

Deceptive Subsidiary Scam: Case Study of "valanitc.biz"







1. Introduction:

This case study explores the fraudulent activities of a fictitious company named "valantic.biz," which pretended to be a subsidiary of a renowned German multinational corporation, "Valantic GmbH." The study highlights the deceptive tactics employed by valantic.biz to scam innocent individuals and examines the repercussions of such unethical practices.

2. Background:

valantic.biz is a fraud services company that sought to exploit the reputation and trust associated with Valantic GmbH, a prominent multinational technology conglomerate. By impersonating a subsidiary, valantic.biz aimed to deceive potential customers, gain their trust, and ultimately defraud them of their money.

3. Deceptive Tactics:

- **a.** False Representation: valantic.biz created a sophisticated website and marketing materials that mimicked Valantic GmbH' branding and design elements. They strategically used similar logos, color schemes, and fonts to present themselves as a genuine subsidiary.
- **b. Phony Partnerships**: To further enhance their credibility, **valantic.biz** showcased fabricated endorsements and testimonials from these fictitious partners to create an illusion of legitimacy.
- c. Misleading Communication: The company's representatives engaged in deceptive communication practices. They would introduce themselves as employees of Valantic GmbH or downplay their affiliation with valantic.biz, deliberately obscuring the fact that they were not an official subsidiary.

4. Targeting Innocent Individuals:

valantic.biz specifically targeted individuals seeking return on their investment. They actively approached potential clients through messages on telegram and other means.

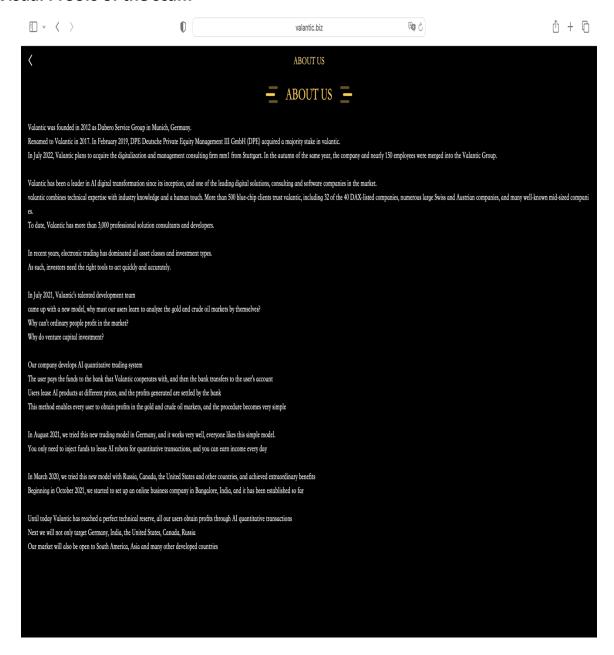
5. Uncovering the Scam:

- valantic.biz is luring people into the scam of fixed regular return on investment. In this scam
 people are required to transfer certain amount which is multiple of 500 INR (approximately 7
 USD) in order to get daily return on their investment.
- **valantic.biz** claims that they invest this money in artificial intelligence quantitive trading in order to give higher and regular return.
- The only mode of payment is through UPI id and this UPI id changes for every individual.
- It is suspected that these UPI ids belonged to dead people so that if you want to file complaint, there won't be any living person to fight with.



- This also seems to be a pyramid scam which again lures people to invite more people to trap in return of a promise to pay additional money.
- Already thousands of people have invested and became the victim of this scam.

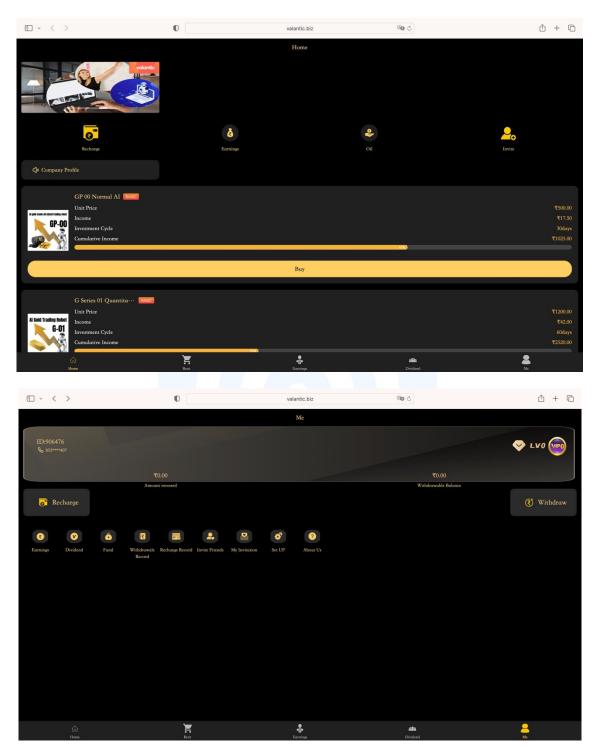
6. Visual Proofs of the scam



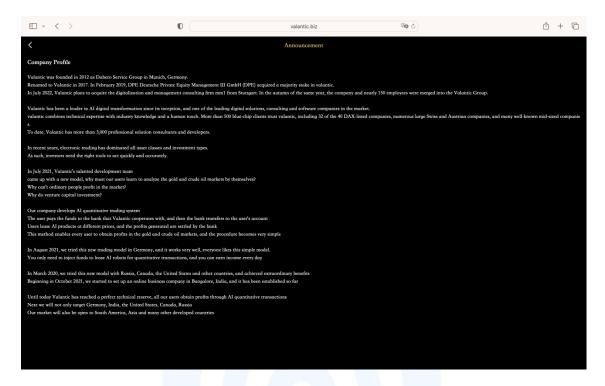


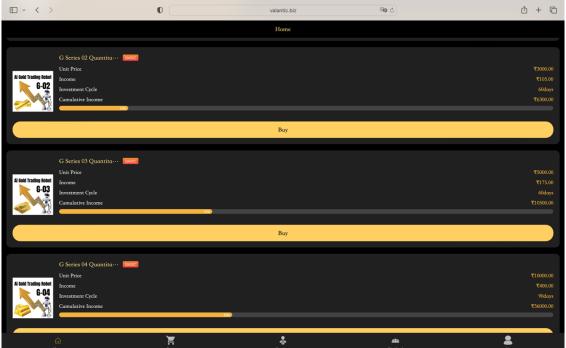


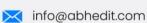






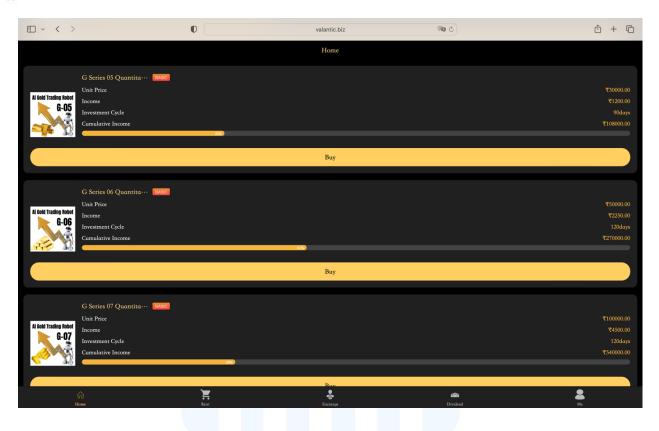








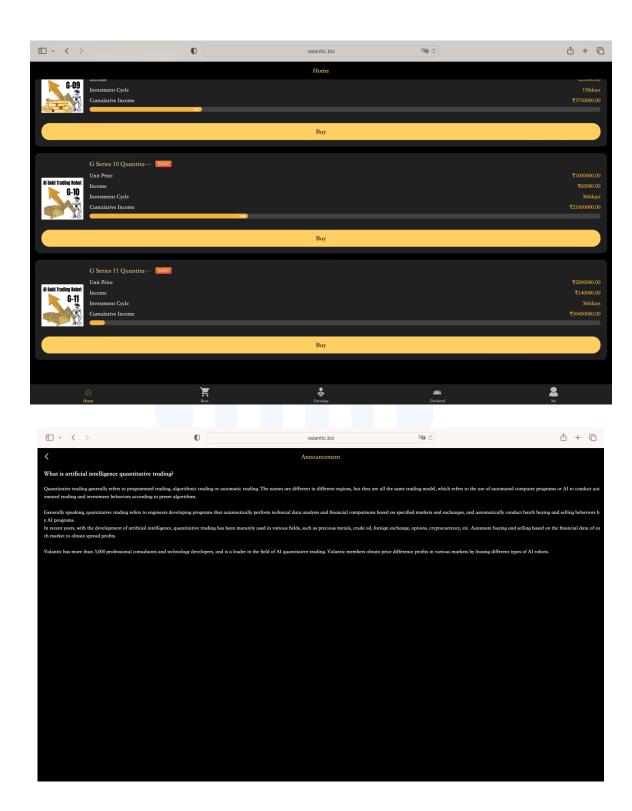




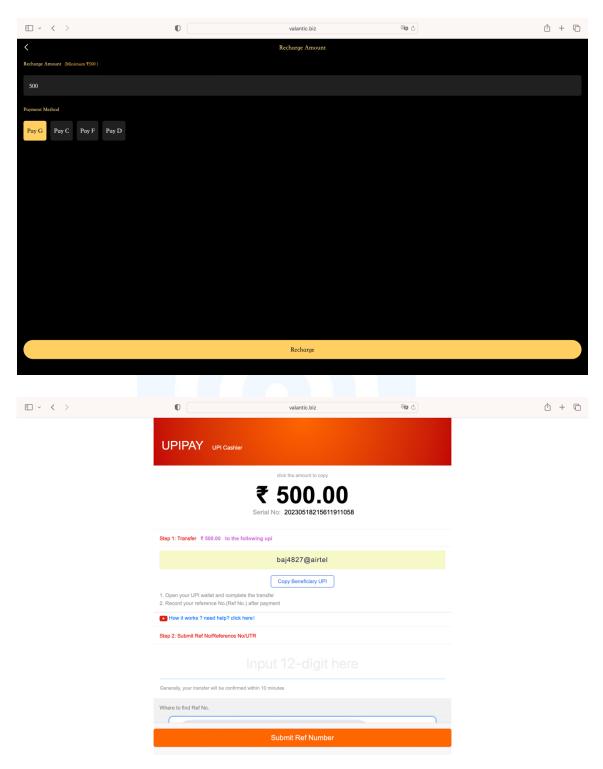




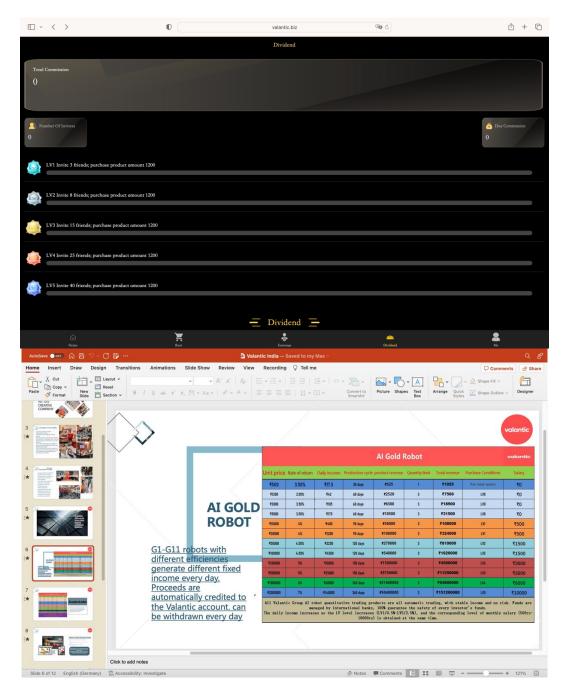




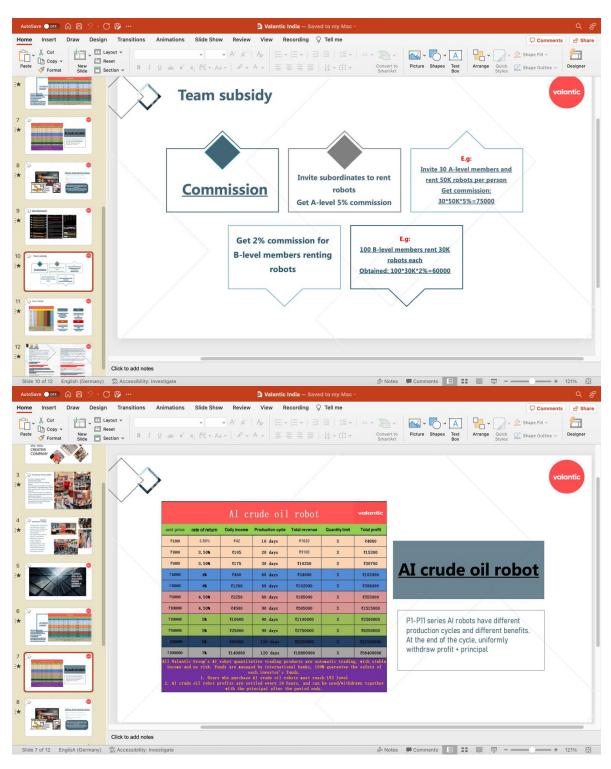




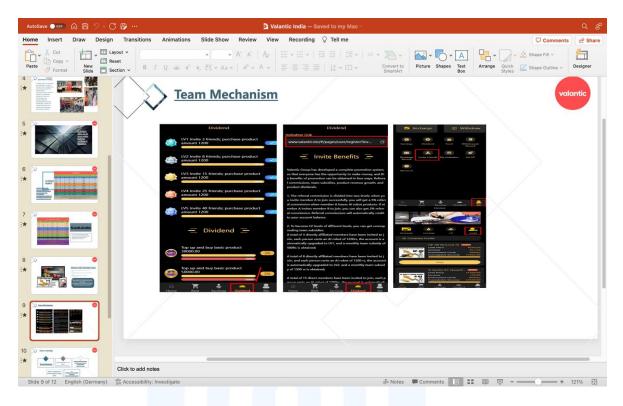












7. Lessons Learned and Prevention:

- **a. Strengthening Security Measures**: **Valantic GmbH** should implement stricter authentication processes and monitoring systems to prevent unauthorized use of their branding and protect customers from similar scams.
- **b.** Education and Awareness: The incident highlighted the importance of educating individuals about the risks associated with online transactions and the need to verify the authenticity of companies before engaging in business with them.

8. Conclusion:

The case study of **valantic.biz** demonstrates the dangers posed by fraudulent entities pretending to be subsidiaries of reputable companies. It emphasizes the need for vigilance, due diligence, and awareness to protect oneself from falling victim to such scams. Companies should take proactive measures to safeguard their reputation and support law enforcement in combating such fraudulent activities.



9. Important point to note

The exact same type of a scam happened in the year 2021 called "Powerbank Scam" where 11 people looted almost 150 crore INR (182 million USD) and faced legal consequences.

10. References

https://valantic.biz/#/

11. Other similar scams (Click at your own risk. These might be phishing sites)

https://mystarlink-plan.com/reg.html?v=A81HNG

https://www.hgn-gorup.com/#/?invite=72866543

https://m.shiningheat.com/#/pages/login/reset?inviteCode=8fc906c6

https://m.lendingkart-vip.com/signup.html?invitation_code=QH99Y

https://dualpower.in/

http://greenfd.online/login.html?code=2FVNVP

https://www.sunsma.com/#/pages/register/register?id=904811

https://t.me/A2fAMreal