



FINANCIAL INTELLIGENCE AGENCY MEDIA ADVISORY

BEWARE OF VIRTUAL ASSETS AND ILLEGAL INVESTMENT SCAMS

The Financial Intelligence Agency (FIA) has observed a growing trend in cyber criminality in the form of virtual assets, in particular, bitcoins and illegal online investment schemes. These scams promise unsuspecting members of the public a quick financial return and normally rely on social media platforms for recruitment.

The FIA is issuing this advisory to enhance public awareness around these scams to avoid falling prey to the fraudsters. The advisory is based on FIA's analysis of financial disclosures filed by specified parties, information from open sources and law enforcement partners. The advisory contains the description of the scams and the associated red flag indicators.



FOREIGN EXCHANGE (FOREX) SCAMS

Fraudsters present a purported opportunity to invest in foreign exchange promising quick and high returns. Individuals are usually incentivised to recruit more people by receiving tiered commission. With this type of scam, the emphasis is placed less on trading but more on recruiting new members through deceptive, dishonest and fraudulent means. Our observation is that the Investors' funds are instead diverted and laundered to finance assets such as vehicles, real estate and to support lavish life styles of the Fraudsters while the Investors are left with huge financial losses.



CRYPTOCURRENCY RELATED SCAMS

Criminals are exploiting advances in technology to drive acts of criminality. With the increased online usage, cybercrime continues to rise in scale and complexity affecting businesses and individuals alike. The FIA has observed an increasing trend in financial crimes related to virtual currencies, particularly crypto currency scams. A crypto currency scam involves a promise to act as an agent and trade in crypto on behalf of the individual investors. Unsuspecting individuals are normally coerced into engaging purported agents as they are assured that investing through an agent enables the broker to pool more funds from people and make larger investments which result in much higher returns than what an individual investor can generate.

Of recent, we have observed a trend where criminals use social media platforms such as WhatsApp to create investment groups and lure a large number of people to the group. The group members would be provided account details to deposit initial capital and top-ups for investment. Electronic money wallets and deposit taking automated teller machines are also used to channel contributions for investment. Often, after collecting the deposits from a sizeable number of people, the Fraudsters would delete the WhatsApp group, stop communicating and block communication from all the WhatsApp group members. Proceeds from the scams are usually laundered to purchase cars, houses and other assets.

The public is therefore advised to exercise caution and to carry out due diligence before entrusting individuals or entities with their money. You have the responsibility to educate yourself, the more you know the less likely you are to be taken advantage of. Don't let a scammer enjoy your hard earned cash!

WHAT TO LOOKOUT FOR TO AVOID BEING SCAMMED

1. Avoid investing with individuals or entities which are not licensed and regulated.
2. Avoid investment schemes that are driven through social media platforms by strangers or through your social cycle (friends, family, and colleagues).
3. Watch out for promises of high returns on investment, normally within a short period.
4. The investment is normally portrayed to involve little or no risks.
5. High number of investors flocking for the same investment opportunity at the same time.
6. Social media is the modern platform of preference as it enables creation of fake identity and provides access to a wide net of potential victims. There is little or no monitoring of this platform.