EFRI INITIATIVE

EU-Commission

Vice President Dubravka Šuica

Rue de la Loi 200

1049 Bruxelles, Belgium

Vienna, 18 November 2020

Re: Initiation of infringement proceedings for failure to apply correctly EU Anti-Money Laundering Directives in GERMANY, NETHERLANDS and BULGARIA as outlined under Article 258 (ex, Article 226 TEC) of the Treaty on the Functioning of the European Union

To whom it may concern,

1. The European Funds Recovery Initiative (EFRI) was launched in 2018 and now represents 876 European consumers who have been scammed by international cybercriminals.

2. In 2016, 2017, 2018, 2019 and 2020, these 876 victims transferred a total of more than EUR 45.9 million to the owners of fraudulent websites through various banks/financial service providers.

3. Based on a study of the transaction data provided to us by the victims, we created the enclosed Follow the Money evaluation (Supplement 1). This evaluation lists the financial institutions through which the 876 European consumers have transferred their money in accordance with the instructions received from the scammers.

4. Of the total of EUR 45.9 million of these 878 European consumers, EUR 36.03 million (76.45%) were transferred via wire transfers and EUR 6.9 million (15.10%) via credit/debit card

transfers, i.e. through the traditional financial system, to the cybercriminals. Only EUR 2.9 million (6.35%) went to the scammers by direct transfer of crypto currencies.

5. EUR 36.03 million were thus cleared through accounts of pure shell companies with mainly European financial institutions through bank transfers. EUR 6.9 million were processed by licensed acquiring organisations and subsequently paid out to bank accounts of shell companies – which have entered into contractual relationships with the acquiring organisations as merchants.

6. These shell companies, founded solely for the purpose of receiving and transferring the illegally acquired money to the fraudsters (also called “Money Mules”), form an integral part of the international cybercrime organisations.

7. These shell companies (only legal entities) all meet the following criteria:

- Incorporation was done as a legal entity by Company Builders or by “Incorporation Services" by the acquiring organizations.
- No physical presence in the respective countries (registered letters mailed to the addresses entered in the public registers were returned as undeliverable).
- These shell companies had foreign directors or owners without corresponding residence or residence in the country of incorporation and no information about these directors or shareholders can be found via an extensive internet search ("straw men").
- None of these companies had employees.
- The commercial purpose of these companies indicated in the public registers did not correspond to the exclusive activity of these companies (Money Mules).
- Most of these companies were newly established shortly before receiving the payments or were newly acquired legal entities.
- None of these companies has or has had an online presence, although the majority of companies, according to the public register, have a business activity that can be described as internet-savvy.
- The funds transferred to the accounts of these shell companies - amounts in the millions of EUROS within a very short period of time - were collected at regular - but above all very short-term - intervals.

- The entire life of these companies lasts often only a few months, after usage as an illegal financial service provider, the companies are liquidated or deregistered due to lack of assets.

8. All these shell companies run bank accounts with European financial service providers, and this is the key to enabling the illegal flow of stolen money to the fraudsters.

9. From the criminal records of the Israeli GAL BARAK, who was convicted in Vienna, Austria for serious fraud and money laundering as of September 1, 2020, the stolen money is apparently transferred usually to (shell) service companies in order to legalize the money as a service fee before it is transferred finally to the offshore companies that are officially owned by the cybercriminals. This process also requires countless shell companies, which must have bank accounts with various European financial institutions[1].

## Increasing Cybercrime

10. The increasing digitalization of society in general and the associated virtualization of money in particular poses a new, massive threat to consumers - transnational cybercrime. The combination of state-of-the-art technologies with new social marketing methods and a massive disparity in the tech affinity of Internet users create an unprecedented ecosphere for criminals, which is reflected in the massively increasing numbers of reported cybercrime cases.

11. It became clear to our victims that, although the European Union is trying to promote digitization, eliminate cash and promote the online payment industry, neither local law enforcement authorities nor European law enforcement authorities know how to tackle cybercrime appropriately. State-of-the-art technology mixed with criminal energy requires appropriate training and experience of the authorities. At this time, when the EU's cyber society is still at the beginning of the learning curve, our victims have had to pay a high price - their life savings - to learn this.

12. The single currency in the EU's internal market, combined with progress in the common payment area, is still a problem.

13. The extreme need to combat and prevent the use of the financial system for cybercrime purposes is therefore clear and is one of our most important objectives.

[1] Pls compare our discussion about Bulgaria Section 40 to 49 in this letter

14. We are convinced that preventing the use of the European financial system to transfer the stolen funds to cybercriminals is a high and perhaps the only effective contribution to curbing cybercrime.

15. The use of the traditional financial system to defraud thousands and thousands of European consumers is only possible because it appears that although the EU directives on Anti- money laundering have been implemented by law in the individual countries of the European Union, failure to apply them correctly has not been penalised or sanctioned in any way.

16. Based on our following experience with three countries: Germany (Section 17-29) , Netherland´s PAYVISION (Section 30 – 39) and Bulgaria (Section 40 – 49) , we will illustrate the Issue of Europe´s banks and supervisory authorities. Please be aware that these are only three examples as our Follow the Money sheet shows that financial organizations throughout Europe are used by scammers and evidently have serious issues with complying with the current Anti-money-laundering regulations.

# Germany the Money Laundering Paradise for Cybercriminals

17. Of the total of EUR 36 million wire transfers, EUR 12.03 million (26.21% of total transfers) were handled via bank accounts opened by shell companies with German banks. DB/Postbank (totalling EUR 4.5 million) and Wirecard AG (totalling EUR 3 million) have taken on a leading role over the years.

18. Wirecard BANK AG has evolved over the years from a processor for porn, gaming and binary options, Forex to the primary bank of some of the scammers. So, the fraudsters themselves run the accounts to receive and transfer illegal cash flows (in contrast to Money Mules).

19. In the case of DB/Postbank, we identified 83 (!) bank accounts of illegal payment service providers (Money Mules) through which stolen funds from various fraud systems were collected and forwarded.

20. Since our Initiative represents only a small part of the day-to-day online fraud in Europe, it can be assumed that Wirecard and DB/Postbank have enabled hundreds, if not thousands, of such shell companies to transfer stolen funds.

21. The activities of the German Wirecard Group in the illegal sector have been known since the company was founded in 1999. In 2017, a comprehensive report on the Group's money laundering activities was published and submitted to the competent German authorities (Zatarra report). The authorities did not start to get active. Over the years, there have been repeated reports of massive money laundering activities by the company and irregularities in the accounting of the DAX company. On 1 February 2020, the EFRI Initiative presented BAFIN and the relevant Munich Public Prosecutor's Office with a money laundering complaint with extensive facilities (Supplement 2). Two weeks later, EFRI informed the Munich Public Prosecutor's Office of the existence of a money laundering complaint by a Wirecard correspondent bank about suspicious transactions in connection with the fraud scheme #24Option (countless European victims) amounting to EUR 220 million. The Munich Public Prosecutor's Office did not get active.

22. Deutsche Bank also has a long list of convictions for money laundering (see also points 21.1 to 21.6 of our attached money laundering complaint (Supplement 3), which we submitted to BAFIN and the Frankfurt Public Prosecutor's Office on 27 March 2020. The criminal complaint we have brought before the Frankfurt Public Prosecutor's Office is still unprocessed due to a lack of human resources (!) (according to the prosecutor in charge.

23. It is particularly striking that the public warnings and prohibitions of individual fraudulent undertakings issued by European Financial Supervisory Authorities are not taken into account in any way by the German banks when opening accounts or maintaining ongoing account connections.

24. The example of GRENKE Bank, which maintained an account of FinTechServices GmbH and made it possible to accept illegal funds until late summer 2018, shows that even warnings from the Federal Financial Supervisory Authority (BAFIN) are ignored by the German banks.

25. The Federal Financial Supervisory Authority (BAFIN) has not commented on our money laundering report on Wirecard Bank AG or on the Deutsche Bank/Postbank money laundering report. Based on media reports, we know that BAFIN simply did not feel responsible for WIRECARD - obviously not even for the bank.

26. Over the years, thousands of desperate European consumers, who have been seeking help from BAFIN in investigating the crime committed against them, have also been kindly but resolutely rejected over the years.

27. On the basis of the available analysis of the financial transfers of only 876 victims of such fraud schemes, and with the knowledge that thousands and thousands of European victims of such fraud schemes have deposited their stolen funds into German accounts, it can be assumed that in the years 2016 to 2020 millions, if not billions (life savings of European citizens) of stolen funds, went to scammers through German accounts to cybercriminals.

28. BAFIN appears not to be fulfilling its obligations to supervise the banking sector with regard to money laundering.

29. According to the media coverage, the Financial Intelligence Unit's system was apparently never effectively implemented in Germany. The non-processing of thousands of SARs registered with the German Financial Intelligence Unit became apparent in the Wirecard scandal and has been a topic of German media coverage since the announcement of the balance sheet fraud and the bankruptcy of the group.

## PAYVISION - a Dutch FinTech

30. PAYVISION B.V., registered in Amsterdam, is a payment service provider founded in 2002 and acts as a payment service provider for online shops. In addition, PAYVISION B.V. enabled the online shops to accept credit/debit card payments and acted as an acquiring partner for the operating companies (merchants) of the websites. The financial flows were done via specially created vehicles such as Stichting Trusted Third Party PAYVISION.

31. The sole beneficial owner of PAYVISION is ING Groep N.V., Amsterdam, The Netherlands. As part of the implementation of its FINTECH strategy, ING Group N.V. acquired 75% of the shares in the start-up PAYVISION in spring 2018 for the valuation of EUR 360 million, based primarily on the "highly positive business development" of the company. At the end of 2019, ING subsequently acquired the remaining 25% of the shares in PAYVISION and bought out the founders.

32. Based on the statements of the accused UWE LENHOFF and GAL BARAK from the criminal file 9 ST 16/19p-116 as well as from the statements of Rudolf BOOKER/CEO PAYVISION, it is confirmed that the following fraud systems were handled via PAYVISION as acquiring partner:

- Option888, ZoomTraderGlobal, Tradovest, Lottopalace, (more than EUR 55 million) (2016 - 2019)
- XTraderFX, OptionStarsGlobal, Safemarkets, Goldenmarkets (more than EUR 77 million (2016-2019)
- EasyTrade, Binary Options (beneficial owners not yet known)
- AlgoTechs/BEALGO (beneficial owners not yet known)
- GetFinancial (the extent of payments unknown).

33. According to PAYVISION's documents, the companies and platforms attributable to Uwe LENHOFF showed a total processing volume of EUR 55.6 million (stolen money). The companies and platforms to be assigned to Gal BARAK showed a total processing volume of EUR 75.6 million (stolen money):

| | 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** |

34. The EUR 130 million stolen money processed by PAYVISION represents only the credit/debit card payments of these fraud schemes made in the years 2016 up to the beginning of 2019. In addition, around EUR 140 million in bank transfers flowed 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 only results from 8 online trading platforms[2].

35. Operators of the above-mentioned and other scams have always been shell companies with straw men as directors (nominee directors) and shareholders (nominee shareholders). Most of these shell companies have been registered in countries such as Samoa, Marshall Island, St. Vincent and Grenadines, Seychelles, but also in Bulgaria, Hong Kong, and London.

36. Since 2016, warnings issued by various financial market supervisory authorities against these fraud schemes have been issued, while PAYVISION, a payment service provider and the acquiring organization under the supervision of the Central Bank in the Netherlands, ignored all these warnings.[3]

[2] There are thousands of such trading platforms out there.

[33] https://www.fca.org.uk/news/warnings/gpay-limited-trading-cryptopoint.

Die österreichische Finanzmarktaufsichtsbehörde (FMA) hat mit Bekanntmachung im Amtsblatt zur Wiener Zeitung vom 30. März 2018 mitgeteilt, dass *New Markets S.A. (OptionStarsGlobal)* mit Sitz in Novasage Chambers, Level 2 CCCS Building, Beach Road, Apia, Samoa nicht berechtigt ist, konzessionspflichtige Bankgeschäfte oder Wertpapierdienstleistungen in Österreich zu erbringen. Es ist dem Anbieter daher der gewerbliche Handel auf eigene oder fremde Rechnung (§ 1 Abs 1 Z 7 BWG) sowie die gewerbliche Portfolioverwaltung (§ 3 Abs. 2 Z 2 WAG 2018) nicht gestattet.[3]CONSOB warning against Option888 and its operators: https://smnweekly.com/2016/12/28/italys-consob-warns-of-ayrex-option888-binary-options-brokers-broker-yard-forex-broker/ (dated **December 28, 2016)**

[3]FCA warns against Option888 and its operators https://smnweekly.com/2016/12/28/italys-consob-warns-of-ayrex-option888-binary-options-brokers-broker-yard-forex-broker/ (**dated May 2018**).

37. On 5 June 2019, EFRI sent a statement of facts to the Central Bank of the Netherlands, presenting the facts and requesting an investigation into the facts and information which provided additional information. So far, no reaction.

38. On 10 October 2019, EFRI again sent the letters of receivables addressed to PAYVISION to the Dutch Central Bank with the offer to provide more information – again, no response to today's date.

39. In general, the high earning potential of online investment fraud had resulted in a development of the payment services industry for the fraud websites at an immense pace.

---

https://www.fca.org.uk/news/warnings/gpay-limited-trading-cryptopoint.

The Austrian Financial Market Supervisory Authority (FMA) has announced by notice in the Official Journal of the Wiener Zeitung of 30 March 2018 that New Markets S.A. (Option Stars Global), based in Novasage Chambers, Level 2 CCCS Building, Beach Road, Apia, Samoa, is not entitled to provide bank transactions or investment services in Austria subject to concessions. The provider is therefore not permitted to trade commercially on his own or outside account (Section 1 (1) Z 7 BWG) as well as the commercial portfolio management (Section 3 sec. 2 Z 2 WAG 2018).

CONSOB warning against Option888 and its operators: https://smnweekly.com/2016/12/28/italys-consob-warns-of-ayrex-option888-binary-options-brokers-broker-yard-forex-broker/ (dated December 28, 2016)

[3]FMA wars against Option888 https://www.fma.gv.at/capital-force-ltd-option888/ https://www.fma.gv.at/capital-force-ltd-option888/ **(dated 25. November 2017)**.

FCA warns against Option888 and its operators https://smnweekly.com/2016/12/28/italys-consob-warns-of-ayrex-option888-binary-options-brokers-broker-yard-forex-broker/ (dated May 2018).

FMA wars against Option888 https://www.fma.gv.at/capital-force-ltd-option888/ https://www.fma.gv.at/capital-force-ltd-option888/ (dated 25 November 2017).

---

# BULGARIA The EU Scam and Money Laundering Hub in Europe

## The Money Laundering System of the Gal Barak Cybercrime Organisation

40. On 1 September 2020, the Vienna Regional Criminal Court reached its first verdict in the context of the so-called Vienna Cybercrime Trials. The Israeli citizen Gal BARAK was found guilty of serious fraud and money laundering as the operator and economic owner of the cybercrime organisation of E&G Bulgaria, located in Sofia, Bulgaria.

41. In the course of the investigation into this criminal case, the Bulgarian bank accounts of more than 46 companies were opened by the Austrian and German law enforcement agencies.

41. All these companies showed the following characteristics:

- With the exception of the Boiler Room (Call Center) operators and two technology service providers, they were exclusively shell companies.
- Only three of these companies had employees.
- Only 11 of these companies were registered in Bulgaria, the majority of the companies were registered in British Virgin Islands, Marshall Islands, Hong Kong, London, Samoa, Serbia, etc.
- All these shell companies had installed nominees, mostly Eastern European citizens, as managing directors and owners.
- All managing directors of the shell companies gave the actual beneficial owners (scammers) a power of attorney (PoA) for money transactions. In most cases, the owner of the authority was the wife of Gal BARAK, Marina Barak (formerly Marina ANDREEVA)
- Marina BARAK's telephone number was deposited as a contact person for inquiries but also for the execution of online banking transfers.
- Based on evaluations of the IP addresses, it was apparent for the Austrian criminal authorities that Marina BARAK actually administered the majority of the accounts and carried out the transactions[4].
- In fact, only the beneficial owners of the scams actually did all the banking transactions.

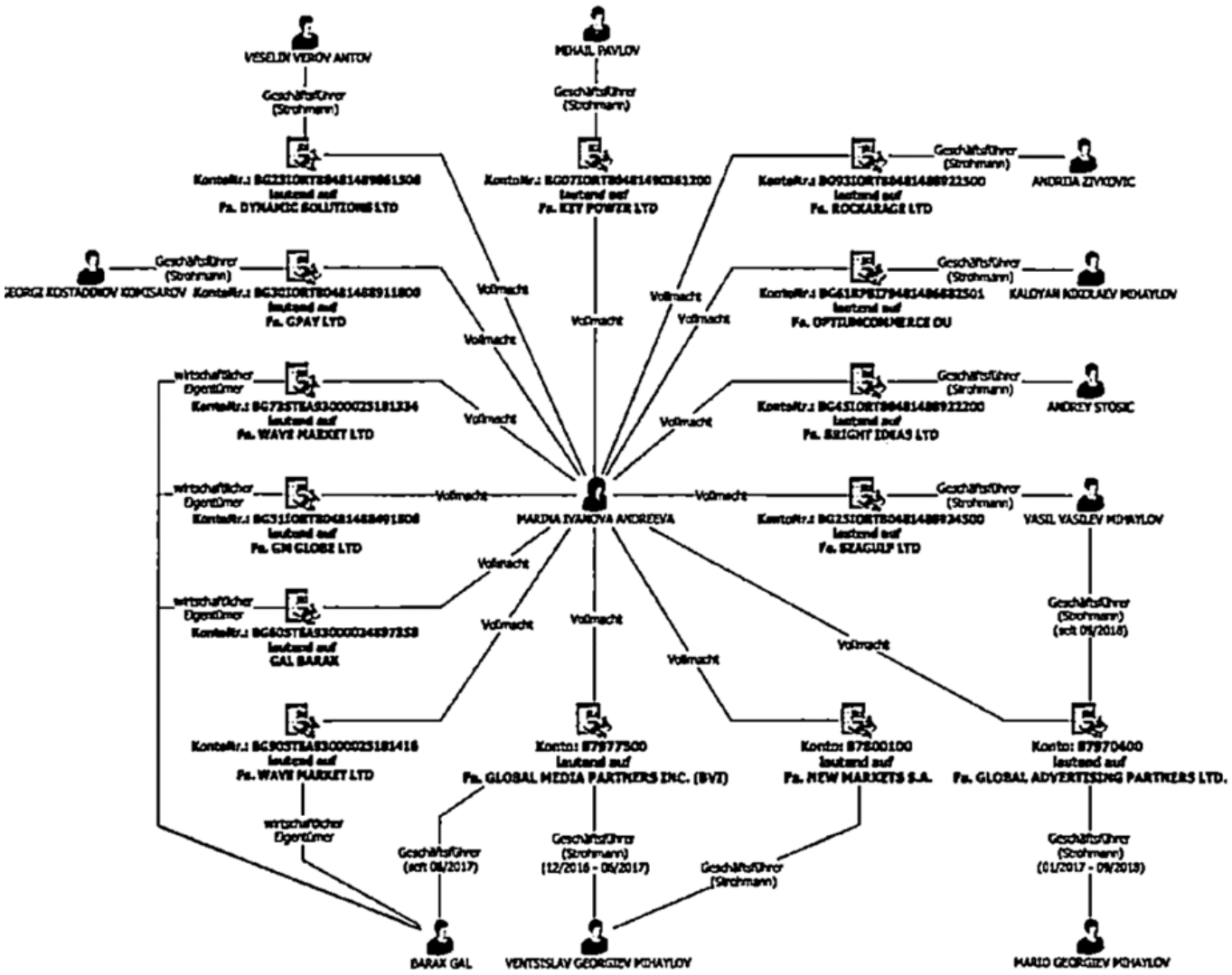
43. These identified **46 shell companies had more than 82 bank accounts with Bulgarian banks:** 50 with Investbank (IORTBGSF XXX - INVESTBANK PLC, Sofia) 10 with the DKS Bank

[4] As it must also have been evident for the Bulgarian banks.

(STSABGSFXXX BIC/SWIFT Code - DSK BANK AD Bulgaria ... and 11 with the Eurobank (BPBIBGSFXXX BIC/SWIFT code - EUROBANK BULGARIA ...) and some smaller banks.

44. A total of EUR 200 million of stolen funds flowed through the accounts of these companies between 01.01.2016 and 31.03.2019.

Graphically, the importance of Marina BARAK was illustrated by the criminal authorities for the most essential bank accounts as follows:



45. A critical factor in setting up a money laundering system is access to Company Builders (offshore and in Europe), who equip an almost infinite number of shell companies with straw men as managing directors and nominal owners and with corresponding bank accounts and make them available to the operators of the scams.

46. According to witness statements of Alexander I. – a former call centre (boiler room) employee of Gal BARAK at the cybercrime unit in Bamberg Germany in July 2019, there are **60 call centres in Sofia, Bulgaria, following the example of the Boiler Room operated by GAL BARAK.**

47. This statement by Alexander I. is consistent with our observations received from the registrations of the victims registered with us. There are countless Bulgarian companies that appear in the documents of various fraud schemes, either as operators or as service companies. The conclusion that accounts with the Bulgarian Investbank PLC, Sofia or DKS Bank AD Bulgaria are used to transfer millions, if not billions, of stolen savings from mainly Western Europeans to offshore countries every day is obvious.

48. How critical a good 'interaction' is with European banks is evident when understanding the money laundering systems of fraudsters. However, it is also clear how unlikely it is that the support, of the Bulgarian banks, may be a mere non-compliant application of the European money laundering directives. There is much to be said for the intent of the banks involved, or for mere incurrence of illegal funds being laundered on an immense scale through the accounts of Bulgarian banks.

# Violation of the implementation of the 4th and 5th Anti-Money Laundering Directives of European Countries

49. It is estimated that the volume of money laundering transactions worldwide amounts to 2 to 5% of world gross domestic product. That is a staggering EUR 1.9 trillion that will be used to finance bribery and corruption, to develop criminal activities and to support terrorist organisations.

50. Nearly 70% of money laundering and terrorist financing are carried out through legitimate financial institutions. However, the United Nations Office on Drugs and Crime estimates that "less than 1% of global trade is seized and frozen."

51. With the EU Anti-Money Laundering Directives, the European legislator addresses this issue and wants to improve the preventive system in order to combat money laundering practices and terrorist financing even more effectively.

52. Both the provisions of the 4th as well as the 5th EU Anti-Money Laundering Directive contain precise and detailed requirements for the individual Member States to ensure an effective fight against money laundering in the respective Member State.

53. Under the provisions of the 4th and 5th EU Anti-Money Laundering Directives (4th Money Laundering Directive 26 June 2017 and 5th Anti-Money Laundering Directive 20 January 2020), each Member State is obliged to establish an appropriate structure to combat money laundering or terrorist financing in its country and to ensure its effectiveness.

54. Based on the surveys we have carried out[5] and based on the examples of problem areas in only three European countries, it is clear that the various European countries have so far not implemented either the provisions of the 4th Anti-EU Money Laundering Directive or those of the 5th Anti-Money Laundering Directive in a timely manner.

55. Based on our experience we have analysed in Germany, so we are deeply convinced that Germany has not yet implemented the 4th EU Anti-Money Laundering and Counter-Terrorist Directive

• Germany has not taken adequate steps to assess, understand and mitigate the risks of money laundering and terrorist financing (Article 7 (1) – (4)).

[5] Vgl. Appendix 1: Follow the Money evaluation of the EFRI-Initiative.

• Germany has not so far ensured that obliged entities have policies, controls and procedures in place to effectively mitigate and manage the risks of money laundering and terrorist financing identified at Union, Member State and self-identified risks. (Article 8)

• Germany has not so far ensured that obliged entities apply due diligence obligations to customers when establishing a business relationship (Article 11 ff)

• The Financial Intelligence Unit set up in Germany is demonstrably not equipped with the appropriate financial, human and technical resources to carry out its tasks. (Capital IV, Section I, Article 32)

• Germany has failed to ensure in a timely manner that the effectiveness of its anti-money laundering or terrorist financing system can be verified by providing comprehensive statistics on factors relevant to the effectiveness of such systems. (Article 44)

• Germany has failed to ensure in a timely manner that the competent authorities carry out effective monitoring and take the necessary measures to ensure compliance with the 4th EU Anti-Money Laundering Directive (Article 48).

• Germany has failed to demonstrate that policy makers, FIUs, supervisory authorities and other competent authorities involved in the fight against money laundering and terrorist financing also have an effective mechanism in place to fulfil their obligation under Article 7, enabling domestic cooperation and coordination in the development and implementation of policies and measures to combat money laundering and terrorist financing (Article 49).

# SUMMARY

56. Based on the examples Germany (DB/Wirecard), the Netherlands (PAYVISION), Bulgaria (Investbank,..) it is apparent that the European anti-money laundering ("AML") and counter-terrorist financing "CFT") system which has been established over the past 30 years is not fit-for-purpose.

57. The European financial organisations do not fulfil their purpose to be a gatekeeper for financial crime.

58. The stated objective of the 4th and 5th EU Anti-Money Laundering Directives, which is to prevent the use of the Union's financial system for the purposes of money laundering and terrorist financing, is simply not met.

59. These not-fit-for-purpose issues make unsuspecting European consumers easy victims for cybercriminals.

61. On behalf of the 876 European victims of cybercriminals, we request the opening of infringement proceedings against the countries of GERMANY, BULGARIA and the NETHERLANDS

62. We ask you to request full refunds for the damages suffered by the victims. We are convinced that only if banks and financial organizations realize that they are liable for supporting scammers, they will stop supporting them. We urgently need functioning gatekeepers for the increasing cybercrime threats.

Please contact us in case of any questions.

Yours sincerely,

Elfriede Sixt and Nigel Kimberley

(CEO of the EFRI Initiative)

Appendices

| | |
|---|---|
| Supplement 1: | Follow the Money evaluation of the EFRI Initiative |
| Supplement 2: | WIRECARD Money Laundering Notice of 1 February 2020 - German |
| Supplement 3: | Deutsche Bank/Postbank Money Laundering Notice of 28 April 2020 - in German |