EFRI INITIATIVE

EU-Commission
Attn. Vice President Dubravka Šuica
Rue de la Loi 200
1049 Bruxelles, Belgium
Email: cab-suica-contact@ec.europa.eu

EU-Council
Attn. Charles Michel
Rue de la Loi / Wetstraat, 175
B-1048 Bruxelles/Brussel
Belgique/België
Email : ec.president@consilium.europa.eu

EU-Parliament
Rue Wiertz/Wiertzstraat 60
B-1047 Bruxelles/Brussel
Belgique/België
Email: eplobelgium@europarl.europa.eu, epluxembourg@europarl.europa.eu

Bcc:
European Banking Authority (EBA)
Tour Europlaza
20 avenue André Prothin
CS 30154
92927 Paris La Défense CEDEX
France
Email: info@eba.europa.eu

Vienna, July 14, 2021

Request to the European authorities to request the European Banking Authority (EBA) to initiate Breach of Law (BoL) investigations against Denmark/DNB for not taking appropriate steps regarding ING/PAYVISION (Article 17 of Regulation 1093/2010 (The EBA Founding Regulation))

To whom it may concern,

1. The *European Funds Recovery Initiative (EFRI)* is a victim protection organization in line with the Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 ("Victim Protection Directive"). We support victims of cybercrime in coping with the crime

committed against them, cooperate with law enforcement authorities all over Europe and act on behalf of victims in claiming damages.

2. EFRI, an association in Vienna, Austria, founded in spring 2020, now represents 988 European consumers who were scammed by cybercriminals (mainly boiler room frauds) for more than EUR 55,78 million of their lifetime savings over the past 60 months.
3. The damage done to thousands of European consumers - mainly elderly and vulnerable people - by the various types of investment fraud and boiler room scams is huge now and amounts to about 1 bn EUR on a monthly basis.
4. Innocent European consumers rely on the promises of cybercriminals about advantageous investment possibilities, transfer their lifetime savings, and, after months, realize that they have become the victims of unscrupulous transnational criminal organizations (TOC).
5. This type of fraud has been going on for more than 10 years and poses a threat to our society due to the resulting manifold financial and mental consequences such as old-age poverty, depression, loneliness, mental and physical consequences.

The use of the incumbent financial system as critical success factor for Cybercriminals

6. In addition to sophisticated software tools, aggressive marketing campaigns and unscrupulous call centers, the critical success factor for Cybercrime is the cooperation with the incumbent financial system required to get hold of the stolen funds.
7. The usage of the Incumbent financial system is essential to the intake of the victims' money, to launder it and, finally, to transfer the money to bank accounts under the direct control of the scammers.
8. It is only through cooperation with authorized payment service providers that the boiler room scams build up sufficient trust to convince thousands of European consumers to transfer their lifetime savings.
9. Without their illicit proceeds used to fund criminal activities, the lifeblood of the scammers operations is disrupted.

EFRI`s Request to the EU Commission to start infringement proceedings against Germany, Netherlands and Bulgaria dated November 16th, 2020

10. Already as of November 16th 2020 we approached the EU Commission to start infringement proceedings against Germany, Netherlands and Bulgaria forr failure to transpose EU Money Laundering Directives properly in their country (Article 258 (ex, Article 226 TEC) of the Treaty on the Functioning of the European Union) as these have been the countries we encountered most frequently in our fraud research. (Compare Appendix 1)
11. In February 2021 the EU Commission initiated the first stage of infringement proceedings against Germany regarding the implementation of the 4th Anti-Money Laundering Directive.
12. As the EU Commission has not taken appropriate procedures against Netherlands, we approached again the Central Bank of Netherlands (de Nederlandsche Bank) and delivered

extensive evidence about the involvement of PAYVISION – a 100% subsidiary of ING Group B.V. – in vast cybercriminal activities.

The role of a Dutch payment institution (licensed with the DNB) in a transnational criminal organization

13. PAYVISION B.V., registered in Amsterdam, has been a licensed payment service provider in accordance with the EU Directive Payment services (PSD 2) - Directive (EU) 2015/2366 for many years.
14. In a cybercrime court case in Vienna it got evident that PAYVISION B.V. has been acting since 2015 up to raids and the arrest of the cybercriminals (GAL BARAK and UWE Lenhoff) in January 2019 as the main acquiring payment service provider for a vast boiler room scam organization.
15. ING Group B.V. – one of the largest European banks - acquired 100% of the shares in the FINTECH PAYVISION in spring 2018 at a valuation of EUR 360 million just months before ING settled an agreement for massive laundering charges with the Dutch prosecutor.
16. According to PAYVISION's documents handed over to the Austrian and German law enforcement agency, PAYVISION processed a volume of EUR 55.6 million (stolen money) for the fraudulent websites of Uwe LENHOFF. The companies and platforms to be assigned to Gal BARAK showed a total processing volume of EUR 75.6 million (compare Appendix 2):

	Sum Transaktionen	Anz Transaktionen	Sum Chargeback	Anz Chargeback	Sum Fraud	Anz Fraud
Payific ltd	18.272.610,96 €	73.665	613.041,87 €	667	372.237,76 €	650
Hithcliff ltd	27.547.372,92 €	36.848	1.059.749,17 €	1.162	353.792,57 €	631
Celtic Pay ltd	9.826.550,91 €	12.104	378.170,62 €	344	58.923,66 €	174
Zwischensumme	**55.646.534,79 €**	**122.617**	**2.050.961,66 €**	**2.173**	**784.953,99 €**	**1.455**
Markets Development	28.101.859,97 €	26.843	2.125.984,71 €	1.252	1.065.605,74 €	971
Cool Markets	1.750.215,06 €	1.427	104.127,50 €	50	18.382,05 €	28
Optiumcommerce	4.806.545,28 €	4.868	819.898,78 €	310	51.485,14 €	103
Matching Blue Consulting	3.487.272,43 €	2.684	384.003,55 €	204	68.850,48 €	83
Gpay ltd	37.464.887,13 €	34.195	3.849.711,24 €	2.242	1.491.477,50 €	1.144
Zwischensumme	**75.610.779,87 €**	**70.017**	**7.283.725,78 €**	**4.058**	**2.695.800,91 €**	**2.329**

17. The EUR 130 million stolen money processed by PAYVISION represents only the credit/debit card payments of these fraud schemes. In addition, around EUR 140 million in bank transfers flew to the fraudsters with the help of Money Mules in Europe and Serbia, as well as a further EUR 20 million in cryptocurrencies. It should be noted that the total volume of EUR 290 million EURO only results from 8 online trading platforms. Thousands of unsuspecting European consumers lost their lifetime savings to the cybercriminals with the help of PAYVISION.
18. On 1 September 2020[1], Gal BARAK, a citizen of Israel, 33, was sentenced to 4 years in prison at the Regional Court of Vienna, by the Senate of lay judges chaired by Judge Christian Böhm for serious commercial fraud and money laundering. GAL BARAK was the beneficial owner of numerous fraudulent websites like xtraderfx, safemarkets... As of July 5th, 2020 Uwe LENHOFF

[1] https://efri.io/gal-barak-former-ceo-of-a-bulgarian-boiler-room-and-beneficial-owner-of-a-major-international-binary-option-and-forex-fraud-scheme-sentenced-to-4-years-in-prison-in-vienna-austria

– the beneficial owner of several fraudulent websites option888, Tradovest... was found dead in his cell in Saarbrücken.

19. Further investigations in other boiler room scams as well as in court filings in the US revealed that PAYVISION not only facilitated the laundering of the stolen money for the busted criminal organization around Gal BARAK and Uwe LENHOFF but also has worked for several other criminal organizations and facilitated their money transfers.
20. Already on June 5, 2019 EFRI sent numerous documents about the cooperation of PAYVISION with the criminal organizations of Gal BARAK and Uwe LENHOFF to the relevant supervisory authority in Denmark (de Nederlandsche Bank/DNB) as well as to ING for appropriate actions against the former board of management.
21. The enclosed criminal complaint details all allegations and provides all evidences found (Appendix 3 and enclosures)
22. Up to now we have not learned about Dutch money laundering investigations being launched at a request of DNB against the former board of management of PAYVISION resp. PAYVISION.
23. Despite ING supports the idea about Environmental Social Governance (ESG) in so many press releases and stress the importance of integrity heavily, they evidently do not care about harmed European consumers.
24. Not investigating PAYVISION and the former board of management publicly for proven failure to comply with Know Your Customer rules and transaction monitoring for so many years and their evidenced involvement with criminal organizations specially after the close personal relationship between the board of management and the beneficial owners got evident, does not seem to be appropriate with all the Cybercrime Threats ahead of us and with the specific drug situation in the Netherlands[2].

Cybercrime Threat

25. The world faces several threats, one of the newest threats we are facing, and perhaps the fastest growing, are those in cyberspace. Cyber criminals, hackers and foreign adversaries are becoming more sophisticated and capable every day in their ability to use the Internet for nefarious purposes.
26. We are dependent on the Internet – we use it for everything. We communicate online, bank and shop online, and store much of our personal information there. The economies globally count on having ready access to the Internet and its many capabilities as we go about our daily routines. The Internet opens new worlds to users and to criminals.
27. The cost of cybercrime – already in the billions of dollars and Euros – rises each year.
28. In general, the high earning potential of Cybercrime results in a development of the payment services industry for the fraud websites at an immense pace.

[2] https://www.addictioncenter.com/news/2020/01/netherlands-narco-state/

29. With the Cybercrime Threat rising, the importance of the financial industry to act as gatekeeper becomes more and more important as well as the request for the financial supervisory authorities to do their job properly and to act decisively and swiftly.

Why we want EBA to get active

30. Within Europe, Europol estimates that the value of suspicious transactions is equivalent to about 1.3 % of EU GDP. Across the globe, the figure is estimated to be close to 3 % of world GDP. Recent data shows that over 75 % of suspicious transactions reported in the EU came from credit institutions in more than half of the Member States[3].
31. Financial institutions must act as gatekeepers to the financial system and have therefore an important role in the collective fight against financial and economic crimes.
32. Financial institutions failing to do proper customer due diligence and to monitor transactions undermine the trust of citizens in financial institutions, negatively affect market integrity and threaten the stability of the financial system.
33. The EBA recently got an enhanced mandate to lead, to coordinate and to monitor AML/CFT efforts in the European Union,
34. We understand that EBA is supposed to coordinate supervisory actions at Union level to ensure that financial institutions apply effective and robust AML/CFT controls wherever they operate in the single market[4].
35. The EBA[5] has the power to investigate a potential breach of Union law (BUL) relating to AML/CFT legislation at Member State level. This could involve inadequate supervision allowing large volumes of ML/TF to take place in a bank
36. EBA seems to be the appropriate authority considering cybercrime attacks like boiler room frauds do not know country borders and damage and hurt victims all over Europe.
37. It is evident that national interests can prevent the start of a criminal investigation for money laundering notwithstanding evident evidences and proofs are given.

Our Request

38. On behalf of 988 European victims from cybercrime attacks we ask the EU authorities to start fighting money laundering seriously and to start to hold the management of financial industry players responsible for supporting cybercriminal activities.

---

[3] Press Release on the Report of the European Court of Auditors on The EU needs a stronger and more coherent oversight framework for combating money laundering

[4] https://www.eca.europa.eu/Lists/ECADocuments/SR21_13/SR_AML_EN.pdf

[5] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/ EC and repealing Commission Decision 2009/78/EC, OJ L 331, 15.12.2010, pp. 12-47, as lastly amended by Regulation (EU) 2019/2175 of the European Parliament and of the Council of 18 December 2019.

In case of any questions pls get back.

Yours sincerely,

Elfriede Sixt and Nigel Kimberly

(CEO of the EFRI Initiative)

Attention to the Financial Action Task Force (FATF)
2, rue André Pascal
75775 Paris Cedex 16 FRANCE
Email: Contact@fatf-gafi.org

Attention to the European Central Bank
Europäische Zentralbank
Sonnemannstraße 20
60314 Frankfurt am Main
Germany
Email: info@ecb.europa.eu