is available anytime – it's actually already gone – and their investment is reversible and covered by SEC/FCA mandate – it's not. In the group chat, each "investor's" money can be seen increasing in value, potentially leading them to invest even more, but attempts to withdraw it will be met with threats. Eventually, inevitably, the number will zero out, or nearly so.

A small consolation: their return would always be zero after the *Bitcoin* left the victim's account.

There will be no recourse for recouping the lost money. Cryptocurrency, in general, has no infrastructure to trigger an automatic reimbursement. Contacting the apparently wealthy original influencer will result in no solutions. After all, that influencer was always just an affiliate marketer posing for pictures in a lifestyle that an offshore investment bank paid for.

Forex fraud on the rise

Social media-based forex fraudsters have settled on a working formula for enticing new victims. Their Instagram pages are designed to make young peoples' get-rich-quick brains percolate.

For the most connected and tech-capable generations, it's much more likely to rub shoulders with a fraudster than in the unconnected world. In the same avenue that the internet and social media make the world smaller and closer together, they also connect the young and innocent with the cynical and malicious.

Many of us learn our most valuable lessons through the process of trial and error. We might waste five dollars getting upsold or get scammed out of twenty by trusting the wrong person. Relatively small mistakes, and ones that can inform your inner trust barometer when you find yourself being pursued by a forex "influencer."

However, getting duped by a forex fraudster running a glorified *Ponzi scheme* is a decidedly more expensive first lesson to learn. Educating on the potential

dangers and warning signs is a less expensive option, albeit less tearful and thus potentially less effective.

Tips for spotting Forex scams

Even if you have a skeptical brain from a lifetime of experience, shifting those experiences to social media can be challenging. What do the traditional, on-the-ground scams you're already familiar with look like when they're on Instagram? What's the forex fraud equivalent of three-card monte?

Sophisticated, efficient fraud prevention involves scrutinising a user's behaviour at various touchpoints, enriching what we can observe with additional data points to determine the likelihood they are malicious.

What does this look like on the side of platforms, exactly? There are ample examples based on the industry. For instance, in banking, digital onboarding can be challenging because challenger banks look for the most seamless, user-friendly experience, but they still cannot afford to become victims of fraud. So the idea is to gather data at this stage and evaluate it behind the scenes. This applies to forex, too. *Fraud detection automation* solutions can scrutinise customer touchpoints – digital onboarding, authentication, know-your-user protocols, deposits, and payouts – for signs of risk without introducing unnecessary amounts of friction.

A high score indicates a high risk of fraud. Similarly, here is a list of potential red flags that your brain should consider when someone approaches you on Instagram with a too-good-to-be-true deal (adjust your risk threshold accordingly):

> Unsolicited contact: Serious investment bankers don't "cold call" through Instagram. An unknown person reaching out to you offering a great opportunity is actually offering anything but.
>
> "Risk-free" or "No downturn" investments: No investment is risk-free, and every market has periods of downturn. Characterising an investment opportunity as either of these things is an obvious misrepresentation and should be treated carefully.
>
> Requests for personal information: Not exclusive to forex scams, anyone approaching you online asking for personal info should be kept at a distance.
>
> Dangling unrealistic returns: Wordings like guarantees of large returns on small investments or being just a few steps away from wealth if you *just* continue down this path should make you wary, as no such investment

opportunities actually exist.

Unconvincing clout: Forex scammers will try to convince you of their legitimacy and will often overshoot reasonability. The person with the lavish Instagram account will also be a VP, cite other big investors, or sit on a big secret they're willing to let you in on. People with real clout like this don't go about advertising it, particularly to strangers.

Suspicious velocity/currency: Scammers will want to "close deals" by impressing a sense of urgency on the "deal". There may be only hours or days to become an investor, pressuring you into making a fast (bad) decision. As well, payment via a method that you aren't familiar with is an easy way to keep you rattled and compliant. Be wary of people asking you to pay in BTC or through an app you're unfamiliar with.

Staying frosty and fraud-free

Though it's unadvisable to invest money through anything but a trusted broker, there are ways to keep yourself as secure as possible beyond a cagey disposition and good working knowledge of the fraud landscape.

Real-time data lookups give you a massive pool of information on any (legit) online persona. This way, personal data points provided by an apparently legitimate "forex trader" can be checked for validity. You will find out how risk-prone this person is based on their device, connection details, and overall digital footprint, or if they appear on any sanctioned lists like PEP or OFAC. If they have provided a fake name, you will see just how unrealistic the digital presence of Thick McRunfast is and why they should not be trusted.

And why should *forex platforms* care? Simply put, users reward good service, and punish those platforms that do not protect them. At the very least, a platform may incur chargeback requests and consumer complaints. So everyone benefits from the prevention of forex fraud. Everyone except fraudsters that is.

Though there is no definitive way to ward off the occasional bout of gullibility, having a solid checklist for suspicious behaviour is a good fallback plan when interacting online. Fraud-fighting technology provides a massive digital checklist, but the other half of the battle is ensuring you have your own.

PJ Rohall is the Head of Fraud Strategy & Education at *SEON Fraud Fighters.*

Article by PJ ROHALL