2024

Activity report

the

European Funds Recovery Initiative

www.efri.io

Contents

1 FOREWORD

In an increasingly digitalised world, where digital transactions and communication have become the norm, "**trust**" in secure and functioning settlement processes is essential. However, this trust of consumers and retail investors in effective supervisory and law enforcement measures against companies and individuals who violate applicable law is being massively undermined in Europe.

Law enforcement agencies are understaffed and under-resourced, so cybercriminals often go unpunished. At the same time, numerous European regulated financial companies and IT service providers (including social media) enable online fraud against thousands of small investors with impunity and high rewards.

Whether due to ignorance about the role of fintechs in fraud schemes or unconscious ignorance on the part of the financial supervisory authorities, the inadequate enforcement of regulatory provisions has serious consequences.

Since the founding of our initiative, our focus has therefore been on the fight against those (often regulated) European financial services companies that enable cyber criminals to carry out their activities and deliberately or grossly negligently ignore fraud signals, as well as against the inaction of European financial supervisory authorities.

EFRI's successes prove that public pressure can bring about change: The business activities of Payvision BV, Deutsche Handelsbank and Kobenhavn Andelskasse have now been discontinued and criminal proceedings have been conducted - probably also due to our sustained exposure of their deep involvement in cybercrime since the beginning of our activities.

In the area of recovering stolen funds, 2024 was a decisive year for EFRI: for the first time, we succeeded in securing settlement payments for victims of BARAK and LENHOFF (fraud platforms: xtraderfx, safemarkets, optionstars(global), zoomtrader(global), xmarkets, tradovest, tradeinvest90, option888). The Dutch, now former financial services company Payvision BV, a subsidiary of ING Bank NV, paid out compensation to over 140 defrauded victims from various European countries, represented and supported by our organisation, who received a large part of their lost money back. This helped to alleviate massive suffering.

This case impressively demonstrates how essential EFRI's work is - and how efficiently we operate as an independent transnational organisation. Our commitment goes mere information: we focus on legal enforcement, systematic research and the mobilisation of those affected.

This annual report provides a detailed insight into our activities since the founding of our organisation, successes and challenges. Our goal remains

unchanged: a financial world in which small investors are protected and fraudsters are consistently held accountable.

In the future, we will continue to step up our efforts to support even more victims and denounce regulatory abuses. Our fight is far from over.

We would like to thank all supporters, whistleblowers and those affected who are standing up for justice together with us.

European Funds Recovery Initiative (EFRI)

2 WHY EFRI

Digitalisation has enriched our lives in many ways - but it also has a dark side: **cybercrime.** The number of cases of fraud on the internet has increased dramatically in recent years.

Cyber criminals operate internationally, using state-of-the-art technologies such as artificial intelligence, cryptocurrencies and automated e-money transfers to cover their tracks. The consequences are dramatic: **worldwide, the estimated annual cost of cyberattacks is up to six trillion US dollars[1].** In Germany alone, the economic damage in 2020/2021 amounted to **223 billion euros** - a doubling compared to 2018/2019[2]. However, the official figures only show a fraction of the problem, as many of those affected (whether companies or private individuals) do not report their losses to the law enforcement authorities.

2.1 Private individuals: The forgotten victims of cybercrime

It is a sad fact that private individuals and small businesses in particular defencelessly exposed to the growing threat of online fraudsters. Fraudsters lure people in with false investment offers, steal identities or empty bank accounts with phishing attacks. **For 2022, the direct costs of cybercrime for private individuals in Germany were estimated to be at least 3.1 to 3.7 billion euros[3].** However, the number of unreported cases is likely to be far higher.

But the financial loss is only part of the problem. **Many victims suffer long-term psychological stress.** The feeling of powerlessness, fear, shame and anger often leaves deep scars. Studies also show that cybercrime increases the risk of poverty in old age, as many victims lose a significant proportion of their savings. The risk of cancer, dementia, etc. increases massively within the affected population group due to the trauma suffered.

2.2 Law enforcement: Overstretched, ineffective and forgetful of victims

While cyber criminals operate via international networks, **victims face bureaucratic hurdles and a lack of support when it comes to prosecution.** Reports often have to be made in person or even by post, while fraudsters large sums of money out of the country in seconds via crypto transfers. Even if perpetrators are identified

[1] https://www.expressvpn.com/de/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/
[2] https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Billion-euro loss per year
[3] News from criminological research; research report and costs and damage caused by cybercrime in Germany; Unit IZ 36 - Cybercrime Research Christine Weber; file:///C:/Users/esixt/Downloads/2024KKAktuell_Kosten_Schaeden_Cyberkriminalitaet.pdf

If the offences are committed, prosecution and convictions are very rare.

The situation is even more dramatic when it comes to **recovering stolen funds.** While there are organisations in the USA that publicly denounce financial services companies after misconduct has been identified and call for funds to be returned to thousands of victims (such as the US Consumer Financial Protection Bureau), there is a lack of comparable organisations in Europe. Bank transfers disappear into an opaque web of offshore accounts and crypto wallets, while victims are left empty-handed. European law enforcement agencies are currently doing little to address this issue.

2.3 Cross-border cooperation: a major obstacle

Cybercrime is a global problem, but prosecution in Europe too often fails at national borders. Criminals operate from countries with weak law enforcement, using offshore servers and encrypted communication channels to evade prosecution.

European authorities often work together ineffectively due to a lack of standardised legal frameworks and fast procedures for exchanging information. **Requests for mutual legal assistance take months or years - while cyber criminals can abscond abroad with stolen funds in minutes.**

Even when perpetrators are identified, arrests or extraditions rarely materialise as many countries do not have a clear legal basis for combating international online fraud. While criminal networks adapt flexibly and utilise the latest technologies, European law enforcement agencies struggle with outdated structures and a lack of resources.

2.4 The role of financial crime enablers

Financial crime enablers (FCEs) are actors that facilitate financial crimes either deliberately or through negligence. They play a critical role in the execution and concealment of illegal activities by providing infrastructure, services or legal protections that help fraudsters carry out their schemes and evade prosecution. The term financial crime enablers also includes banks, payment service providers, fintech companies and crypto exchanges that make it easier for cybercriminals to launder funds and feed them into the regular financial circuit.

Financial crime enablers provide criminals with access to payment systems and help to channel and conceal illegal funds.

The problem is exacerbated by the fact that many of these institutions hide behind legal constructs and deny their responsibility. While law enforcement authorities are often understaffed and technically under-resourced, FCEs use regulatory loopholes or operate across borders to evade scrutiny. This makes it increasingly difficult for victims of financial fraud to recover stolen funds as they are disguised through an extensive network of payment service providers, offshore accounts and cryptocurrencies.

Ultimately, FCEs are an indispensable part of modern financial crime. Without their services, it would not be possible for fraudsters to move illicit funds and evade prosecution. It is therefore crucial to pursue not only the direct perpetrators, but also those who provide the infrastructure for financial crime in the background

2.5 EFRI: In favour of victims' rights and the recovery of stolen funds

EFRI is committed helping victims of cybercrime. Our aim is to give a voice to private individuals who have been defrauded by cyber criminals and to support them in their fight for justice.

EFRI's demands include

- **Better rights for victims** and transparent procedures so that those affected are actively involved in criminal proceedings.
- **More efficient law enforcement** with technical and personnel upgrades for the investigating authorities.
- **Faster international cooperation** to combat cyber fraud.
- **A European programme to recover stolen funds**.

Cyber criminals must not go unpunished. Together, we can ensure that internet fraud no longer goes unpunished and that the recovery of stolen funds is finally given the priority it deserves by the judicial authorities.

3 OUR MISSION

The EFRI European Funds Recovery Initiative (EFRI European Funds Recovery Initiative) supports European consumers and retail investors who fallen victim to cybercrime.

Our initiative focuses on victims of online fraud, especially those who victimised by fraudulent investment offers on digital platforms. This form of fraud is also as "investment scams", a subset of pig butchering scams.

Any such fraud damages the victims and their families financially, emotionally and psychologically.

EFRI's mission is to be a helping partner to these victims!

4 Why pig butchering scams?

Pig butchering scams (investment scams) are particularly dangerous for small investors for several reasons:

Aggressive advertising on social media channels
Fraudsters advertise their supposed financial offers intensively on platforms such as TikTok and Instagram or in messenger services such as WhatsApp. However, these are to be dangerous traps.

Building an emotional relationship
After the initial deposit of a small amount (usually between €250 and €350) (usually by credit card payment), the fraudsters build up a trusting and supposedly financially profitable relationship with the victim over a period of weeks or months. Professionally trained call centre employees use sophisticated psychological tactics to gain trust and manipulate the victims.

Fake investment platforms
The fraudsters professionally designed but fake investment platforms that initially show small returns. This is designed to give the appearance of a legitimate investment and deceive inexperienced investors.

High financial losses
The average losses due to such scams are considerable. According to an Austrian study, the average loss rose from around 900 euros in 2021 to around 5,400 euros in 2024 - an increase of 600%. According to the Bavarian Cybercrime Centre, the average loss per case is almost 80,000 euros.

Massive financial and psychological consequences
In 2024 alone, fraudulent investment platforms stole around 95.5 million euros in life savings from hundreds of Austrian retail investors[4]. In addition to the financial losses, many victims suffer from depression and anxiety. In extreme cases, this can even lead to suicide.

Collaborative and highly professional fraud systems
Criminal records and studies by universities specialising in criminology show that investment scam websites are operated by transnational cybercriminal organisations. They operate in a highly professional manner based on a division of labour.

1 [4] Caution, investment scams: Recognising and avoiding investment scams; https://www.onlinesicherheit.gv.at/Services/News/Investment-Scams-Betrugsformen.html

4.1 EFRI: the controversial advocate

As of today (28 February 2025), EFRI has 1,658 members - European consumers who were victims of investment scams between 2016 and 2024 and lost more than 60 million€ (mostly their entire life savings) to cybercriminals.

We support our members through:

4.1.1 Emotional support

Victims of scams are not only damaged financially, but also emotionally. Above all, they need comfort, explanations, encouragement and psychological support. As an organisation and advocacy group for the victims of online scams, we therefore try to offer this support. We have set up social media channels for this purpose.

Members share their experiences in Telegram channels and Facebook groups. This makes the victims realise that they are not alone in their role as victims, but that this type of fraud affects many people and is no reason to be ashamed.

4.1.2 Support with data processing and criminal charges

EFRI supports victims in preparing relevant data for criminal charges and provides sample letters that can be sent to banks and credit card institutions.

4.1.3 Support with the recovery of funds

EFRI or an authorised legal representative takes on the representation of victims in criminal proceedings as a private party representative. EFRI also templates that victims can use to register as private parties in criminal proceedings. Furthermore, EFRI supports victims in filing complaints against perpetrators and accomplices based on a detailed analysis of the criminal files.

4.1.4 Clarification

EFRI provides information on how these fraud schemes work and warns against further scams by supposed "recovery organisations".

5 ACTIVITIES

5.1 Database structure

EFRI creates databases based on the fraud documents submitted by victims and by inspecting criminal files. We analyse parallels, identify beneficial owners of fraud schemes and record accomplices and financial crime enablers, such as IT service providers, financial service providers and marketing companies that regularly and frequently appear in fraud schemes.

5.2 Activities based on the collected data

The following actions are taken based on the data collected **on the fraud systems**:

- Informal coordination of European criminal prosecution authorities: We network public prosecutors' offices in different countries in order to
  to make investigations more efficient. Examples: Blue Trading, Kayafx, AlgoTech.
- Support in identifying new victims and determining the actual extent of damage
- Referral of whistleblowers to law enforcement authorities
- Carrying out campaigns, e.g. the petition for the extradition of GAL BARAK from Bulgaria to Austria in autumn 2019.
  more than 300 victims sent pre-prepared letters to the competent Bulgarian court.

The following actions are taken based on the data collected on the identified **financial crime enablers**:

- Filing comprehensive money laundering and criminal charges against regulated financial service providers with financial market supervisory authorities and
  Public prosecutor's offices (e.g. Wirecard 2020, Payvision BV 2019, Deutsche Bank 2020, Deutsche Handelsbank autumn 2020).
- Public relations work on the involvement of regulated payment service providers in fraud schemes.
- Participation in criminal proceedings and filing claims for frozen assets in cooperation with lawyers.

Public relations work on the information compiled on the fraud systems.

- Passing on information to media websites (e.g. FinTelegram) about new fraud schemes and players involved;
- Providing information to journalists across Europe on fraud schemes, criminal proceedings and fraud methods (examples:
  Handelsblatt, Profil, Süddeutsche, Falter, Wirtschaftswoche, etc.).

With these measures, EFRI is actively committed to combating cybercrime and protecting European consumers and retail investors.

6 Legal measures for the individual cases 2024

6.1 Lawsuits and criminal proceedings against Payvision

BV for victims of BARAK/LENHOFF

EFRI, through involved legal representatives, has already taken extensive legal steps in 2019 to initiate criminal proceedings against the Dutch formerly licensed financial services company Payvision BV and the former shareholders and board members of Payvision BV, Rudolf Booker, Cheng Liem Li and others. It is clearly thanks to EFRI's efforts that the Dutch authorities finally took action against Payvision and the individuals responsible.

On **5 April 2024**[5], the Dutch Public Prosecution Service announced that Rudolf Booker and Cheng Liem Li, the former board members of Payvision BV, had been fined 330,000 euros for massive, systematic and structural neglect **of know-your-customer regulations** and transaction monitoring in the years 2016 to January 2019**.**
€ were convicted. Payvision BV itself was not prosecuted as it had already ceased its business activities, as the public prosecutor's office stated.

Following publication of the decision on 5 April 2024, EFRI called the Dutch supervisory authority **De Nederlandsche Bank (DNB)** to its obligation and appeal this disproportionately low penalty. The aim was to prevent further damage to European consumers caused by the activities of Rudolf Booker and Cheng Liem Li.

Despite repeated requests and with reference to the DNB audit report from 2020, which found that Booker had "wilfully" neglected its supervisory duties, DNB has not, to our knowledge, lodged an objection to date.

6.1.1 Civil proceedings in the Netherlands

The civil proceedings initiated in Amsterdam in September 2023 by two victims registered with EFRI against **Payvision BV, ING Bank NV and ING Group NV** for damages were heard in Amsterdam on 20 June 2024.

The proceedings are based on a claim for tortious damages for payments made by the victims to the **Barak and Lenhoff** fraud schemes. **Payvision BV** has acted as the main payment service provider for these fraud schemes since 2015/2016 and, according to its own information, processed over 150 million euros in credit card payments between September 2015 and January 2019. Regulatory requirements such as **know-**

[5] https://www.om.nl/actueel/nieuws/2024/04/05/geldboetes-voor-voormalig-bestuurders-betaaldienstverlener-vanwege-tekortkomingen-bij-het-bestrijden-van-witwassen

Your Customer (KYC) and **transaction monitoring** were systematically disregarded, and fraud signals were ignored.

Following the hearing at the Amsterdam Commercial Court, settlement negotiations were held. Repayments totalling **around 3.7 million euros** were achieved for **around 140 victims**. The negotiations proved to be extremely difficult due to various circumstances. The court proceedings, which were interrupted for the duration of the settlement negotiations, are still ongoing.

EFRI now represents **more than 590 victims** of BARAK/LENHOFF (as of 27 February 2025) including the **140 victims** already settled**).**

6.1.2 Civil proceedings against Payvision BV in Austria

Three victims supported by EFRI have already **filed civil lawsuits against Payvision BV** in Austria in previous years.

All proceedings ended with a settlement. In all three cases, the over
Payvision, plus a share of the costs.

6.1.3 Civil proceedings against Payvision BV in Germany

A victim supported by EFRI (legal costs are borne by a litigation funder) has filed a **civil suit** in Germany **against Payvision BV** and its parent company ING Bank NV, Rudolf Booker). The proceedings are still pending and the credit card payment (processed via Payvision BV) has already been repaid.

6.2 Frozen funds in Bulgaria for BARAK victims

Back in **2019**, the **Austrian authorities** managed to secure around **2 million euros** in victims' money in **Bulgarian bank accounts**.

To this day - **six years later** - the authorities/courts have not succeeded in releasing the frozen funds from Bulgaria and paying them out to the victims.

In the meantime, **Marina Barak (BARAK's wife and accomplice)** has **filed a claim for the money**. In the meantime, according to information from the Bulgarian banks to the Bulgarian court, more than 40,000.00€ have already been incurred in custody costs, this amount reduces the money to be paid out to the victims.

After exhausting all legal means in previous years, EFRI has repeatedly approached the **Austrian Ministry of Justice** and asked for support. Each time we were referred to the responsible judge at the Regional Court for Criminal Matters.

6.3 Frozen funds at P2P GmbH, Cologne

In **2019**, after receiving our **money laundering complaint** against the **illegal money collection centre P2P GmbH**, the **public prosecutor's office in Cologne** seized several million euros in their accounts at **Sparkasse Aachen, Germany** and **BUNQ Bank** in the Netherlands.

In **September 2024** - after several **changes of the responsible judicial officer** - we were informed that **claims** are now being accepted.

EFRI represents several **victims from various European countries** who made payments to accounts at **Sparkasse Aachen** and **BUNQ Bank** as part of the **Lenhoff and Barak fraud schemes**.

6.4 Lawsuit Postbank Frankfurt

An EFRI-supported victim from Germany, lost over **70,000€** through the **Blue Trading fraud scheme**, has filed a lawsuit against **Postbank/ Deutsche Bank subsidiary.**

The victim transferred more than **€30,000** to an account of one of the more than one hundred shell companies for which **Postbank** provided accounts to online fraudsters. Although Postbank itself had already filed a **money laundering report** regarding a money movement on this account - before the plaintiff transferred her money to this account - we could not convince the German court that Postbank should have warned the victim in time. Postbank pointed out that the Cologne public prosecutor's office had authorised this specific transaction.

We have waived our right to appeal, but now have further evidence at our disposal thanks to the renewed **inspection of criminal files**, which will enable us to take further legal action.

6.5 Kobenhavn Andelskasse criminal proceedings

Between **2016 and 2018**, the Danish bank **København Andelskasse** facilitated the collection and transfer of **hundreds of millions of euros** in stolen funds to fraudsters.

In a **report published in 2018**, the Danish Financial Supervisory Authority **(FSA)** identified serious **shortcomings** in the bank's **compliance** and management. In particular, these included inadequate measures to **combat money laundering and terrorist financing**.

Despite **the imposition of a fine** of **DKK 794 million (approx. €103 million) in 2024, none of those responsible** have been **brought to justice** and the victims have **not** received **any compensation**.

We have sent an official letter to the **Danish public prosecutor's office** requesting a statement and have informed the Danish penal authority that we will be joining the **criminal proceedings against the responsible board members.**

7 From victims to members

As at **28 February 2025**, **EFRI** has **1,658 members**.

The organisation represents the interests of a total of **1,685 affected citizens** through various legal representatives in several European countries, of which **only 55 are from non-European countries**.

An overview of the largest fraud schemes and claims we have dealt with is as follows:

Fraud system	**Number of EFRI members affected**	**Total loss (€)**	**Status of the offenders**
Lenhoff/BARAK (e.g. Xtraderfx, Option888, Tradovest)	585	**20 million**	Offenders convicted in Austria and Germany
Blue Trading	225	**11.3 million**	Perpetrator not identified
ALGOTECH/BEALGO	110	**4.5 million**	Perpetrator not identified
Kayafx/Accountofx	190	**9.5 million**	Perpetrators convicted in Germany
ASIA SCAM	145	**15.5 million**	Perpetrator not identified

EFRI members have lost a total of more than **60 million euros** as a result of the fraud schemes mentioned.

8 OUR FINANCES

Revenue 2024

New members or victims pay a one-off membership fee of €75 upon joining, although exceptions are possible in individual cases. In the event of a successful out-of-court recovery of lost funds, EFRI receives a success fee of 10% of the amount refunded to the victim.

EFRI's income in 2024 was significantly influenced by the legal action taken against PAYVISION BV on behalf of the BARAK and LENHOFF victims. On the one hand, EFRI waived the one-off membership fee for the 170 new victims of BARAK and LENHOFF who joined the initiative in 2024. On the other hand, EFRI's activities from spring 2024 focused on the court case and the subsequent out-of-court settlement negotiations with Payvision BV. As a result, only 11 victims of a new Austrian investment scam identified by EFRI were included in the autumn.

Success fees were received in particular from the successful out-of-court recovery of funds from the Kayafx, Kontofx and Upfx fraud systems and from the settlement negotiations with Payvision BV.

In 2024, only 0.002% of total revenue was attributable to membership fees and the rest to success fees. This is a drastic change compared to previous years, as membership fees accounted for 75% of revenue in 2023 (2022: 83%) and success fees from out-of-court settlements only made up a small proportion of revenue.

With **effect from 15 November 2024**, the **Federal Ministry of Finance** granted EFRI **preferential treatment for donations in accordance with Section 4a (4) EStG 1988.** This enables us to accept **donations from companies (up to the legally permitted amount)** that wish to support our activities.

In future, EFRI will also endeavour to obtain public funding at national and international level.

Expenditure 2024

The costs recognised in 2024 in connection with legal cases (30% of total costs) primarily relate to expenses in connection with planned legal action against the Danish bank København Andelskasse and other legal measures against Postbank (a subsidiary of Deutsche Bank). Based on

The documents now available also allow legal action to be taken against the beneficial owners and management of VELTYCO Ltd, a listed company that enriched itself through Lenhoff's crimes.

The costs of the legal action against Payvision BV were borne by a litigation funding company with which EFRI concluded an agreement in the summer of 2023.

In recent years, EFRI has mainly financed itself through membership fees and has therefore established a lean administrative structure. Members are mainly supported via Telegram channels, in which new developments are communicated and discussed, by EFRI's extended board. This consists of several members who support the board for several hours a week and receive an expense allowance in return.

9 STRATEGIC LEADERSHIP

Sixt Elfriede

Elfriede Sixt is a long-standing Austrian auditor and tax advisor who, as a board member of the European Funds Recovery Initiative (EFRI), makes a significant contribution to the strategic direction and financial integrity of the organisation. With many years of expertise in auditing and tax consulting, she brings in-depth knowledge in the areas of accounting, compliance and risk management - essential building blocks in the fight against fraudulent financial practices and cybercrime. In previous years, Sixt has published on the topics of FinTech[6] and cryptocurrencies[7] with SpringerVerlag and thus also brings indispensable knowledge to this area.

Nigel Kimberley

With his extensive experience in communications consultancy and as a university lecturer, Nigel Kimberley (a Briton living in Finland) plays a key role on the board of the European Funds Recovery Initiative (EFRI). His first-hand experience of fraudulent investment schemes - confronting their facilitators and navigating the financial safeguards designed to protect consumers, from banks and regulators to law enforcement agencies - forms the basis of his expertise at EFRI. More importantly, he has worked extensively with victims, helping them build organised communities that empower them to take action and continue to advocate for justice. These efforts have been instrumental in strengthening EFRI's membership and international influence.

[6] Crowdfunding and the swarm economy, SpringerVerlag 2016
[7] Bitcoins and other decentralised transaction systems: Blockchains as the basis of a crypto-economy, Springer Verlag September 2016

10 CHALLENGES AND OUTLOOK

10.1 Next steps

The settlement negotiations with Payvision BV conducted in the summer of 2024 impressively demonstrated the dramatic situation of many victims. Countless victims who have lost all their savings through the machinations of Barak and Lenhoff are facing existential challenges. The fate of elderly victims is particularly harrowing, as they are forced to return to work despite their advanced age and health restrictions just to cover the constantly rising cost of living. For many, poverty in old age and illness are a direct consequence of the fraud they have suffered.

Some of those affected have had to sell their homes, while others have suffered serious health consequences. In many cases, the psychological stress caused by the fraud has favoured serious illnesses such as cancer or dementia - not least due to countless sleepless nights and the enormous emotional strain.

In view of this harrowing reality, we have decided to continue the fight for the victims of Barak and Lenhoff with determination. In cooperation with the Lower Austrian State Office of Criminal Investigation and the Vorarlberg Chamber of Labour, we have launched a campaign to reach other victims - especially those who were previously unaware of our activities. Our aim is to involve them in our fight and to take joint action against Lenhoff and Barak's accomplices, above all Payvision, in order to hold them to account.

However, contacting the thousands of affected victims is proving difficult. Fraudulent "recovery" companies that specifically approach victims - by email or telephone - and want to take money out of their pockets again a major obstacle. This perfidious form of repeated victimisation shatters the already fragile trust of those affected and makes it considerably more difficult to come to terms with cybercrime.

In order to solve this problem, at least for the Dutch victims of BARAK and Lenhoff (the opt-out model applies in the Netherlands), we have decided to submit an application to the Austrian **Federal Cartel Prosecutor** to for **authorisation from EFRI as a "qualified entity"** pursuant to Article 4(3) of Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EF, OJ No. L 409 of 4 December 2020 p. 1 on the bringing of cross-border representative actions.

Recognition in accordance with Section 1 (1) QEG will enable EFRI to act as a qualified entity **in accordance with** Article 4 (3) of Directive (EU) 2020/1828 **on** representative actions for the protection of collective consumer interests.

This would enable us to bring class actions on behalf of the victims and take action against the perpetrators and companies responsible.

This would be the next important step in the fight against those FCEs (Financial Crime Enablers) who make online fraud against thousands of European retail investors possible in the first place.

10.2 Future prospects

The lax or inadequate enforcement of existing supervisory regulations in the area of anti-money laundering and data protection in Europe has allowed cyber criminals to operate almost unhindered. With the help of regulated banks and payment service providers, they are able to deprive unsuspecting small investors and consumers their entire savings - often without having to fear serious legal consequences.

So far, only prosecution by US authorities has provided a certain deterrent. However, recent political developments in the US, particularly the massive deregulation of sensitive areas such as cryptocurrency services, give rise to fears of the worst for the global fight against cybercrime. A weakening of regulatory control could open up even greater room for manoeuvre for criminal networks and further undermine confidence in the financial market.

At the same time, technological progress in the field of artificial intelligence (AI) is advancing rapidly. While AI offers enormous potential for positive innovation, it also harbours considerable risks. Cybercriminals are increasingly using advanced algorithms to automate fraud systems, utilise deepfakes for identity theft and exploit targeted vulnerabilities in IT infrastructures. These developments indicate that the digital space is becoming more dangerous for all of us than ever before.

In view of these threats, it is all the more important that consumer protection organisations such as EFRI are given a stronger voice in the fight against financial crime. Targeted education, more intensive international cooperation and increased pressure on authorities and financial institutions can significantly improve the protection of investors and consumers. Without decisive action, trust in the financial market risks being damaged in the long term - with potentially serious consequences for the economy and society.