The scale of investment scams in Europe

The threat to European small investors from online investment scams and international cybercrime organizations

Elfriede Sixt[1]

Abstract

The monthly damage currently caused to European small investors by fraud on online trading websites (hereafter also referred to as broker scams or investment scams) in Europe is estimated to be 1 billion[2] euros per month(!). This is only a rough estimate, since up to now - 10 years after the beginning of this type of crime - there has been no uniform collection of criminal complaints for this type of crime in the individual European countries.

This lack of uniform collection of data also hinders any central, efficient and effective prosecution of this type of crime within the individual European countries, not to mention a Europe-wide coordinated prosecution of these crimes.

This leaves European retail investors helplessly at the mercy of the global mafia-organised cybercriminals behind the hundreds of investment scams available on the Internet.

Fraudulent international criminal organisations, which have massive financial resources (12 billion euros* 10 years) at their disposal due to the long inactivity of the law enforcement authorities, are building up global organisational structures, deliberately exploiting the inability of the European law enforcement authorities to work across borders. These criminal organizational structures include online media houses, legal and illegal financial services companies, a booming boiler room industry and trading technology providers, as well as service providers such as lawyers and tax consultants who administer the countless shell companies involved. New Investment scams with new domains, supporting payment service providers and the appropriate boiler room support can be put onto the Web, by means of so-called white label solutions, in under 24 hours.

The suffering and crime that is happening daily in Europe, obviously unnoticed by the media and the public, is gigantic.

The unscrupulousness of the operators of these systems is indescribable and the given hubris of the criminals is the result of being able to carry out their criminal activities unchallenged, especially in Western Europe, for years now.

However, the scale of the crime may increase as we observe that criminal organisations are increasingly moving towards using crypto currencies for this type of crime, thereby increasing the difficulty for law enforcement agencies.

---

[1] CPA in Vienna, Austria, Co-Founder of the EFRI-Initiative

[2] This estimate is based on an average small investor deposit of € 1.700 and an average customer base of 9.500 per broker system.

Appeal: European countries must immediately put increased efforts into the active, efficient and effective (at least Europe-wide coordinated) prosecution of this type of crime, otherwise any further digitisation effort of the European countries will be absurd.

Borderless cybercrime

The increasing digitalisation of society and the economy in general and the associated virtualisation of money bring a new, massive threat - cybercrime. The combination of state-of-the-art technologies with new marketing methods and a massive gap in the technological affinity of some Internet users create an unprecedented ecosphere for criminals. Traditional crimes such as bank robbery or car theft prove to be far less lucrative than cybercriminal activities.

Cybercrime knows no national borders. By means of sophisticated social media web campaigns, billions of people can be reached in the simplest way.

The costs of the damage from the various online fraud systems reach immense amounts. According to the UK National Crime Agency, cybercrime already accounted for more than 50% of all reported crimes in the UK in 2018[3]. According to the UK Financial Conduct Authority (FCA), investment scams alone caused GBP 197 million in damage in the UK in 2018[4].

The *Measuring the Changing Cost of Cybercrime study* conducted in 2019 by several European universities also provides evidence of the above facts[5]:

The study estimates that by 2019 6% of the European population had already become victims of cybercrime.

Statistically, people in Europe are now more likely to become victims of cybercrime than of traditional crime.

It should be noted, however, that the data on which the evaluation of figures is based in the area of cybercrime is currently still thin. Cybercrime is still a relatively new phenomenon for both statistics and authorities.

Findings of the EFRI initiative

The European Fund Recovery Initiative, based in Vienna, started in January 2019 to conduct online campaigns to recover investor funds from various investment scams in the area of online trading.

Since January 2019, more than 1.300 injured parties have registered on the website www.efri.io with a total loss of more than 23 million euros. Ninety-nine percent of the injured parties are European small investors aged between 50 and 85.

[3] Office for National Statistics, Crime in England and Wales: year ending March 2019, Link https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2019

[4] FCA warns the public of investment scams as over £197 million reported losses in 2018, Link https://www.fca.org.uk/news/press-releases/fca-warns-public-investment-scams-over-197-million-reported-losses-2018

[5] https://www.paccsresearch.org.uk/wp-content/uploads/2019/06/WEIS_2019_paper_25.pdf

After reviewing the facts, descriptions and documents submitted by the injured parties, it becomes obvious that the mere registration with an investment scam is usually enough to start a fatal cycle for a European retail investor.

Social media channels serve as the main advertising channel

Small investors are lured by seductive adverts on social media - especially Facebook and YouTube - that inspire trust and promise quick profits.

Boiler rooms/call centres as a critical success factor

After registration on the online trading platforms, the boiler room employees of the fraud systems will contact you immediately.

Call centres are called boiler rooms. Their employees receive massive commissions from each successful deposit from the small investors, they then systematically encourage the small investors to transfer larger and larger amounts using professional psychological methods.

In Bulgaria, Serbia and Bosnia-Herzegovina huge call centres have emerged in recent years with employees who have a wide range of language skills. These call canters work with state-of-the-art technologies, databases and customer relationship management (CRM) systems.

Psychologists train the boiler room agents; professional writers develop the interview guidelines and experts create sophisticated customer profiles. Customer data is obtained from a wide variety of sources; customers are selected and processed as required.

Sophisticated technology as the basis of fraud

The unsuspecting small investors are misled by the most modern trading technology and professionalism and convinced that their transacted investments will obtain high profits and the investments are at their disposal.

In this time of happiness, boiler room agents build a deceptive relationship of trust with the retail investor. This relationship of trust is ultimately used to deprive the retail investor of all their assets and leave them financially and psychologically exploited.

Legal and illegal European payment service providers act as an enabler for the fraud

Due to the pure online characteristic of the investment scam business, well-structured payment service providers accepting, authenticating and facilitating electronic payments on behalf of merchants are critical. Payment service providers (PSPs) or payment processors use software as a service model and form a single payment gateway for their clients (merchants) with multiple payment methods.
Only by careful structuring of the payment channels, facilitating the flow of the money from the victims to the final beneficiaries, a successful investment scam business is established.
So parallel to the evolution of the investment scams their payment service providers have also evolved during the past ten years, concentrating on developing, establishing and integrating omnichannel payment platforms.
The broadly defined segment of payment service providers (PSPs), also called FinTech, must in principle be differentiated between the following:

- registered (licensed) PSPs
- and unregistered PSPs.

Registered PSPs have received permission for their activities from a financial market supervisory authority and have developed payment technologies ("payment platforms") in order to efficiently process payments across different payment channels and providers online.
Sspecifically, cash transfers to the investment scams are facilitated through:

- bank wires
- credit and debit card payments or
- increasingly via crypto-currencies and crypto payment service providers.

For cultural reasons Western European retail investors (A, CH, DE) prefer to transfer material amounts (exceeding € 1.000) by real-time bank transfers.
For bank-based payments such as direct debits, bank transfers, and real-time bank transfers, the involvement of European financial institutions is indispensable because unsuspecting European small investors trust in the legal certainty of the European financial market and this trust results in the fact that large amounts are transferred without hesitation.
To facilitate real-time bank transfers PSPs structure the money flow as follows:

- Either accounts with licensed European Fintech companies for the receipt and forwarding of customer funds are set up with European banks. Examples are Altair Entertainment Ltd, Curacao (WireCard) or UPC Consulting Ltd at Kobenhavn Andelsklasse. From these accounts, the funds are subsequently transferred directly to offshore accounts of the beneficiaries of the fraud systems.
- Or the PSPs make use of the services of illegal payment service providers: therefore shell companies are systematically set up in Western Europe opening accounts with well-known European banks. These accounts are very often orchestrated centrally and are used to systematically facilitate the flow of funds to offshore accounts of the perpetrators.

In both cases, the agreed commission payment (calculated from the amount of money transferred) for the PSPs are deducted before the transfer to the offshore accounts.
Shell companies (from all over the world) with German bank accounts are traded as "premium accounts" and are provided with a high commission for the service.

Total loss as a result

As soon as the small investors want their investment to be paid out, together with the earned profits, the customer relationship immediately deteriorates and within a short time the simulated profits translate into a total loss of the investment. The incorrect procedure is acknowledged with threats, the closure of the account and the inaccessibility of the client advisor.

In ninety-nine percent % of all cases, registration with the fraudulent systems results in a total loss of savings for these small investors. In the worst case even with an additional financial burden, as many victims are encouraged to take out a loan through false promises and assurances.

If it is obvious that nothing more can be “earned” from a specific retail investor, the customer data is sold to other operators of online trading platforms or to so-called fund recovery organisations. This is the beginning of a new journey of harassment by email and telephone for the injured parties. Countless spam emails and callers from all over the world continue to harass the victims for months.

These recovery organizations are often run by the same fraudsters as the trading platforms, now consciously trying to exploit the distress and desperation of those cheated. It is promised against the down payment of further money to retrieve the money lost in the fraud system. This money is also lost as a result.

The path of suffering continues

The drama of the twice-cheated small investors, however, is not over yet, because after the depressing and disturbing realization that they may have been cheated twice, a new tale of suffering begins for them: the trip to the financial institutions involved, supervisory authorities and law enforcement agencies with the request for assistance.

Rejection of financial institutions

The countless chargeback requests from desperate investors at credit card companies and banking institutions from such transactions are decisively rejected, mostly with reference to personal responsibility for investments in online gambling systems.

Requests for information about the online payment service providers involved, with reference to the fraud committed, are also rejected 99.9% of the time, with reference to the confidentiality obligations for the acquiring organisations.

Rejection by financial market supervisory authorities

For years, financial market regulators in Europe have received complaints from injured retail investors. These complaints from retail investors are either not responded to at all or are answered with meaningless and dismissive mass e-mails.

No prosecution by the law enforcement authorities

The reporting of fraud to law enforcement is also frustrating for the victims: the lack of understanding of the nature of this cybercrime results in most of the of criminal cases

- not being accepted at all,
- being rejected within a few weeks - for example, due to the involvement of foreign relations (!)
- being dismissed as "conscious gambling".

Most of the aggrieved parties said that even when the criminal complaint was accepted by the prosecution authorities, the enforcement agency told them upfront that there was virtually no chance that the fraudsters could be caught, and the stolen money recovered.