

Advertisements with celebrities spotted on social media? Beware of fraud

15/11/2024 Warning



The Financial Services and Markets Authority (FSMA) is once again drawing the public's attention to the dangers posed by fraudulent trading platforms. These platforms lure investors online with promises of quick and easy earnings. Their offers look attractive, but often they are nothing more than sophisticated scams that can lead to significant losses.

How does a fraudulent trading platform work? (flowchart)

1. Modes of contact

Fraudsters use various techniques to contact their targets.

A fake advertisement in which a celebrity is mentioned;

a website intended to “recruit” victims;

a fake account on social media or on a dating app;

a message that you have received allegedly by accident (SMS, WhatsApp, etc.).

2. Registration

Interested investors register on the platform and deposit funds to their trading account. Generally, investors begin with a relatively small sum, such as 250 euros. Sometimes the swindlers offer to help their victims by taking over their device remotely in order to make certain transfers on their behalf, which of course allows them to download viruses or spyware.

3. Manipulation and pressure tactics

Once the funds have been deposited by the victim, the platform manipulates the transactions to give the impression that significant profits have been achieved. However, these earnings are fictitious and the funds have not really been invested. The fraudsters then put pressure on their victims to invest more money. They do so by means of repeated phone calls, time-limited offers to which investors must respond quickly, or by issuing threats.

4. Withdrawals seem impossible

To gain victims' trust, fraudsters sometimes allow them once to withdraw a small amount. However, once an investor wishes to withdraw a larger amount, the fraudsters use various pretexts not to have to pay back any money (high costs, taxes, etc.). In the end, the fraudulent platform disappears completely, taking with it all the investors' money.

The FSMA has noted that the following websites were putting consumers in contact with fraudulent trading platforms:

- **BitGPT** (<https://bitgpt.app>, <https://bit-gpt.app>, <https://bit-gpt-app.com>);
- **Immediate2.0 ProAir** (<https://immediateproair.ai>, <https://immediateproair.co>, <https://immediate-proair.co>, <https://immediateproair.com>, <https://immediatetrade.pro>);
- **Neoprofit** (<https://neoprofit.org>, <https://neoprofitai.com>, <https://the-neoprofit-app.net>);
- **Oil 4.4 Evex / Gas XP Evex** (<https://oilevexai.com>).

The FSMA strongly advises against responding to offers made by the following trading platforms:

- **4AI** (<https://4ai.com>, <https://4ai.net>);
- **Aifactor** (<https://aifactor.ai>, <https://premiumaifactor.vip>);
- **Artosnomics** (<https://artosnomics.com>);
- **Axemarket** (<https://axemarket.com>);
- **Axe Trade Capital** (<https://axetradecapital.com>);
- **Axia Group (Clone)** (<https://axiagroup.io>, <https://axiagroup.co>);
- **Bacco Capital** (<https://baccocapital.pro>);
- **Boley** (<https://boley.im>);
- **Bull-Markets** (<https://bull-markets.com>);
- **Capital Group Fund** (<https://capitalgroup-funds.com>);
- **Commondigital** (<https://commondigital.eu>);
- **Dax40** (<https://dax40trade.online>, <https://user.dax40trade.ltd/login>, <https://wt.dax40trade.info>);
- **Finance Wise Global Securities Pty Ltd** (<https://wiseglobal.info>);
- **Fina-Nova** (<https://fina-nova.com>);
- **FORE XF** (<https://forexf.cc>, <https://bdsu-fx.com>);
- **Forex SX** (<https://forexsxpro.com>);
- **FusionLots** (<https://fusionlots.com>, <https://platform.fusionlots-techp.com>);
- **Geminix** (<https://geminix.app>, <https://geminix.trade>);

- **Global Prime Treasury PTE. LTD** (<https://globalprimetreasury.com>);
- **Inside the Fund** (<https://insidethefund.com>);
- **Investing Ideas** (<https://investingideas.world>);
- **InvestiRay** (<https://investi-ray.com>);
- **Kimonsage** (<https://kimonsage.io>) ;
- **Optimum Markets** (<https://optimum-markets.com>);
- **Premium Yields** (<https://premiumyields.com>, <https://premium-yields.com>, <https://premiumyields1.com>, <https://pytradingmarket.com>);
- **Quantumstar** (<https://quantumstar.net>);
- **Qwebank** (<https://qwebank.com>);
- **Rumblenomic** (<https://rumblenomic.co>, <https://rumblenomic.io/login>);
- **TheBiggestFuture** (<https://thebiggestfuture.com>);
- **TheMellonFX** (<http://themellonfx.com>);
- **Tradelly** (<https://tradelly.ai>);
- **TradeMasterCFD** (<https://trademastercfd.com>);
- **Traderoom24** (<https://traderoom24.com>, <https://app.traderoom24.com/login>);
- **Weinsteincorp** (<https://weinsteincorp.biz>, <https://weinsteincorp.com>);
- **WT Central** (<https://webtrader.wtcentral.org>, <https://wtcentral.com>).

I've fallen victim. What should I do?

- 1. Stop making any transactions and break off all contact with the platform:** don't deposit any more money and don't provide any additional personal or financial information. Break off all contact with the fraudsters. They may try to manipulate you in order to take even more money from you.
- 2. Contact your bank:** inform your bank immediately if you have made any payments to the fraudulent platform.
- 3. Report the fraud to the competent authorities:** Contact the FSMA and file a complaint with the police.
- 4. Document all exchanges of data and transactions:** gather all evidence of your exchanges of data with the platform, including emails, messages, account statements and screen shots of the transactions. These items will, of course, be very valuable when you report the fraud.
- 5. Beware of 'recovery rooms':** fraudsters contact victims of a previous scam and offer to help them - for a fee - recover their lost money. Often this constitutes yet another attempt at fraud.

For more recommendations on how to avoid investment fraud, please consult the 'How to recognize and avoid fraud' page on the FSMA website. Please watch our awareness-raising videos as well (available in Dutch and French only).