Mag. Elfriede SIXT
CPA
[redacted]

To

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

Marie-Curie-Straße 24-28,

60439 Frankfurt am Main,

Deutschland

Staatsanwaltschaft München I

z. Hd. Hildegard Bäumler-Hösl

Linprunstraße 25

80335 München

Deutschland

Europäische Zentralbank

Sonnemannstraße 20

60314 Frankfurt am Main

31 January 2020

Ref: Money laundering complaint against WIRECARD AG (DE0007472060), 85609 Aschheim und der WIRECARD BANK AG, 85609 Aschheim

1 First, I would like to inform you that I am a co-founder of the European Funds Recovery Initiative (EFRI). The European Fund Recovery Initiative, based in Vienna, Austria, was established in November 2018 in cooperation with the Consumer Protection Centre of the Vorarlberg Chamber of Labour in response to the massive increase of victims of various fraudulent online trading websites (hereinafter also referred to as "investment scams") in Europe. Since January 2019, more than 1,450 aggrieved parties have registered on the website www.efri.io with a total loss of more than EUR 30 million. 99% of these victims of fraudulent online trading websites are European retail investors aged between 50 and 85 years.

2 The EFRI initiative now represents more than 790 victims of various fraudulent online trading websites (also known as investment scams) vis-à-vis public authorities and fraud

organisations in their claims for compensation for damage suffered totalling more than EUR 29m[1].

3 We would also like to inform you that we have the necessary documents, statements, and evidence to substantiate the suspicion that the WIRECARD Group listed in the DAX group with its subsidiary WIRECARD BANK AG, München, Germany in particular has connections with many fraudulent online trading (Forex & Crypto) websites, where they facilitate financial transfers of monies using credit card payments as well as illegal online (Forex & Crypto) or gaming websites. This has continued to happen for many years, unhindered and unpunished, thus contributing to the alleged fraud perpetrated on thousands of European retail investors for years.

The money laundering complaint is structured as follows:

I. Payment processing for investment scams(Forex & Crypto).

II. Suspicious customers and transactions in detail

III. Extremely poor risk management and compliance monitoring

IV. Determination of the actual amount involved in money laundering by Wirecard

V. Hints on knowingly acting

I. Processing of illegal transactions

4 The "success" of fraudulent online trading websites (Forex & Crypto) websites (hereinafter "investment scams") and unlicensed online gaming providers depends to a large extent on being able to process payments for their customers or victims unhindered.

5 The documents appended with the present complaint prove that WIRECARD BANK AG or the WIRECARD Group (hereinafter "WIRECARD") enables the operators of illegal or unauthorised transactions to receive and forward funds:

[1] In the context of this paper, I refer to websites that offer investments either unlicensed or unlicensed to European private investors as alleged fraud models and / or investment scams, these websites violates both the ESMA restrictions (ban on selling to private investors, ban on bonuses, ...) as well as the licensing terms of the respective regulatory authorities. These fraud models usually do not have separate accounts, nor are customers' money actually invested through licensed exchanges or brokers. For these investment scams, there are usually a large number of customer complaints and / or criminal complaints from investors and / or investigations by the responsible law enforcement authorities already pending and / or warnings from financial regulators are already available. This applies, for example, to online trading websites such as Option888 (no license), HandelFX (no license) or AlgoTechs / Bealgo (no license). Fraud models are characterized by the fact that payments to customers do not take place or only partially and after intensive complaints and that the money invested by private investors is transferred directly to offshore countries.

5.1 Unlicensed gambling: WIRECARD has provided unlicensed online gaming operators, or shell companies [2]acting on their behalf, with bank accounts to receive funds for the purpose of carrying out their illegal business activities. This was done inevident disregard of the existing prohibition of involvement in payments in connection with illegal gambling (§ 4 para. 1 sentence 2 alternative 2 in conjunction with § 9 para. 1 sentence 3 no. 4 GlüStV).

5.2 Investment Scams: WIRECARD has also made bank accounts available to operators of allegedly fraudulent online trading sites or shell companies acting on their behalf for the receipt and forwarding of illegally acquired funds.

5.3 Fake Online Stores: WIRECARD, as an acquirer bank, third-party acquirer and reseller in the card-not-present business, has enabled unlicensed gambling providers and investment scams to accept credit card payments, thus allowing assets from illegal sources to be smuggled into the legal economy via credit or debit card payments. There is a specific risk here that WIRECARD, through its international network of partner companies and acquiring partners, which has grown over the years, may be involved in the establishment and use of fake online stores and transaction laundering[3].

II. Suspicious customers and transactions in detail

6 Licensed financial service providers such as WIRECARD are obliged to report suspicious customers and transactions to the competent supervisory authority. In any case, those customers, and their transactions against whom public warnings have already been issued by financial market supervisory authorities should be considered suspicious.

7 Based on public documents and information provided to us by victims, as well as by whistleblowers, it can be proven that WIRECARD Bank AG has provided bank accounts to investment scams such as Banc de Binary (2015 - ?)[4], Option888 (February 2014 - end of

[2] These shell companies acted as illegal payment provider (money mules) on behalf of investment scams.

[3] Fake online stores are online shops that are systematically used to undermine national legislation and the restrictive regulations of credit card companies regarding high risk business activities and high risk countries. Fake Online Stores are used to provide access to credit card acquirers to merchants in high-risk business areas such as pornography, gaming and fraudulent online trading websites. By setting up such structures, there is a risk that criminal organisations will pursue their activities in Europe and that financial resources, some of which originate from serious commercial fraud (cybercrime), will be absorbed into the financial cycle. The facilitated money laundering also poses a massive risk of terrorist financing.

[4] It was a binary options provider licensed in Cyprus. The company returned its trading license in January 2017, thus forestalling a ban by the regulatory authorities. On 6 June 2013, Banc de Binary was accused by the CTFC and the SEC of violating US financial laws. Both institutions filed lawsuits against the company for

2016), HandelFX[5] (October 2019 - January 2020)[6] and 24Option (2012 - ?) despite public warnings (according to Appendix 1, we represent victims with a total loss volume of EUR 2,535,341.18).

8 WIRECARD has provided merchants of the investment scams Algotechs/Bealgo, AnyOption, EZ Invest[7], etc. (see Appendix 2) with the possibility to accept credit card payments via WIRECARD BANK AG and/or various WIRECARD subsidiaries in their capacity as acquirer, third-party acquirer and/or reseller (see Appendix 2).

9 Criminal investigations are pending against the operators of the aforementioned suspected investment scams Banc de Binary, Option888 , AlgoTechs/BEALGO, HandelFX, AnyOption, 24Option etc. in Europe and internationally, and a large number of criminal charges have been filed in various jurisdictions worldwide. In many cases, at the time of receipt of the funds by the WIRECARD companies, warnings of various financial market supervisory authorities had already been published. A brief examination of the bank client's or merchant's business activities (which is in any case required by law and by the credit card companies' regulations) would have revealed this.

10 Here, particular reference should be made to the alleged fraud scheme 24option of Rodeler Ltd., licensed in Cyprus as Cyprus Investment Firm (CIF) under CIF No. 207/13. (branch office in Cologne, Germany):

- The Ontario Securities Commission (OSC), Canada, has already issued a warning on April 3, 2013 against Rodeler Ltd. and the fraud scheme 24Option and the numerous fraud schemes it operates: "Rodeler Limited doing business as 24option.com, 24fx.com, zoneoptions.com, grandoption.com and binaryoption-affiliate.com"[8] .

- On August 2, 2016, the French AMF prohibited any activity of 24Option in France.[9]

profit skimming. In addition, financial penalties and other injunctions and injunctions were to be imposed. According to various forums, the system was purely fraudulent and there are said to be countless victims of this system in Europe.

[5] HandelFx was (in the meantime the site has been blocked) an unlicensed provider of FOREX transactions.

[6] All systems are unlicensed providers of investment services (especially FOREX, ...) where the offer was also directed at German investors.

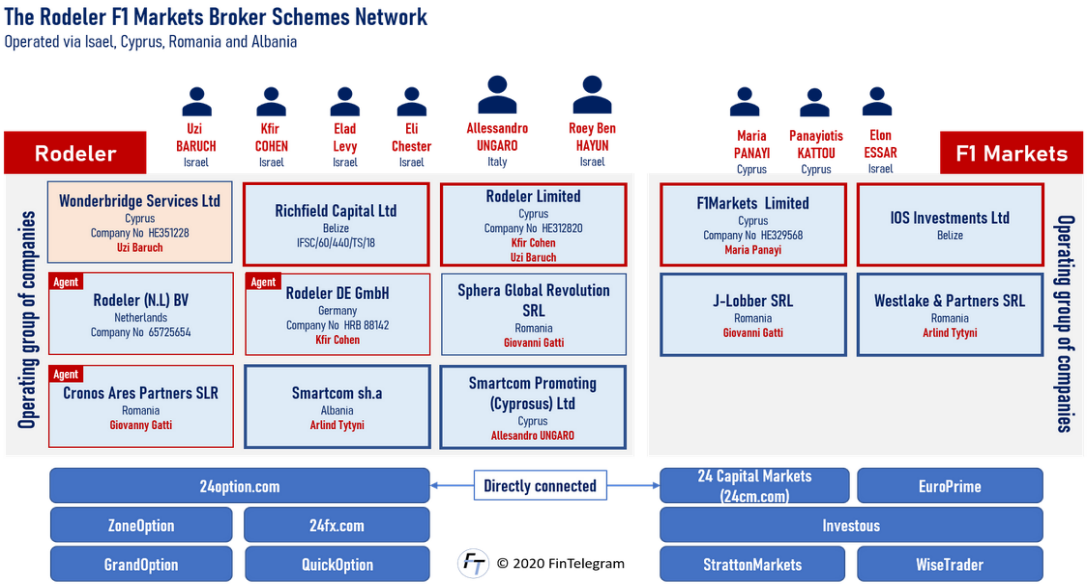
[7] All systems are unlicensed providers of investment services (especially FOREX, ...) where the offer was also directed at German investors.

[8] Rodeler Limited doing business as 24option.com, 24fx.com, zoneoptions.com, grandoption.com and binaryoption-affiliate.com

[9] The Autorité des Marchés Financiers (AMF) bans Rodeler Limited ("24option") from providing financial services in France.

- On December 24, 2019, CONSOB in Italy suspended all domains related to 24Option and the brands it operates[10].

  These warnings from financial market regulators have not prevented WIRECARD BANK AG from maintaining accounts for Roedeler Ltd and Richfield Capital Ltd (DE04 5123 080000064665) for years. WIRECARD Card Solutions Ltd is/was involved in the acceptance of credit/debit cards (Appendix 3/3) There are indications that the operators of the 24Option system now operate a very large number of various questionable websites.



11 Another example of this is the fraudulent system HandelFX. The Austrian Financial Market Authority issued an investor warning for this fraud system as early as 15 October 2019. Despite this investor warning, WIRECARD BANK AG accepted deposits totalling EUR 2,430,341.18 for the shell company FIKSU Media Inc (DE09512308000000122768) from 17 October to 24 December 2019 and forwarded them directly abroad (see Appendix 1).

12 There are victims who discovered the fraud shortly after making the transfer and turned to WIRECARD BANK AG, the police authorities or BAFIN for help. An example of this is Option888, a fraud scheme that is now pending before the criminal courts, for which complaints were received by WIRECARD AG or the Bavarian police and BAFIN throughout 2016[11].

III. Extremely poor risk management and compliance monitoring

[10] Consob Bans 24Option Trading Services in Italy.

[11] Cf. criminal case against Uwe Lenhoff on account of serious commercial fraud and gang formation at the Vienna Public Prosecutor's Office or Enclosure 4 and Enclosure 5 and Enclosure 6

13 WIRECARD BANK AG is obliged pursuant to § 6 para. 1 GwG to create appropriate systems for its customers and to keep them up to date in order to detect and prevent fraud, money laundering and other misuse of the financial system. These systems must include, inter alia, the development of internal principles, procedures and controls relating to various risks and obligations. This also includes, for example, the appointment of money laundering officers or the corresponding review and training of employees (Section 6 (2) GwG). Financial service providers must carry out regular monitoring and ensure that customer payments are allocated through legitimate channels or payment methods.

14 The important responsibility of payment providers in combating illegal business activities was established by the statutory prohibition of participation in payments in connection with illegal gambling (Section 4 (1) sentence 2 alternative 2 in conjunction with Section 9 (1) sentence 3 no. 4 GlüStV). Comparable to the illegal gambling market are the countless illegal online trading websites that offer their products to private investors without permission and also quite obviously in contravention of the ban imposed by ESMA in the European area since July 2018.

15 In our opinion, the activities of WIRECARD described under point 4 constitute a violation of the provisions of the German Money Laundering Act (GwG) or its amendment (GwGErgG) as well as an obvious disregard of the compliance regulations of the credit card companies when accepting high-risk merchants.

16 In our opinion, the frequent occurrence of WIRECARD in all these cases of fraud is a strong indication that the risk management systems and fraud detection systems required by law and regulations are either not in place or are not properly applied at WIRECARD. This is the only way that operators of investment scams and illegal online gambling - for years - can succeed in gaining access to the international financial system via the services of WIRECARD - in whatever form - and carry out their fraudulent activity with the help of this financial service provider.

17 Altair Entertainment N.V., a company registered in Curacao, can be cited as <u>an example of compliance deficiencies due to intent or gross negligence:</u>

- This offshore company was the operator of the suspected fraud system Option888 and account holder of the WIRECARD account DE02512308000000060530 from February 2014 until the end of 2016.

- Although classified as a high-risk customer with the MCC code 7995, neither a content nor legal website check had taken place at the beginning of the business relationship, or during the business relationship, as this would have immediately revealed the obvious inconsistencies of the fraud system.

- Nor do the account documents of Altair Entertainment N.V. submitted to the Munich Public Prosecutor's Office in a letter dated September 28, 2017, contain any documents to prove that a necessary audit of the business activity was conducted.

- In the meantime, Option888 arrests have been made in connection with the suspected fraud case and countless house searches have been conducted in various countries. The damage to European - and above all German - small investors is in the three-digit million range.

- Reference is made to the pending criminal proceedings in Saarbrücken against Uwe Lenhoff, beneficial owner of Altair Entertainment N.V., and the media coverage[12] - which speaks of countless platforms attributable to him.

- The appended account documents of the Altair Entertainment account (DE02512308000000060530) show that the persons entitled to the account in the Altair Entertainment environment were, or are, entitled to dispose of a large number of other WIRECARD accounts (Appendix 7/1, 7/2, 7/3 (also from the criminal case of Uwe LENHOFF). The blocking of an account due to suspected illegal activities should, in our opinion, also lead to an examination of the other accounts in which the persons involved are authorized to dispose, especially if the authorised signatories are obviously active in the already questionable online gaming sector.

18 In our opinion, it should not be possible for persons who are connected to a blocked account to be able to maintain other accounts for companies with WIRECARD without further ado or to be accepted as their authorised representatives. There is no proof whether these WIRECARD accounts, which are obviously connected to the Option888 fraud case, were also blocked at the end of 2016. This is explosive insofar as, for example, Payific Ltd (WIRECARD account DE02512308000000061611) was also the operator of the Option888 fraud system for a long period of time.

IV. Determination of the actual amount involved in the money laundering by Wirecard

19 The fraud systems of the investment scams have developed from illegal online gaming (gambling) in 2009/2010 and have now reached an enormous scale. It is estimated that the damage caused by these fraudulent websites amounts to up to EUR 1 billion per month. The estimated number of those who do not file a criminal complaint and quietly accept the loss of their life savings is gigantic. Only a very small proportion of the victims of these fraud systems report the crime or join initiatives such as the European Funds Recovery Initiative. Many try to deal with the psychological and financial damage in other ways, some victims commit suicide.

20 This type of fraud is made possible by European financial service providers who provide their services to fraudsters recklessly, negligently, or even intentionally, thus contributing to the fraudulent activities of thousands of Europeans.

[12] Arrest of UWE Lenhoff

21 The Board of Directors of WIRECARD repeatedly points out that the roots of the company are to be found in the porn, gambling, adult entertainment business, etc. The execution of payment processing of poker websites (Full Tilt Poker and PokerStars), sports betting sites and porn sites by the WIRECARD Group's Click2Pay online payment tool is accepted public knowledge. In this respect, WIRECARD is to be understood as a pioneer of payment processors of digital goods. Due to the historically long activity of WIRECARD in the field of online payment processing in the adult entertainment sector, it can be assumed that the management of WIRECARD should be sensitized to the topic of misuse possibilities of the financial system and especially the card-not-present business.

22 According to WIRECARD, in 2018, only 6 -10% of the payment transactions carried out by the Group were attributable to gambling (poker, casino, sports betting) and adult entertainment. According to the company's annual report, the transaction volume of the WIRECARD Group in 2018 amounted to EUR 124.9 billion (2017: EUR 91.0 billion), 10% of which would be EUR 12.5 billion and EUR 9.1 billion respectively for 2017, which would be a gigantic volume if only some of the transactions were of illegal origin.

V. Hints on the knowingly acting of Wirecard

23 According to various media reports, there are enough indications that WIRECARD Bank AG has experience of the risks of possible misuse of bank accounts for illegal payment services.

23.1 It is only worth mentioning the role of WIRECARD Bank AG in connection with the subscription traps[13] in the years 2008 to 2010: Even then, various WIRECARD bank accounts were repeatedly mentioned in connection with the various fraud schemes (for example the ProPayment GmbH account: 15792 BLZ: 512 308 00 WIRECARD Bank AG)[14].

23.2 Alternatively, reference may be made to the issued in spring 2019 against DG International Limited (DE 53512308000000050494) for an account with WIRECARD Bank AG. This account was relevant in connection with the lawsuit filed by a US ISP (Internet Service Provider) against an online dating portal (Zoobuh, Inc. v. Savicom, Inc. (D. Utah), because of massive spamming by ISP customers (mails with partly pornographic content). [15]

24 Indications that WIRECARD Bank AG knew, or should have known, about the risks of abuse of the card-not-present business are as follows:

[14] Content4u und Deutsche Zentral Inkasso : Eine Unendliche Geschichte

[15]

24.1 Court documents relating to the trial of the US Department of Justice (DOJ) against Michael Schütt for circumventing the ban on gambling in the USA[16]. According to the relevant court documents, several accounts (including the account of Bluetool LTD 34 Rosedahl Ave, Blackhill Consett Row, Durham) with WIRECARD BANK AG, Germany, were used to circumvent the US gambling prohibition and to enable payouts in the range of USD 70 million to US citizens from gambling winnings (2007 - 2010)[17].

24.2 Reporting on the involvement of the WIRECARD Group in the establishment and use of over 1,000 English shell companies in Durham, Ireland (the above mentioned Bluetool LTD was one of these shell companies). The suspicion that, by setting up special company structures using related partner companies, a systematic concealment of the actual extent of WIRECARD's involvement in high-risk online payment processing transactions was and is intended to be achieved has been repeatedly discussed in the media for years. In the meantime, the involvement of WIRECARD in the shareholder structures of these Irish companies, but also the frequent appearance of these shell companies with accounts at WIRECARD Bank AG in criminal files of various countries can be regarded as proven.

24.3 A good example of this is Bluemay Enterprises Limited, Unit 1 Derwentside Business Centre, Consett Business Park Villa Real, Consett, County Durham, England, DH8 6BP. According to the report of the British bankruptcy court, the account with WIRECARD Bank AG was used for EUR 36,259,489 between 1 January 2011 and 18 March 2013. However, the business purpose of the company could not be determined to date due to the lack of any documents from the company.

24.4 At this point it should also be noted that EW Trading Ltd (Company No: 07664160), through which presumably card-not-present payments were processed by WIRECARD BANK AG for the fraud system AlgoTechs/BEALGO and also for the fraud system 10Trading in 2018/2019 (see Appendix 2), is also located at 10a Milton Street, Darlington, County Durham, DL1 4ET.

24.5 WIRECARD BANK AG accounts have also appeared in connection with the money laundering scandal surrounding FBME Bank Ltd. This is the Cypriot branch of a bank from Tanzania, against which the U.S. FinCEN has issued a ban on the use of the US financial market in 2015 on suspicion of massive money laundering and terrorist financing. The accusations against the FBME Bank read like quotes from a handbook for organised crime in the financial sector: formation of shell companies, **miscoding of credit card transactions, processing of financial transactions of child pornography, etc. According to research reports by the consultants involved (Kroll Associates UK), WIRECARD Bank AG held numerous accounts (e.g. Magnoliafield and**

[16] Criminal Complaint, Case 2:10-mj-01015-SPC Document 1 Filed 02/17/10

[17] Wirecard und die 1000 englischen Briefkastenfirmen

Medina Networks Ltd., 6 Fairview Drive, Consett, County Durham, England, DH8 6QX and Opalta Ltd/Bulova Investments (DE 035123080000058281)) for some of the suspected criminal organisations until 2012. With WIRECARD bank accounts of these obvious shell companies, multi-digit million euro amounts were transferred to FBME bank through correspondent banks. It is only under pressure from these correspondent banks that WIRECARD BANK AG is said to have restricted the business relationship with the beneficial owners of these accounts.

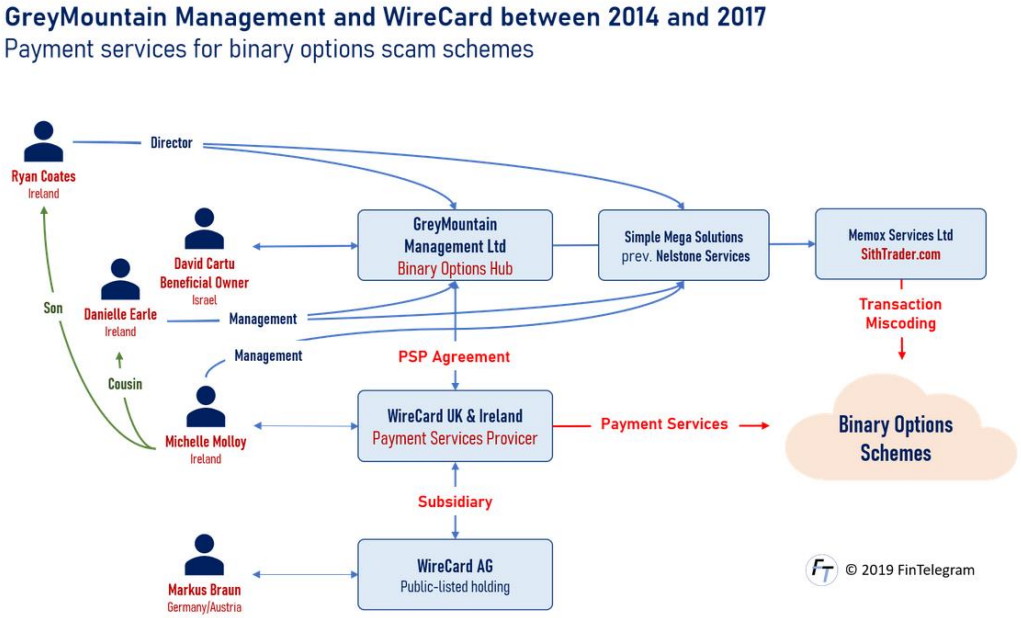
24.6 Involvement of WIRECARD in the Banc de Binary fraud system (until 2017).

24.7 Involvement of WIRECARD in the activities of AlliedWallet Inc (US) and Allied Wallet (UK). The Allied Wallet group of companies is a service company which was active as a payment facilitator/payment processor for various online fraud systems and against which the US FTC (Federal Trade Commission) filed a criminal complaint (No. 2: 19-CV-4355) on 20 May 2019 for complicity with a loss of more than USD 110 million due to transaction laundering through the establishment of fake online stores and miscoding (until 2017).

24.8 Involvement of WIRECARD or executives of WIRECARD in the criminal proceedings of the Israeli payment service provider Credit Card Ltd (ICC-CAL Criminal Proceedings), a subsidiary of the Israeli discount bank, which concerned Transaction Laundering on a large scale / specifically miscoding of transactions for illegal online gaming, pornography (child pornography) and illegal distribution of pharmaceuticals .

24.9 Involvement as a payment service provider in the various fraud schemes of Grey Mountain Management Ltd ("GMM"), Ireland. GMM was based in Dublin at the address of WIRECARD UK and Ireland. Between 2014 – 2017, financial market regulators issued numerous warnings and cease-and-desist orders against the various investment scams of the Israeli entrepreneurs David Cartu and Jonathan Cartu. Lawsuits filed by aggrieved GMM investors are still pending in Ireland and Israel. There must be innumerable victims of these fraud systems, which have not yet been dealt with, where there were obvious personnel interlocks with the WIRECARD Group.

.[18]



24.10 It is noticeable that WIRECARD Bank AG frequently carries out transactions with countries which pose a high money laundering risk for Germany, such as Curaco, Cyprus, Malta. All these countries favour non-transparent transactions. Criminals are thus given the opportunity to conceal transactions. Malta is a focal point for online gambling, which is associated with very many transaction flows. These are hardly traceable, let alone attributable to specific persons.

On December 9, 2019, the Bavarian State Office of Criminal Investigation issued a warning against rip-offs of financial investments on the Internet and pointed out that the total loss in Bavaria alone has now risen from just under EUR 100,000 in 2015 to over EUR 15 million in 2019. It is highly probable that part of this loss was settled via WIRECARD in whatever form (bank accounts or card-not-present).

The suffering of European retail investors caused by investment scams and online casinos is unimaginable. Righteous citizens are losing their life savings to mafia-like organisations, trusting in a secure digital environment and a proper financial system in Europe. Banking and payment providers have an important role to play in combating crime and the threat of terrorism. Payment service providers and banks have both the financial and technical means to fulfil their obligations to society in this respect, especially in comparison with private investors, and therefore any negligent or even deliberate failure to comply with money laundering obligations, and hence the possible aiding and abetting of multiple acts of fraud by

[18] Aussage eines früheren Mitarbeiters der Grey Mountain Management Ltd. vgl. Beilage 10

any banking institution against European private investors, must be condemned in the strongest possible terms and punished without fail.

Yours sincerely

Elfriede Sixt