Fiscal Information and Investigation Service (FIOD)
Postbus 19266
3501 DG UTRECHT

Netherlands

Openbaar Ministerie Amsterdam

IJdok 163

1013 MM Amsterdam

Netherlands

Vienna, 31. August 2021

Reference: Criminal complaint against Rudolf BOOKER Van der Helpstein 3, 01072 Ph Amsterdam, Gijs OP DE WEEGH, Cheng LIEM LI former members of the board of Management of PAYVISION B.V. Molenpad 2 Amsterdam, 1016 GM for complicity in serious commercial fraud and money laundering

Ladies and gentlemen,

General

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 processing 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 1.060 European consumers who were scammed by cybercriminals for more than EUR 56,8 million in the form of investment scams also referred to as boiler room scams.

3. The damage done to thousands of European consumers - mainly elderly people - by the various types of investment fraud and boiler room scams is huge now and amounts to about 1 bn EUR monthly.
4. This type of fraud has been going on in Europe 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.

Payment service providers as critical success factors for this type of cybercrime

5. In addition to sophisticated software tools, aggressive marketing, fraudulent affiliate campaigns and unscrupulous call center, the critical success factor for this type of online fraud systems above all is the cooperation with regulated European payment service providers.
6. These European payment service providers are essential to the intake of the victims' money, to launder it and, finally, to transfer the money to bank accounts under the control of the scammers.
7. It is only through cooperation with regulated payment service providers that the fraud websites get the necessary seriousness to convince thousands of European consumers to transfer their life savings to the online fraud websites.

Background of PAYVISION B.V.

8. Based on the records of the victims we represent, as well as based on the findings in criminal and civil files in Europe and the USA, one of the European payment service providers, which has been heavily used for many years by various international criminal organizations, is the Dutch PAYVISION B.V. (in the following "PAYVISION").
9. PAYVISION B.V. Molenpad 2, 1016 GM Amsterdam (KVK number: 3707811) is a Dutch limited liability company founded in 2002 by Rudolf BOOKER and its co-founder Gijp op DE WEEGH.
10. Until 7 May 2020, the Board of Management of PAYVISION consisted of Rudolf BOOKER, CEO, Gijp op DE WEEGH, COO and Cheng Liem LI, CCO.
11. In addition to PAYVISION B.V., the PAYVISION Group includes PAYVISION Holding B.V. founded on 24-5-2012: KVK number: 55358942 and ACAPTURE B.V; KVK number 58184082 (today Cetler B.V.) founded on 20-6-2013.
12. Furthermore, the special vehicles **Stichting Trusted Third Party PAYVISION** and **Stichting Trusted Third Party ACAPTURE** are part of the group.
13. On 29 January 2018, Rudolf HAMERS – the then CEO of ING Groep B.V. – announced that ING Groep NV (subsequently ING), one of the largest banks in the Netherlands, had entered into an agreement to acquire a 75% stake in PAYVISION, Amsterdam[1]. The agreed purchase price amounted to EUR 380 million. The achieved valuation was

[1] https://www.globenewswire.com/news-release/2018/01/29/1313302/0/en/ING-further-invests-in-payments-business-with-acquisition-of-majority-stake-in-Payvision.html

thus 12* the annual gross profit achieved on sales as of 31.12. 2017 (EUR 29 million). According to various media reports, the founders of PAYVISION had long been looking for a buyer.

14. In November 2019, ING agreed to acquire the remaining 25% share of PAYVISION in three tranches between November 2019 and April 2020, based on the initial valuation of EUR 380 million, resulting in an additional payment of EUR 90 million.
15. In May 2020, Rudolf BOOKER, Gijs op de WEEGH and Cheng LIEM left their board positions.
16. In the annual report of ING as of 31 December 2020 (published in March 2021), page 65 details that a write-down of EUR 260 million on the goodwill of PAYVISION was carried out in the financial year 2020. On page 175 of the Annual Report, it is stated that already at the time of the acquisition of PAYVISION, ING would have recognized that the nature of the customers of PAYVISION (porn and gambling is mentioned in the specific) would not be part of the activities of ING and therefore began to reduce this type of customer as early as 2018.

Business activities of PAYVISION

17. PAYVISION is a payment service company licensed as such by the Dutch Central Bank (De Nederlandsche Bank (DNB)) in accordance with the European Payment Services Directive (PSD2).
18. In addition, PAYVISION is a licensee of credit card companies (MasterCard/VISA), which allows PAYVISION to act as an acquirer for both the card-present and the card-not-present environment, and to be able to accept credit card and debit card orders for operators of online websites (dealers) on bank accounts held by PAYVISION for the merchants and subsequently pay them out to the merchants. [2]
19. As subsequently stated, PAYVISION, like WIRECARD, the now insolvent German FinTech, due to the higher achievable margins, has concentrated on the business with high-risk merchants from the start of their business activities.[3]

[2] Or. stiched Trusted Third Party PAYVISION and Stichting Trusted Third Party ACAPTURE.

[3] Credit card companies classify certain business verticals as "high risk" from an underwriting point of view. Some merchants are classified as "high risk" because they are more vulnerable to payment card fraud and chargebacks. Others can be considered "high risk" because they operate in industries that are subject to a high level of regulatory and enforcement control and therefore pose a higher level of regulatory and reputational risk to Mastercard and VISA and payment service providers. Common "high risk" categories are: Adult Entertainment, Firearms, Alcohol/Hard Alcohol, Tobacco/eCig/VAPE, Nutraceuticals, Auction Webseiten, pharmacies, multi-level marketing. Betting, Lottery Tickets, Casino. binary options, Forex. Due to the nature of the transactions processed or the high reputational risk, many acquirers or payment service providers do not work with High-risk traders. Therefore, High-risk traders willing to pay higher margins to acquirers who are willing to process their transactions. Unscrupulous payment service providers and acquirers exploit this dependency ratio by using fraudulent and illegal tactics to circumvent legal requirements to support fraudsters and fraudsters.
In this way, the unscrupulous payment service provider not only violates the law and card brand rules, but also facilitates fraudulent transactions and allows fraudsters to rip off innocent people who depend on the integrity of payment service providers.

20. PAYVISION has for years – before and after the acquisition by ING until today – handled transactions for high-risk merchants such as porn (e.g., PORNHUB), gambling or trading (binary options, forex, CFD).
21. In addition, however, PAYVISION has also participated in fraud schemes of international criminal organisations in violation of the legal provisions imposed on the company as a regulated payment service provider (mainly on money laundering), but also in violation of the requirements of credit card companies to its licensees.
22. PAYVISION has also intentionally, knowingly, and willingly provided services to other unscrupulous financial service providers, such as T1 Payments LLC (see section 88f) and Allied Wallet (see section 109ff).
23. Summarizing we are convinced that PAYVISION was knowingly and willingly involved in numerous fraud schemes of European and US citizens, fraudsters managed to rip off tens of thousands of European consumers by hundreds of millions of their life savings over the years through the deliberate help of PAYVISION, for proof pls refer to:

- Information from the criminal facts of LENHOFF/BARAK at the Criminal District Court of Vienna (730 Js 1545/18).
- Statements of the exCEO of the company Rudolf BOOKER in above criminal files.
- Deposit confirmations (bank transfers and credit card billing) for scams.
- Information from public records of legal cases pending in the United States involving PAYVISION.

Acting as an accomplice of GAK BARAL and UWE LENHOFF

24. On 29 January 2019, the Austrian and German law enforcement authorities arrested Uwe LENHOFF, a German citizen. He was charged with serious commercial fraud and money laundering. Lenhoff had been identified by investigators as the beneficial owner of the following fraud websites (trading platforms): **Option888, ZoomTrader, ZoomTrader, Tradovest, TradeInvest90, Lottopalace, Xmarkets**. Since 2016, there have been countless criminal complaints from damaged Europeans to the European criminal authorities about these fraud websites.
25. There have also been countless warnings from supervisory authorities about the fraudulent websites like:

OPTION888	Österreich	25.11.2017	https://www.fma.gv.at/capital-force-ltd-OPTION888/
TRADEINVEST90	Österreich	13.02.2019	https://www.fma.gv.at/celestial-trading-ltd-TRADEINVEST90/
XMARKETS	Österreich	06.04.2018	https://www.fma.gv.at/sg-innovation-ltd-XMARKETS-com/
TRADOVEST	Österreich	13.06.2018	https://www.fma.gv.at/celestial-trading-ltd-TRADOVEST/

26. The criminal proceedings against LENHOFF were opened in Vienna and then handed over to Saarbrücken, Germany. On 5 July 2020, LENHOFF was found dead in his cell in Saarbrücken.
27. According to the client lists in the LENHOFF criminal records, 29,000 victims (mainly European consumers) transferred more than EUR 60 million to LENHOFF´s fraudulent systems Option888, Xmarkets and ZoomTrader, between 2015 and 2018.
28. On 29 January 2019, Gal BARAK, an Israeli citizen, and close business partner of LENHOFF, was arrested in Sofia, Bulgaria. BARAK operated call centers in Sofia, Bulgaria and was also the beneficial owner of the fraud websites (trading platforms) xTraderFX (formerly CryptoPoint), OptionStars/OptionStarsGlobal, Goldenmarkets and Safemarkets.
29. There have been countless criminal complaints from aggrieved Europeans since 2016 as well as countless warnings from supervisory authorities about the fraudulent websites.
30. FMA warned against Capital Force Ltd (Option888) as of November 25, 2017; FMA warned against New Markets S.A (OptionStarsGlobal) on 20 March 2018; FCA warned against GPAY Ltd as CryptoPoint from 14 May 2018; FCA warned against the scam website xtraderfx (operated by Gpay Limited) from 7 July 2018; FCA warned of safe markets a trading style of OptimumCommerce OU from 3 January 2019.

31. According to the customer lists included in the criminal files of GAL BARAK, more than 35,000 victims (95% are European consumers) have transferred for the fraudulent systems of GAL BARAK in total more than EUR 120 million
32. After more than 24 months of criminal investigations, Gal BARAK was found guilty of serious commercial fraud and money laundering by the Criminal District Court of Vienna on 1 September 2020 (122 HV 4/20g).
33. In its judgment the Austrian Criminal Court (Appendix 1) considers it proven that the funds of thousands of innocent European customers have never been used for investments, as promised by the fraud websites or the call center employees.
34. On the contrary, the traceable cash flow show that the funds received were laundered across different layers into shell companies and ended up in the fraudsters' offshore accounts.
35. The indictment and the judgment of Gal BARAK identifies the Dutch **PAYVISION** as the main payment service provider for the fraud websites of LENHOFF and BARAK for the years 2015 to January 2019.
36. According to the Austrian/German law enforcement authorities in the criminal proceedings against BARAK (beneficial owner of fraud systems such as xtraderfx, safemarkets, goldenmarkets, Cryptopoint, OptionStars/OptionStarsGlobal) and LENHOFF (beneficial owner of the fraud systems like xMarkets, Option888, Lottopalace) PAYVISION has processed in the period from autumn 2015 to January 2019 more than EUR **131.2 million** of the victims of these systems (the numbers are based on documentation provided by RUDOLF BOOKER in his interrogations during the criminal proceedings).

Total stolen money processed by PAYVISION2)

	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**

37. The above figures do not include bank wires made by victims on instructions of call center employees of the fraud schemes via illegal payment services providers with bank accounts at various ING subsidiaries.

38. Thousands and thousands of unsuspecting European consumers transferred their life savings to the criminal organisations of LENHOFF and BARAK by means of their credit and debit cards.

39. The financial flows for card processing (acquiring) ran through accounts of specially set up vehicles such as Stichting Trusted Third Party PAYVISION and Stichting Trusted Third Party ACAPTURE with Deutsche Bank accounts and ING bank accounts.

40. PAYVISION transferred the customer funds collected bi-weekly, minus its margin and other handling fees (for example charge-back fees, etc., to the accounts of the scammers) and minus a rolling hold back.

41. PAYVISION also did refunds to the victims on request of the scammers. Minor refunds to the scammers are given to give them trust and to lure them in higher transfers.

42. PAYVISION also acted as one of the payment gateway providers for the fraud websites and referred ING bank accounts for bank wire transfers to the victims.

43. About 20% of the total stolen victims´ money remained with PAYVISION.

Shell companies as exclusive contractual partners of PAYVISION

44. RUDOLF BOOKER attached a list of PAYVISION's onboarded merchants for the different fraudulent websites to his interrogation statement to the Austrian police on 23 May 2019 (Appendix 8) and provided the names of the directors who signed the contracts with PAYVISION (Appendix 2).

Uwe LENHOFF zuzurechnen:

Firmen Geschäftspartner	Verbundene Gesellschaften	Verbundene Plattformen	Offizielle Unterzeichner
PAYIFIC LTD	Keine	www.option888.com www.lottopalace.com www.kulbet.com www.getmyads.com www.zoomtrader.info	Neville Cutajar
HITHCLIFF LTD	Winslet Enterprises ltd	www.option888.com www.zoomtrader.com www.xmarkets.com www.tradeinvest90.com www.tradovest.com	Ralph Stuart Poppleton
CELTIC PAY LTD	4COM Network slr Golden Anchor Ventures ltd	www.option888.com www.zoomtrader.com www.xmarkets.com www.tradeinvest90.com www.tradovest.com	Spas Galev

Gal BARAK zuzurechnen:

Firmen Geschäftspartner	Verbundene Gesellschaften	Verbundene Plattformen	Offizielle Unterzeichner
MARKETS DEVELOPMENT EOOD	Rockarage ltd	www.optionstarsglobal.com	Rumen Gogov
COOL MARKETS OU	Matching Blue Consulting slu	www.goldenmrks.com	Anton Georgiev
OPTIUMCOMMERCE OU	Rockarage ltd	www.safemarkets.com	Kaloyan Nikolaev Mihaylov
MATCHING BLUE CONSULTING SLU	Start Markets ltd	www.goldenmrks.com	Valentin Stoyanov Altanasov
GPAY LTD	Keine	www.xtraderfx.com	Georgi Komisarov

45. All the companies shown as business partners of PAYVISION were pure shell companies, the directors were strawmen, all dealings were done explicitly between BOOKER and GAL BARAK/Uwe Lenhoff as told by GAL BARAK in his interrogation
46. According to this list (Appendix 2) several fraud websites (referred to in the paper as platforms) had one and the same onboarded merchant of PAYVISION, that accepted credit/debit card payments from customers for these platforms.

47. Furthermore, according to this list, there were also "affiliated companies" which subsequently received client funds on the instructions of BARAK [4] and LENHOFF, without having a contractual relationship with PAYVISION. Some of these companies were in offshore countries such as the Marshall Islands, the British Virgin Islands and SAMOA.
48. In accordance with the statements in the criminal case, PAYVISION also transferred client funds to other companies not included in BOOKER´s list on the instructions of LENHOFF and BARAK (see below). These companies, which do not appear, were also based not in Europe, but in countries such as the Marshall Islands, Republic of SAMOA, and the British Virgin Islands.
49. Most of the fraud websites (=platforms) had offshore companies shown on the public websites as the owners of the websites, these owners sown on the websites were different from PAYVISION´s onboarded merchants.
50. For example, New Markets SA, SAMOA, was the owner of the website www. optionstarsglobal.com (Appendix 3) for 2016 to 2018. PAYVISION`s onboarded merchant for this website was the (shell)- company Markets Development EOOD, Bulgaria.
51. The fraud platform www.Xmarkets.com was owned by Capital Force Ltd, Republic of SAMOA (Appendix 4). [5] The contracting party of PAYVISION was the (shell) company Celtic PAY Ltd, London for the processing of the transactions of the customers of the www.xmarkets.com or Hithcliff Ltd, London.
52. The investigations in the criminal proceedings concerning PAYVISION's onboarded merchants revealed the following facts:

    Each of PAYVISION's onboarded merchant was

    - a company that has just been founded or acquired without a history
    - without employees and
    - without business plans, without any accounting records
    - and with exclusively straw men - some of them homeless - as managing directors and UBO
    - without office space and with no website.
    - Bank accounts of the obviously inactive companies were mainly in Sofia, Bulgaria with the same banks.
    - None of these companies had a license as a payment service provider or as a financial service provider.
53. The ownership and operating companies listed on the fraud websites, as well as PAYVISION's merchants, have been changed depending on the extent of the negative ratings on each fraud website.

[4] The term "connected" company is not explained by BOOKER in this context.
[5] The reason for the use of offshore companies is to increase the difficulty for the victims who, after realizing the fraud, try to approach the owners and operators of the fraud websites.

54. If there was a change of the contractual partner of PAYVISION, these ex-contracting companies were usually deleted from the register of company's house within a few months due to lack of documents. Examples are (compare Appendix 5) Hithcliff Ltd and/or Celtic Pay Ltd (Appendix 6).
55. Since 2016, warnings have been issued by European supervisory authorities against many of merchants onboarded by PAYVISION as well as some of the ownership companies listed on the fraud websites.

Close personal trust between BOOKER/ BARAK and LENHOFF

56. The signing managing directors of the official contractors of PAYVISION never had any contact with PAYVISION. This was revealed, for example, by the interrogation of RUMEN Kirilov GOGOV (Appendix 9). GOGOV was the registered managing director of Markets Development EOOD, Sofia, Bulgaria and thus a contractual partner of PAYVISION for Gal BARAK's most successful fraud website.
57. All day-to-day communication for the merchants to GAL BARAK's fraud systems was through a Bulgarian employee of Gal BARAK.
58. The entire day-to-day communication for all merchants of LENHOFF's fraud systems was made by an employee of LENHOFF.
59. BOOKER had direct contact with BARAK and LENHOFF, in these discussions the main issues were discussed, such as new to-be onboarded merchants and terms of new contracts.
60. It should be noted that neither BARAK nor LENHOFF held an official management or ownership function with any of the onboarded merchants or with one of the official ownership companies of the fraud websites.
61. Due to the successful informal cooperation over several years, a formal referral agreement between PAYVISION and LENHOFF was entered into in the summer of 2018, PAYVISION undertook to pay a referral fee for the mediation of further fraud platforms to PAYVISION (Appendix 14).
62. Eavesdropping protocols of phone calls between LENHOFF and BOOKER as well as other documentation in the criminal files confirm the close personal relationship between the two, there were personal invitations to birthday parties, shared ski holidays and common other interests (grey capital market) between the fraudster and the CEO of PAYVISION (Appendix 15).

Money transfers to companies owned by BARAK and LENHOFF without a contractual relationship to PAYVISION

63. The "follow the money approach" applied in the criminal proceedings revealed that PAYVISION transferred EUR 4.4 million from the account of **Stichting Trusted Third Party PAYVISION** (trustee account for the victims' fund received from the victims Issuing banks) to

the Bulgarian bank account of Winslet Enterprises EOOD, Bulgaria (BG67STSA93000024171778) between February 2018 and May 2018. The transfers showed the purpose "profit distribution". PAYVISION had no contractual relationship with this company (owned by Uwe LENHOFF).

64. Furthermore, the investigations revealed that PAYVISION transferred EUR 10.2 million victim's money to NEW MARKETS SA, SAMOA between February 2017 to December 2017 based on a one-sider (signed by a straw man) (Appendix 10).
65. NEW MARKETS SA, SAMOA, was displayed in 2017 as an operating company on the website www. OptionStarsGlobal.com. As of 30 March 2017, the Austrian supervisory authority warned against NEW MARKETS SA (see Appendix 7). PAYVISION had no contractual relationship with this company (owned by Gal BARAK).
66. PAYVISION transferred more than EUR 2 million of client funds to the Bulgarian bank account of Rockerage Ltd. Marshall Islands in the period between 4 October 2017 and 17 April 2019. (Annex 2.1). Rockerage Ltd, a "connected" (?) Company on the BOOKER list, had its registered office in the Marshall Islands and was the operating company for the fraud website www. safemarkets. com.

Business activities of BARAK and LENHOFF

67. In his statement as of 23 May, BOOKER stated (Appendix 8) that binary options were offered on the platforms of BARAK and LENHOFF.
68. Gal Barak claimed in his interrogations and in the main hearing before the criminal court that he was active in the (financial) betting business.
69. According to BOOKER, LENHOFF and BARAK told PAYVISION in March 2018 that they would stop the binary options business - considering the new legislation, which was due to come into force in July 2018. To be compliant, they expressed their intentions to switch from binary options to crypto trading and CFD products. Under these new terms, according to BOOKER, Payvision was able to accept to continue processing for the platforms.
70. In fact, the Vienna Criminal District Court found that neither the fraud websites nor any contracts with the clients mentioned binary options and that there was no mention of binary options in the communication between the clients/victims and the call center employees of BARAK and LENHOFF binary options, but only of investments in financial instruments of various kinds.
71. Regulators also warned against an unlicensed supply of financial services on the various websites owned by BARAK and LENHOFF.
72. None of PAYVISION's onboarded merchants listed in Appendix 2 (the list of merchants and other related companies as provided by BOOKER) had a licence to market or sell financial instruments.

73. On July 24, 2018 PAYVISION signed a new contract with GPAY Ltd, London[6] (merchant according to Appendix 2 for the fraud website www.xtraderfx.com), the contract was signed by BARAK, although he was not a registered managing director of GPAY Ltd [7]. In the contract, new regulations were defined for all websites operated by Gal BARAK (which now operated Cryptotrading according to the contract).
74. The handling fees were agreed with up to 7% in combination with additional m fixed fees for any chargebacks processed and call-off fees in this new contract.[8] The contract also provided for a binding deadline for a minimum monthly volume of EUR 4 million for the next three years (!) for all fraud websites operated by BARAK (!) and enabled PAYVISION to charge the difference between the transaction volume processed in a contract year and the minimum processing obligations (Appendix 12).
75. It is highly unusual that any legally acting merchant would accept such evident exorbitant conditions.

Termination of contracts by PAYVISION

76. After it became public on the media website www.fintelegram.com ("FinTelegram") in summer 2018 that PAYVISION was the main payment service provider for the fraud websites of BARAK and Lenhoff, BOOKER contacted LENHOFF expressing concern[9].
77. As a result, PAYVISION was forced to terminate the merchant contracts for the fraud websites as of 6 and 23 December 2018, subject to a period of 4 weeks, according to the statement by BARAK and LENHOFF due to negative media coverage.
78. BOOKER justified the termination with a customer due diligence conducted by PAYVISION in the 4th quarter, in his interrogation statement of May 23, 2019.
79. The criminal files show that PAYVISION made several SAR´s (suspicious activity reports) to the Dutch FIU during the contract period (mainly after summer 2018). Another confirmation that BOOKER was aware of the illegal nature of their customers' business.
80. Despite the termination of the contracts, telephone calls between BOOKER and LENHOFF and BOOKER and GAL BARAK took place until the end of January 2019.
81. Lenhoff met Rudolf BOOKER as of January 16th in London.
82. BOOKER last spoke to LENHOFF a few days before the arrest of LENHOFF (Appendix15.1. Phone call on 11 January 2019) and apparently tried to obtain information on contractual relationships of previous years to supplement his documents.

[6] At that time, the FCA had already announced on 14 May 2018 that GPAY Ltd had been https://www.fca.org.uk/news/warnings/gpay-limited-trading-cryptopoint and on May 7, 2018, gPAY Ltd as xtraderfx. https://www.fca.org.uk/news/warnings/xtraderfx

[7] In the criminal proceedings, BARAK, the managing director of Gpay registered in the Uk Commercial Register, claimed that Ltd not to be known.

[8] The agreed conditions are extremely high even for the high-risk industry and show on the one hand the dependency relationship of BARAK and on the other hand the power ratio of PAYVISION.

[9] Compare the criminal files.

83. When the notice period expired at the end of January 2019 – a few days before the arrest of LENHOFF and BARAK – PAYVISION retained an amount of EUR 4.3million.
84. The e-mail communication seized during the house searches in Sofia, Bulgaria shows that BARAK was promised an early payment of the withheld amount just a few days before his arrest (Appendix 16).
85. The agreement between BARAK and BOOKER on the disbursement of the money in connection with the cleaning up of the company structures (only European operating companies should appear on the fraud websites) could not be implemented due to the arrest of GAL BARAK on 29 January 2019.
86. To date, PAYVISION has not billed for this withheld amount.
87. BOOKER did not mention these withheld client funds in its first statement of 23 May 2019 to the Austrian law enforcement authorities (Appendix 8) or in its second statement of 15 July 2019 (Appendix 11).
88. In the meantime, PAYVISION for sure is aware that the withheld customer funds are stolen money.
89. In summary, PAYVISION appears to have used its position of trust to withhold stolen client funds without authorization to minimize damage on PAYVISION´s side.

Involvement of PAYVISION in other fraud systems

90. In his statement as of 15 July 2019, BOOKER informed the Austrian Public Prosecutor's Office that PAYVISION had already processed the transactions for the fraud platforms of NOVOX Capital Ltd, Cyprus (Optionsbit.com, Optionsxp.com, Optionsmerchants.com) 2013, 2014 and 2015 (Interrogation statement of Booker as of July 2019: Appendix 11).
91. PAYVISION also processed the credit and debit card payments for the fraud website Binex (www.binex.ru). In an e-mail communication seized during the house search at the end of January 2019, the fraud websites that PAYVISION used for credit/debit card transactions are listed by the people of GAL BARAK. (Appendix 13). The fraud platform BINEX was closed in summer 2018. The activities of this illegal website are investigated by police authorities from different parts of the world. One of BINEX's call centers in Kiev was already searched by the Ukrainian cyber police in August 2018. The 60 employees of the call center had been able to persuade more than 15,000 customers in Russia, Ukraine, and other countries (mostly Eastern Europe) to transfer in various (fictitious) financial instruments in tens of millions of dollars in just a few months[10]. The fraud and the raid go a lot of media attention.
92. PAYVISION has also handled credit/debit card orders for the fraudulent website www.24option.com, operated by Roedeler Ltd (Appendix 21). Criminal proceedings are underway in Cologne, Germany against this long-standing fraud system. The UK and Cypriot regulators banned Rodeler Ltd from operating in June 2020.
93. PAYVISION also processed credit/debit card payments for the fraudulent website AlgoTechs/BEALGO in the years 2017 – 2019 (Appendix 20).

[10] https://www.trafikmarket.com/2019/the-raid-of-the-ukrainian-cyberpolice/

94. PAYVISION also processed credit/debit card payments for the fraudulent website EASYTRADE, another binary option website operated by GAL BARAK.

Bank transfers to ING bank accounts of legal and illegal payment service providers for BARAK and LENHOFF fraud system

95. Apparently, BOOKER also arranged bank accounts for illegal payment service providers used by BARAK`s and LENHOFF´s at various ING banks.
96. MoneyNetInt Ltd, London – an e-money and payment institution licensed by the Financial Conduct Authority (FCA) (reference No. 900190)) – had an account with ING Bank "L'ski Spéka Akcyjna" (PL73105000861000009030701412). The account was used for deposits of the victims of the fraudulent website www.optionstarsglobal.com. (Appendix 17.1)
97. As early as July 2016, the Times of Israel reported on MoneyNetInt Ltd's involvement in binary options fraud. In spring 2017, the Polish Financial Supervisory Authority ("KNF") issued a warning about the activities of MoneyNetInLtd (Appendix 17.2).
98. Leonsky Ltd in Madrid, Spain, an illegal financial agent and had an account with ING N.V. SUCURSAL EN ESPAA (ES17 1465 0100 9519 0060 4045). This account has been used for several fraud schemes (including scams of GAL BARAK). (Appendix 18)
99. STICHTING ESCROW ICEPAY (Lottopalace) (ICEPAY B.V., Amsterdam) had an account with ING Bank Frankfurt (DE88 5002 1000 0010 1193 45) and acted as an illegal payment service provider, the company was used to transfer stolen money for the fraud platform of LENHOFF. (Appendix 19).
100. For Stichting WST Capital Ltd, the US CFTC (Commodity Futures Commission) already issued a warning on April 25, 2017 [11] about this illegal Payment service provider, pointing out that the company is involved in the payment processing of binary options. The Stichting WST Capital Ltd, had an account with ING Bank NL75INGB0006984998, and was used to transfer stolen money to the beneficial owners of the fraud system AlgoTechs / BEALGO (compare in detail Appendix 19) 2018 and 2019.

[11] https://cftc.gov/node/221151

PAYVISION's involvement in US legal cases

Beyond Wealth vs T1 Payments and PAYVISION

101. On July 28, 2020, the dispute (2:20-cv-01405-JCM-VCF) between Beyond Wealth PTE LLC, UTAH ("Beyond Wealth") – a US multilevel marketing (MLM) company – and T1 Payments LLC – a Payment Facilitator, in respect of the unauthorized retention of more than USD 4 million in course of the termination of the credit card processing service contract was opened in the United States District Court in Nevada. [12]

102. By written document of 24. 08. 2020 of Beyond Wealth, PAYVISION B. V. Amsterdam ("PAYVISION") was included in the action as a counterclaim defendant.

103. Beyond Wealth claimed that T1 Payments LLC ("T1 Payments") in its main capacity as a Payment Facilitator, had lured them in May 2020 into a merchant agreement for the processing of credit/debit cards by credibly assuring that they were a registered Payment Facilitator.

104. Only weeks later, the contractual relationship was terminated and Beyond Wealth found that T1 Payments was not a registered Payment Facilitator and that T1 Payments' ability to process Beyond Wealth's transactions depended on the Dutch PAYVISION (Counterclaim-Defendant) and the breach of legal obligations under the rules of the credit card companies.

105. In summary, Beyond Wealth claims that T1Payments was guilty of committing wire fraud and money laundering in cooperation with PAYVISION.[13]

106. The Beyond Wealth lawsuit describes in detail how PAYVISION processed all Beyond Wealth transactions by opening a sub-account for Beyond Wealth under the master merchant account of T1 Payments. There was no contract between Beyond Wealth and Payvision, although T1 Payments was not a Mastercard/VISA-approved/registered Payment Facilitator. T1 Payments had a merchant account under his name at PAYVISION and PAYVISION deposited the client funds from the processing activity to the T1 Payments bank account at Atlanta Bank in Nevada.

107. In addition, Beyond Wealth claims that while T1 Payments is a US company based in Nevada, the British subsidiaries of T1 Payments (T1 UK and/or TGlobal) had

[12] A payment facilitator is in direct contact with the trader and manages the merchant account with the acquirer on behalf of the subdealers. Billing via a payment intermediary is usually suitable for young companies with even smaller sales.

[13] Sometimes acquirers may enter contracts with third-party organizations to provide merchants with card associations (such third-party organizations may refer to goods in the Visa rules as "third-party agents" and in the Mastercard rules, and hereinafter referred to as "service providers"). A service provider must run only the type of program service for which it is registered and must be registered with the cards. association before a purchaser or merchant stake its services (see e.B. Mastercard Rule 7.2 (Program and Performance of the Program Service).

to be contractors of Beyond Wealth to enable T1 Payments to carry out the credit card transactions.

108. Beyond Wealth LLC was also instructed by T1 Payments to set up a UK Beyond Wealth to enable Beyond Wealth's business with UK T1 Payments. Although the Customer Payment Processing Agreement (CPPA) was a direct agreement between the US companies and although transactions were to be processed related to US Beyond Wealth customers, the transactions were submitted under the names of the British shell companies.

109. T1 Payments oversaw setting up UK Beyond Wealth, or it was obvious to Beyond Wealth that T1 Payments, in conjunction with PAYVISION, had its own start-up service. The establishment of British companies for a fee of USD 250 was a condition for the conclusion of a merchant agreement with T1 Payments.

110. It was only afterwards that Beyond Wealth understood that these shell companies were needed for PAYVISION – a European payment service provider – to enter contracts with these British companies (T1UK or TGlobal) for the settlement of the transactions of the US company Beyond Wealth.

111. The procedure applied by T1 Payments, which was a massive breach of the legal rules applicable to PAYVISION [14] , and to the regional requirements of credit card companies, became clear only after Beyond Wealth learned that T1 Payments did not have an upright registration as a payment facilitator and PAYVISION – a European payment service provider – accepted the transactions for processing

112. According to the British company register, T1UK and TGLOBAL were officially inactive companies that only accounted for GBP 1 in assets. **Red flags which were willfully ignored by PAYVISION when concluding the contract.**

113. In the claim against T1 Payments, Beyond Wealth alleges that T1 Payments conspired with PAYVISION to give the impression that the merchants were in the UK resp. the EU and therefor PAYVISION was eligible for acceptance of the dealership agreement.

114. The credit card companies clearly prohibited T1 Payments from opening Payments Facilitator sub-accounts for Beyond Wealth with a licensee.

115. Beyond Wealth states in its lawsuit that the procedure used by T1 Payments to establish British shell companies is described as a standard procedure in T1 Payment's onboarding instructions. In particular, the materials offer the procurement of an “EU Corp".

116. Beyond Wealth claimed in the lawsuit that T1 Payments used the same illegal structure to all its high-risk merchants and that all these illegal dealership agreements have been processed through PAYVISION for years.

117. A review of the US legal claims register(www.pacer.gov) reveals that there have been dozens of similar lawsuits against T1 Payments in previous years, which

[14] As a European payment service provider, PAYVISION is legally only allowed to conclude and carry out transactions with companies in the EEA. the Mastercard Rule 5.1 (p. 59) in accordance with the corresponding VISA regulations, that acquirers and dealers in Same jurisdiction.

apparently did not deter PAYVISION from offering payment processing services to that company since 2015 and 2016.

118. In PAYVISION's statement filed with the US court on 9 November 2020 (document 103-2), PAYVISION confirmed again that PAYVISION is under Dutch law only allowed to accept European merchants.

119. The Chief Risk Officer of PAYVISION, Maria Alida Johana Ruijters – Terprstra, confirmed in her affidavit that PAYVISION has never offered services in the state of Nevada, since PAYVISION may legally operate exclusively in the EEA area.

120. The documents also submitted by PAYVISION show that PAYVISION has maintained a close relationship with T1 Payments and its British shell companies for many years.

121. To reinforce the statement submitted, PAYVISION provided as evidence an extract of internal customer documents displaying the British T1 Payments companies as customers.

122. PAYVISION did not explain why all transactions performed on these internal documents were denominated in USD.

PAYVISION s Engagement at ALLIED WALLET

123. In its claim as of 23 May 2019 (2:19-cv-04355-SVW-E), the US FTC (Federal Trade Commission) allege Allied Wallet Inc, Nevada, Allied Wallet Ltd, UK, GT Bill LLC, Nevada, GT Bill Ltd, UK, as well as the beneficial owners Ahmad Khawaja, also known as Andy Khawaja, and Mohammad Diab, that these companies and their beneficial owners have been knowingly processing payments for numerous companies engaged in fraudulent activities since at least 2012.[15]

124. Allied UK and Allied Inc are registered as Payment Facilitators with Mastercard and VISA.

125. FTC alleged that Allied Wallet contributed to the fraud of pyramid schemes, various ponzi schemes, and other fraudulent companies by giving Allied Wallet access to the ability to receive credit and debit card payments.

126. The allegation is that Allied Wallet intentionally closed merchant contracts with false information regarding the business to circumvent the requirements of the credit card companies for customer due diligence and transaction monitoring together with their fraudulent resellers, Thomas Wells, and its company Priority Payout.

127. Another allegation by the FTC is that the creation and use of European shell companies to process payments of U.S. merchants in Europe with European payment service providers such as Wirecard or PAYVISION, rather than in the U.S., has allowed Allied fraudulent U.S. merchants to evade the generally stricter regulatory framework of the U.S. financial system.

128. The incorporation of British shell companies to set up high-risk non-EU merchants was a standard procedure at Allied Wallet, the FTC alleges. The need to

[15] Among these customers of the Allied Wallet are companies are also, which have already been the target of various law enforcement actions by the FTC, the Securities Exchange Commission ("SEC") and other law enforcement agencies.

procure an "EU Corp" in addition to the actual form of the merchant was even specified in the internal checklists of Allied Wallet. As a rule, all these foreign shell companies had no employees, no premises, only straw men as managing directors and owners and were wealthless.

129. According to the court documents, both PAYVISION and Wirecard, the now insolvent German fintech, served for years as acquirers for Allied Wallet merchants and carried out the transactions of US high-risk traders.

Information from the FINCENFILES

130. According to information from the FinCen leaks, for years, PAYVISION was on the radar of FinCEN and several American banks for processing suspicious transactions by clients who should not have ended up in the traditional banking cycle. For years, the company served high-risk customers from the porn, gambling, and other sectors, which are often rejected by traditional banks because they are vulnerable to fraud.

131. A deliberate and conspicuous division of large transactions could be established for no apparent reason. In just a few months, tens of millions were transferred to PAYVISION`s customers like the site Pornhub.[16]

[16] According to the report Het Financieele Dagblad of xx

Qualification of non-compliance with legal and contractual regulations

Dutch legislation

132. The purpose of the European money laundering directives, the relevant national legislation, and the contractual obligations of credit card companies to their licensees is **to protect the traditional financial system from use by criminal and terrorist organisations.**

133. In accordance with the Payment Services Directive PSD2, as enshrined in the Dutch Civil Code and the Financial Supervision Act (Wet op[17]*het financieel toezicht – Wft*), the Dutch payment institutions must comply with the Anti-Money Laundering and Terrorist Financing Act (Wwft) and the Sanctions Act 1977 as well as the Supervisory Ordinance under the Sanctions Act 1977 (Sw). The Dutch Ministry of Finance issued the "General Guidelines on the Anti-Money Laundering and Terrorist Financing Act (Wwft) and the Sanctions Act (Sw)". As of December 2019, DNB has issued guidelines clarifying the various obligations under the Wwft and the Sw and has provided instruments to meet these obligations.[18]

134. The guidelines published by the Dutch Ministry of Finance and De Nederlandsche Bank (DNB) on the Anti-Money Laundering, Terrorist Financing (Wwft) Act and the Sanctions Act **underline the call for Dutch financial institutions to take responsibility for the detection of financial and economic crime**. Integrity is cited as a prerequisite for a sound financial system and the supervision of the DNB deals with the integrity of Dutch financial institutions. According to the guidelines, the integrity of financial institutions is one of the pillars of trust and therefore a prerequisite for the proper functioning of the institutions. Section 3.10 and Section 3.17 of the Financial Supervision Act contain the legal requirements for monitoring ethical operational management. The most important condition is that institutions must avoid participating in schemes that violate the law or are considered inappropriate by society, and that they must protect the integrity of their operational management. According to the Guidelines of the DNB (published in December 2019), ethical operational management of financial institutions must be ensured; it is therefore important that the institutions know with whom they are doing business. Wft and Wwft therefore require institutions to operate an appropriate Customer Due Diligence (CDD) system to know their customers and avoid business relationships with individuals who could damage trust in the institution. The main objective of Wft and Wwft is that the institution knows with whom it is doing business, the activity carried out by the company and the continuous monitoring of the business relationship (and reporting all unusual transactions) - to an extent to the risk.

135. It is important to ensure that criminals are prevented from laundering the proceeds of their crimes, that terrorists and sanctioned entities are unable to obtain

[17] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en
[18] https://www.toezicht.dnb.nl/en/binaries/51-212353.pdf

the financial resources to maintain their activities and launch attacks, and that individuals are unable to profit from corrupt practices.

136. Financial institutions serve as the first line of defense against illegal financial transactions in today's fast-moving, networked financial network. Under EU and Dutch law, these institutions must design and implement strategies and systems to prevent and detect illegal financial transactions.

Rules of card companies

137. Licensees of credit card companies agree to comply with all rules that card companies prescribe for their partners– including all acquirers and payment service providers, payment facilitators, etc.

138. The main purpose of the extensive regulations imposed by credit card companies, like the legal provisions, is to prevent fraud, to increase the transparency of payment flows and to increase compliance with anti-money laundering laws, thereby reducing the overall risk to the financial system.

139. Prior to onboarding a new trader (also known as "Merchant") Mastercard and VISA require their license companies to identify the ultimate beneficial owner (UBO) and to have a detailed review of the purpose and nature of the business relationship. The partner companies are also obliged to check the source of the processed financial flows and to continuously monitor the ongoing business relationship.

140. The VISA regulations additionally require the following documents of the trader from the acquirer during the onboarding phase:

- Legal documents
- Description of business activities
- Accounting reports and business plans
- Reports from credit rating agencies, etc.
- Income tax returns
- A physical inspection of the premises of the potential contracting entity
- a review of the website
- and a thorough OSINT[19] analysis

141. Both Mastercard and VISA provide for high-risk merchants particularly high requirements in terms of customer due diligence and monitoring of ongoing transactions.

142. Credit card companies also impose geographic restrictions on their licensees. Licensees may only offer and provide their transaction services to companies located within "within the authorised "area of use"*.

[19] Open-Source Intelligence

Non-compliance with legal and contractual obligations by PAYVISION

143. In summary, PAYVISION – as a licensed payment service provider and licensee of Mastercard/VISA – **is required by law and contractual law to install internal systems and procedures to avoid the use of the financial system for money laundering and terrorist financing and to report any suspected money laundering and/or financing of terrorism in accordance with the law**.

144. Based on PAYVISION's activities set out above, it is obvious that PAYVISION has willfully ignored all legal requirements and rules designed to prevent the use of the financial system for fraudulent criminal organisations to achieve higher transaction volumes, revenues, and profits.

145. It was only through this deliberate, knowing, and willful ignorance that convicted fraudsters such as BARAK were able to steal consumers' life savings on a gigantic scale for years.

146. If PAYVISION had conducted due diligence as required by law, BARAK and LENHOFF would not have been able to use the reputation of a financial service provider licensed in the Netherlands to carry out their criminal activities in Europe.

147. If PAYVSISION had done a proper transaction monitoring transaction as required by law, PAYVISION would have noticed at the beginning of the customer relationship (autumn 2015) that BARAK and LENHOFF were carrying out fraud and this would have resulted in the fraud of BARAK and LENHOFF ending much earlier and thousands of European consumers would not have lost their life savings.

148. The 273 SARS notifications made by BOOKER according to his statement to the Austrian authorities as of 23 May 2019, which PAYVISION sent to the Dutch FIU, clearly shows that BOOKER had sufficient evidence of fraudulent activity.

149. With the 273 SARS reports submitted, a targeted attempt was made to cover up the involvement of PAYVISION in criminal activity.

150. The high number of SARS reports clearly shows that BOOKER knew what was going on or had sufficient evidence of fraudulent activity and that he knew that he should have ended the business relationship immediately according to the Dutch law.

151. A high volume of sales and the presentation of a high growth has obviously been more important for the founders and board members of PAYVISION since the foundation of the company (2002) than compliance with legal and ethical regulations.

152. The procedure of PAYVISION was also motivated by the fact that the main shareholder and CEO BOOKER wanted to sell his shares in the company PAYVISION to ING Group N.V. at an extremely high valuation in March 2018.

153. PAYVSISION has demonstrably ignored all red flags, including

- public warnings from European supervisory authorities on merchants and/or fraud websites
- Massive charge-back (rebooking) requests from victims,
- fraud messages from victims
- raids took place as early as summer 2018.

- Constantly changing merchants, all of which were newly formed shell companies, which had no financial figures, no internet presence, no employees, no premises and whose directors and owners were pure straw men (some of them without residence)
- that the fraud websites whose transactions were processed identified as operating and ownership companies established in SAMOA or Marshall Islands.
- The fact that the actual beneficial owners of the fraud websites did not sign any of PAYVISION`s merchants

154. There was a close personal relationship between the actual beneficial owners of the fraud websites and the founder and CEO of PAYVISION, which resulted in BOOKER apparently repeatedly overruling PAYVISION´s compliance department.

155. Without this ignorance of any legal compliance requirements, it is inconceivable that

- Millions of customer funds from PAYVISION's bank account were transferred to companies with which PAYVISION had no contractual relationship, on the instructions of GAL BARAK (New Markets SA, Republic of SAMOA) and LENHOFF (Winslet Enterprises EOOD) for the purpose of "profit distribution".
- Contracts were concluded with straw men (some of them homeless) with which no one from PAYVISION had ever spoken.

156. The fact that over the years hundreds of fraud complaints were received by PAYVISION regarding the fraud systems of BARAK and LENHOFF and yet BOOKER entered into a referral agreement with LENHOFF in the summer of 2018 for the referral of further fraud platforms indicates the unscrupulousness of BOOKER.

ING Acquisition of PAYVISION by ING in March 2018

157. Any commercial and legal due diligence in course of the acquisition of PAYVISION by one of the largest banking institutions in the Netherlands, ING Groep NV in March 2018, must have revealed PAYVISION's high-risk business activities.

158. ING Groep BV was in the middle of a criminal investigation for money laundering during the period of the acquisition of PAYVSISON (2017), so ING must have been aware of the explosive use of the traditional financial system by criminal organizations.

159. Nevertheless, ING Groep NV accepted a valuation of EUR 360 million for the shady business of PAYVISION.

160. The importance of the touch of seriousness and credibility for the fraud websites, with a subsidiary of ING offering the processing of credit and debit card transactions for these scam websites, PAYVISION was paid by the fraud websites in higher margins and long contract retention periods.

.

INTEGRITY and TRUST

161. Integrity of financial services companies is cited as a prerequisite for a sound and secure global financial system. According to the guidelines of the Dutch Ministry of Finance and the DNB, the integrity of financial institutions is one of the pillars of trust and therefore a prerequisite for the proper functioning of the institutions. Section 3.10 and Section 3.17 of the Dutch Financial Supervision Act contain the legal requirements for the monitoring of ethical operational management. The most important condition is that institutions must avoid participating in actions that violate the law or are considered inappropriate by society, and that they must protect the integrity of their operational management.

Summary

162. We are deeply convinced that PAYVISION knowingly, willingly and without respecting all legal and contractual obligations contributed substantially to the fraud of various international criminal organisations over many years.

163. The contribution of PAYVISION, its founders and managers, has led to the loss of the life savings of thousands of European consumers who have also lost their confidence in the European financial system. PAYVISION's actions and procedures are contrary to all ethical standards set by the authorities in the Netherlands and the European Union.

164. The lack of conscience, ruthlessness, and willfulness of the board of PAYVISION and its multiple involvement in similar fraud structures (cf. T1Payments (point 88-108) and Allied Wallet (point 109-115) clearly indicate that BOOKER and his colleagues have aware of the fraud that took place against many European consumers and that there was a clear will to contribute.

Victims represented by EFRI

165. EFRI represents 325 (mainly) European consumers who have transferred more than EUR 11,2 Mio of their life savings to the boiler room scams operated by Gal BARAK and Uwe Lenhoff.

166. representing and on behalf of the aggrieved parties we represent, we join the criminal proceedings against the management board of PAYVISION as private parties or file an application for adhesion.

Yours sincerely

Elfriede Sixt Nigel Kimberley

EFRI INITIATIVE

Non-Government Organization to fight Cybercrime

Verein zur Bekämpfung von Cyberkriminalität gegen Kleinanleger und Verbraucher

Vienna •Austria • Reg No 1493630560 • www.efri.io • email office@efri.io
Address: Eichenstrasse 28, 2102 Bisamberg, Austria