The Scale of #BrokerScams in Europe

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

A Status Report in Progress
Will be updated permanently

Editor:
Elfriede Sixt[1]
EFRI Co-Founder & Principal
Website: *www.efri.io*
Email: e.sixt@efri.io

1 Abstract

The monthly damage currently caused to European small investors by fraud on online trading websites (hereinafter also referred to as #BrokerScams or #InvestmentScams) in Europe is estimated at 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 recording of criminal charges for this type of crime in the individual European countries.

This lack of uniform recording subsequently prevents 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 helpless at the mercy of the global mafia-organised cybercriminals behind the thousands of #BrokerScams available on the Internet.

Fraudulent international criminal organisations, which have massive financial resources (12 billion USD * 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 media houses (see Crypto Daily (owned by Uwe Lenhoff)), 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 #Broker Scams with new domains, an offer at most diverse payment service providers and the appropriate

[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. Currently we estimate that 550 fraudulent websites (one website is considered #BrokerScam) are out there. The figures are based on the confiscated client lists of BrokerScams xTraderfx (25.000 clients; average deposit of € 1.700) and safemarkets (4.100 clients; average deposit of € 1.400), goldenmarkets and getfinancial (for more details please contact us). (our best guess)

boiler room support can be put by means of so-called white label solutions within 24 hours into the Web.

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 since they have been 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.

Appeal: The 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.

2 Cross-Border Cybercrime

The increasing digitalisation of society and economy in general and the associated virtualisation of money bring with 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 damage sums reach immense amounts with the various online fraud systems. 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.

[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 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

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

3 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 #CyberScams in the area of online trading (i.e. investment scams or #BrokerScams).

Since January 2019, more than 1,108 injured parties have registered on the website www.efri.io with a total loss of more than 20 million euros. 99% of the injured parties are European small investors aged between 50 and 85.

After reviewing the facts, descriptions and documents submitted by the injured parties, it becomes obvious that the mere registration with a #BrokerScam is usually enough to start a fatal cycle for the retail investor:

3.1 Social media channels serve as main advertising channel

Small investors are attracted by trust inspiring and attractive advertising measures on the social media - especially Facebook and YouTube - with the promise of quick profits.

3.2 Boiler rooms/call centers as critical success factor

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

Call centers are called boiler rooms. Their employees receive massive success commissions from each successful deposit of 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 centers have emerged in recent years with employees who have a wide range of language skills. These call centers 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 segmented and processed as required.

3.3 Sophisticated technology as the basis of fraud

The innocent small investors are pretended by means of misleading most modern trading technology professionalism and mediated that their transacted investments 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.

3.4 Legal and illegal European payment service providers another critical success factor

The payments of the retail investors into the #BrokerScams take place

- via bank transfers (offline cash transfers)
- by means of credit card payments (online cash transfers) or
- increasingly via crypto currencies and crypto payment service providers

For bank transfers, the involvement of European financial institutions is indispensable, because 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.

For bank transfer, two alternatives are used

- the #BrokerScams operators open accounts with licensed Fintech companies for the receipt and forwarding of customer funds. Examples are Altair Entertainment Ltd, Curacao (WireCard). From these accounts, the funds are subsequently transferred directly to offshore accounts of the beneficial owners of the fraud systems.
- Or they make use of the services of intermediaries of illegal payment service providers: in the process, shell companies are systematically set up in Western Europe that have accounts with well-known European banks. These accounts are used to receive investor funds, which are then transferred to the offshore accounts of the beneficial owners of the fraud systems after deduction of a commission payment for the payment service providers. These shell companies usually offer this service to several fraud systems.

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.

3.5 Total loss as a result

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

Registration with the fraud systems results in 99% of all cases 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" can be obtained from the retail investor, the customer data is sold to other operators of online trading platforms or to so-called funds recovery organisations. This is the beginning of another month of harassment of the injured parties by email and telephone. 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 they consciously try to exploit the distress and desperation of the cheated again. 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.

3.6 The path of suffering goes again

The drama of the 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 involved financial institutions, supervisory authorities and law enforcement agencies with the request for assistance.

3.7 Rejection of financial institutions

The countless charge back requests from desperate investors at credit card companies and banking institutions from such transactions are determined and 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 rejected 99.9% of the time, with reference to the confidentiality obligations for the acquiring organisations.

3.8 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 rejecting mass e-mails.

3.9 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 99% of criminal cases being reported by regional police authorities in European countries

- not be accepted at all,
- to be directly rejected- for example, due to involved foreign relations (!)
- are be dismissed as "conscious gambling".

90% of the aggrieved parties said that even when the criminal complaint was filed with the prosecution authorities, the enforcement agency told them upfront that there was virtually no chance that the fraudsters could be caught, and that the stolen money could be recovered.

4 Problem-solving approach!

We have identified the following solutions which must be taken as soon as possible by the European governments in order to put a stop to this type of crime:

- The European countries must immediately begin to put increased efforts into the active, efficient and effective (at least Europe-wide coordinated) prosecution of this type of crime.
- Social channels such as Facebook and YouTube must be requested to stop the fraudulent advertising of #BrokerScams - Europe-wide. If necessary, in court.
- EU countries that either allow the #BrokerScams to operate on their territory (especially Bulgaria, Estonia) as well as those countries whose financial market supervisory authorities allow "facilitated" access to "pseudo" licenses (Cyprus, Malta, etc, Estonia and Lithuania) must be stopped.
- The EU accession candidates Serbia, Montenegro (currently home to countless #BrokerScams call centres) are threatened with an immediate halt to accession talks if the hundreds of call centres are not closed down immediately.
- The European legal and illegal payment service providers (fiat and crypto) must be made incomprehensibly clear that any complicity in such criminal activities is classified as contributing to a criminal organisation and is threatened with massive punishments and immediate withdrawal of any granted banking licence.

- a European central law enforcement unit should be set up without delay, specialising in these crimes and seeking international cooperation.
- A media campaign should be launched at European level to draw the attention of retail investors to this type of crime.