Investment fraud

“Investment fraud” involves fraudulent investments. To this end, brazen financial service providers lure customers willing to invest with promises of high yields. Yet above all, those supposedly large profits hide high risks – and frequently even illegal machinations.

Please ensure you always observe the following rules of conduct:

- Take your time to decide where and whether to invest your money.
- Don’t let yourself get dazzled by any unrealistic promises. No reputable financial service provider would ever promise to achieve above-average returns in a short period of time.
- You should always research a provider, for instance on Google, Internet forums and consumer pages.
- Check whether the provider is FINMA-authorised (https://www.finma.ch/en/finma-public/authorised-institutions-individuals-and-products/) or appears in the FINMA alert list (https://www.finma.ch/en/finma-public/warning-list/) or the IOSCO Investor Alerts Portal (https://www.iosco.org/investor_protection/?subsection=investor_alerts_portal) . You should also check Swiss providers’ certificate of registration on www.zefix.ch (https://www.zefix.ch/en/search/entity/welcome) .
- Contact your main bank’s customer adviser if you are unsure.
- With foreign providers, you should always check who you can contact in case of problems.
- Next to their novelty value, innovative technologies and products (such as crypto-currencies) also harbour risks.

Generally, the following applies:

- Where there is a promise of apparently quick profits, remember that one simple truth: There is no quick money without any risk of loss! Those who believe this lose out!

This is how a typical attack works

Phase 1: Baiting

You can find “investment fraud” anywhere:

- In Internet ads, for instance on social media platforms
- In spam mail ads
- In magazine or newspaper ads for lucrative investments

Links inside such ads lead to specially prepared websites. In some cases, celebrities are used to advertise that they have already successfully tried this investment.

The aim is to induce victims to register. Fraudsters are particularly keen to get hold of telephone numbers.

Phase 2: First personal contact

Once victims have registered, they will then receive a call from a broker. Usually, these are met with scepticism.

Such scepticism is deliberately taken into account, and only a small investment sum of some 250 CHF or 500 CHF is negotiated over the phone. Usually, investments in crypto currencies are recommended. Customers are allowed to co-decide.

Once this small investment amount has been remitted, victims are given access to a fraudulent website's e-banking facility, where they will find their investment. Every time they log in, their yields have increased. Victims are convinced their decision to invest was the right one. Their money however has long since been lost.

Phase 3: Building trust

It looks like there is some kind of "personal" care relationship similar to that with a customer consultant. Victims are now contacted by purported brokers ever more often. Due to the yields achieved, customers then start to welcome such calls. These fraudsters have also mastered social engineering (https://www.ebas.ch/en/social-engineering/) techniques.

During calls, they will deliberately refrain from exerting any pressure. Victims are also left to make their own decisions. Pressure is created by offers purportedly only being available for a certain period of time, and options which expire soon. Payments meanwhile are kept in the dark until this point in time, i.e. they are not recognised as fraud by anyone.

It is frequently crypto currency dealers who serve as recipients and who have already opened accounts on behalf of the victims. In this, legitimisation/identification is provided by victims themselves, since fraudsters have requested this of them for passing on. The bit coin wallets associated to such cases however are outside victims' control. Physically, they belong to the fraudsters. A reversal is impossible.

Phase 4: Additional payment

In case victims would like the capital invested back for some reason, it slowly starts to dawn on them that they have fallen victim to a fraud. In some cases, an alleged investment crash is feigned. Victims begin to enter the grieving phase, something the fraudsters will then shamelessly exploit:

- **Denial**: Fraudsters start to mention the character of this investment, which requires victims to remit even more to get their money back. Since victims are unable to get their money back any other way, they feel they are the weaker negotiating partner.
- **Rage/anger**: Victims are transferred to a purported superior, or get called by them. This goes straight up to the purported provider's top boss, who always reassures victims, promising them a brighter future if they invest some more money.
- **Negotiating**: If none of this works, fraudsters will subsequently offer an insurance policy which victims could have already taken out at the start of the investment. To secure victims' investments, they are offered to have this added retroactively. This money, too, is lost.
- **Depression/grief**: Victims are helpless and see themselves as losers trapped in a dependency, having to rely on fraudsters' goodwill. Fraudsters are well aware of this winner's dominance and distance. Further calls and the fact that in victim's perception, nobody is helping them, result in the creation of a surreal sense of still being able to change something about the situation. Suddenly, money can still be transferred back after all. However, victims will have to pay bank, legal or notary charges in advance.

Phase 5: Realising their loss

Once they realise their loss, victims get in touch with their bank and the police. Solicitors are contacted...

Lessons to be learned

Any such investments of your money are usually risky. With the promise of high yields and complex subjects such as crypto currencies, you should exercise particular caution. Fraudsters are then usually never far away.

Should you still wish to invest your money, you should obtain extensive information beforehand and make sure you only do so from reputable platforms and providers.

Report dubious offers

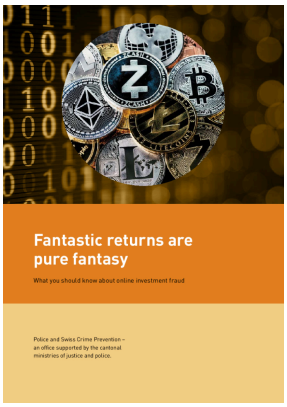
If you encounter dubious offers, you can notify FINMA via their reporting form (https://www.finma.ch/en/finma-public/reporting-information/) . Such reports enable FINMA to discover providers who are acting illegally and to take them out of circulation.

You can find further practical tips in the FINMA video "Protection against investment fraud (https://www.finma.ch/en/documentation/finma-videos/schutz-vor-anlagebetrug/) ".

"Investment fraud" scam tactics involve attacks serving to convince victims to participate in a fake investment. To this end, fraudsters promise to achieve an (unrealistically) high yield to induce their victims to remit money.

It is usually objects such as gold, real estate and crypto currency above all which are invested in. However, any money you part with always ends up straight in fraudsters' pockets.

Info sheet:



(https://www.ebas.ch/wp-content/uploads/2021/03/investmentfraudSKP_en.pdf)