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

Openbaar Ministerie Amsterdam
IJdok 163
1013 MM Amsterdam
Netherlands

Vienna, August 2021

Reference: Criminal complaint: Rudolf BOOKER, Gijs OP DE WEEGH, Cheng LIEM LI former members of the board of PAYVISION Holding B.V. and PAYVISION B.V. Amsterdam for complicity in serious commercial fraud and money laundering.

General

1. The *European Funds Recovery Initiative (EFRI)* is a victim protection organization in line with 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 mentally the crime experienced, 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 of 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 extent of fraud experienced by thousands of European consumers - mainly elderly people - by the various types of investment fraud and boiler room scams is huge at the moment and amounts to about 1 bn EUR every month.
4. Innocent European consumers rely on the promises of cybercriminals about advantageous investment possibilities, transfer their life savings, and, after months, realize that they have become the victims of unscrupulous international criminal organizations.
5. 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, and mental and physical consequences.

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

6. 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 system above all is the cooperation with regulated or licensed European payment service providers.
7. These European payment service providers are essential to the intake of the victims' money, laundering it, and, finally, transferring the money to offshore bank accounts under the control of the scammers.
8. It is only through cooperation with regulated payment service providers that the scam websites get the possibility to convince thousands of European consumers to transfer their life savings to the online scam websites.

Background of PAYVISION B.V.

9. Based on the records of the victims, as well as based on the findings in criminal and civil proceedings 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").
10. 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.
11. 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.
12. 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.
13. Furthermore, the special vehicles **Stichting Trusted Third Party PAYVISION** and **Stichting Trusted Third Party ACAPTURE** are part of the group.
14. 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 agreed to acquire a 75% stake in PAYVISION, Amsterdam. [1] The agreed purchase price amounted to EUR 380 million. The achieved valuation was 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.
15. 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 to Mr. BOOKER and his collegues.
16. As of the end of April 2020, Rudolf BOOKER, Gijs op de WEEGH, and Cheng LIEM left their board positions.
17. The annual report of ING as of 31 December 2020 (published in March 2021), page 65, reports 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

[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

PAYVISION (porn and gambling is mentioned) 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

18. PAYVISION is a payment service company licensed and supervised as such by De Nederlandsche Bank (DNB) in accordance with the European Payment Services Directive (PSD2).
19. In addition, PAYVISION is a licensee and a member of credit card companies (MasterCard/VISA), enabling PAYVISION to act as an acquirer for both the card-present and the card-not-present environment in Europe.
20. PAYVISION enabled online merchants to accept credit card and debit card payments from their customers by collecting and receiving the settlements on bank accounts run by PAYVISION for the merchants (merchant accounts) and subsequently transferring the remittance to the merchants.[2]
21. PAYVISION, like WIRECARD, the now insolvent German FinTech, has concentrated on the business with high-risk merchants from the start-up[3] due to the higher achievable margins,
22. 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), and cannabis.
23. In addition, however, PAYVISION has also participated as an accomplice in fraud schemes of transnational criminal organizations 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 Card Brand rules.
24. In addition PAYVISION has 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).
25. Summarizing we are convinced that PAYVISION was knowingly and willingly complicit to several transnational criminal organizations and enabled scammers to steal the life savings of tens of thousands of innocent consumers over the years, for evidence pls refer to:

- Information from the criminal facts of LENHOFF/BARAK at the Criminal District Court of Vienna (730 Js 1545/18).

[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.

- Statements of the ex-CEO of the company Rudolf BOOKER in the above criminal files.
- Deposit confirmations (bank transfers and credit card billing) for other scams like 24option
- Information from public records of legal cases pending in the United States involving PAYVISION.

PAYVISION and Booker as accomplices of Gal BARAK and Uwe LENHOFF

26. On 25 January 2019, the Austrian and German law enforcement authorities in a joint effort 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 scam websites (trading platforms): Option888, ZoomTrader, ZoomTrader, Tradovest, Lottopalace, and Xmarkets. Since 2016, there have been countless criminal complaints to the European criminal authorities regarding these scam websites.
27. The criminal proceedings against Lenhoff were opened in Vienna and then handed over to Saarbrücken. On 5 July 2020, Lenhoff was found dead in his cell in Saarbrücken.
28. According to the victims' lists in the LENHOFF criminal records, 29,000 victims (mainly European consumers) transferred more than EUR 60 million (figures will be updated soon) to shell companies owned by Lenhoff for fictitious investments offered and marketed via the scam websites Option888, Xmarkets, and ZoomTrader between 2015 and 2018.
29. On 29 January 2019, Gal Barak, an Israeli citizen and close business partner of Lenhoff, was arrested in Sofia, Bulgaria. Barak run boiler rooms in Sofia, Bulgaria, and was also the beneficial owner of the scam websites (trading platforms) xTraderFX (formerly CryptoPoint), OptionStars/OptionStarsGlobal, Goldenmarkets, and Safemarkets. Here, too, have been countless criminal complaints from aggrieved Europeans since 2016.
30. According to the customer lists included in the criminal files of GAL BARAK, more than 35,000 victims (95% are European consumers) have transferred more than EUR 120 million for the fraudulent systems of GAL BARAK.
31. 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).
32. The Austrian Criminal Court (Appendix 1) considers it proven that the funds of the thousands of innocent European customers were never used for investments, as promised by the scam websites or the boiler room employees.
33. On the contrary, the traceable cash flow shows that the funds received were laundered across different layers into shell companies and ended up in the fraudsters' offshore accounts.
34. The indictment and the verdict for Gal BARAK, identify the Dutch PAYVISION as the main payment service provider for the scam websites of Lenhoff and Barak for the years 2015 up to January 2019.
35. According to the Austrian/German law enforcement authorities in the criminal proceedings against BARAK (economical owner of xtraderfx (GPAY ltd), safemarkets, goldenmarkets, Optionstars/Optionstarsglobal (Markets Development)) and LENHOFF (economical owner of the fraud websites xMarkets, Option888, Lottopalace), PAYVISION has processed in the

period from autumn 2015 to January 2019 more than EUR **131.2 million** in credit and debit cards payments of Barak´s and Lenhoff`s victims.

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**

36. Thousands and thousands of trustful European consumers transferred their life savings to the criminal organizations of LENHOFF and BARAK using their credit and debit cards. The sham companies of LENHOFF (Payific ltd, Hithcliff ltd, Celtic pay ltd) and BARAK (Cool Markets, Optiumcommerce, Matching Blue Consulting, Gpay ltd) got onboarded by PAYVISION as merchants.

37. 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 through mainly Deutsche Bank merchant accounts.

38. Payvision transferred the customer funds collected bi-weekly, minus its margin and other handling fees (e.g. . B charge-back fees, etc.,) as well as the rolling reserves to the accounts of the fraudsters.

39. The above figures do not include the bank wires made from victims on the instruction of the boiler room employees to money mules at ING and Deutsche Bank accounts.

Shell companies as exclusive contractual partners of PAYVISION

40. Rudolf Booker attached a list of PAYVISION's contracting parties (merchants) for the scam websites to his written statement to the Austrian law enforcement agency on 23 May 2019 (Appendix 8) and also provided the names of the directors who signed the contracts with PAYVISION (Appendix 2).
41. According to the list provided (Appendix 2) several scam websites (referred to in the paper as platforms) used the same merchant. The companies described by Booker as contracting companies (merchants) were all located in a European country.
42. According to this list, there were "affiliated companies" which subsequently received the customer funds on the instructions of BARAK [4]and LENHOFF, without having a contractual

[4] The term "connected" company is not explained by BOOKER in this context.

relationship with PAYVISION. Some of these companies were located in offshore countries such as the Marshall Islands, the British Virgin Islands, and the Republic of SAMOA.

43. In his statement Booker missed disclosing transfers made to companies under the direct influence of Uwe Lenhoff and Gal BARAK. Also, these non-disclosed transfers were done to companies, not based in Europe.
44. The majority of the scam websites (=platforms) had offshore companies as official owners that did not coincide with the merchants onboarded by PAYVISION.
45. For example, New Markets SA, Republic of SAMOA, was the official owner of the website www.optionstarsglobal.com(Appendix 3) from 2016 to 2018. The merchant for the website www.optionstarsglobal.com was Markets Development EOOD, Bulgaria.
46. The fraud platform www.Xmarkets.com was owned by Capital Force Ltd, Republic of SAMOA (Appendix 4). [5] The merchant onboarded by PAYVISION was Celtic PAY Ltd, London for the processing of the transactions of the www.xmarkets.com resp. Hithcliff Ltd, London (as explained above, several merchants were used to processing the transactions of one website).
47. The investigations in the criminal proceedings concerning PAYVISION´s merchants revealed the following facts:

    Each of PAYVISION´s onboarded merchants was:

    - a company that has just been founded or acquired without a history,
    - without employees and
    - without business plans, without accounting
    - and with straw men - some of them homeless - as managing directors and beneficial owners
    - no office space and no internet presence
    - Bank accounts of the 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.
    - None of these companies had ever a license to offer resp. to market binary options to retail customers.
    - The operating companies displayed on the scam websites, as well as the merchants, have been changed depending on the extent of the negative rating resp. in dependence on the number of warnings on the specific scam website.
    - If a new merchant got onboarded, the ex-contracting companies were usually deleted from the register of Companies house within a few months due to a lack of documents. Examples are (compare Appendix 5) Hithcliff Ltd and/or Celtic Pay Ltd (Appendix 6).
    - Since 2016, warnings have been issued by European supervisory authorities against the scam websites operated by Lenhoff and Barak and serviced by PAYVISION.

Close personal trust between BOOKER/ BARAK and LENHOFF

48. The managing directors of the onboarded merchants had no contact with PAYVISION. This was revealed, for example, in the interrogation of RUMEN Kirilov GOGOV (Appendix 9). GOGOV

[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 scam websites.

was the registered managing director of Markets Development EOOD, Sofia, Bulgaria, and thus a contractual partner of PAYVISION for Gal BARAK's most successful scam website OptionStarsGlobal.

49. All day-to-day communication for the parties to GAL BARAK's fraud systems was through a Bulgarian employee of Gal BARAK (Boyan @Maevar).
50. The entire day-to-day communication for the contracting companies of LENHOFF's fraud systems was made by an employee of LENHOFF.
51. BOOKER had direct contact with BARAK and LENHOFF, in these discussions the main issues were discussed, such as new merchants to be set up and onboarded and terms of new contracts as well as in case too many chargeback and fraud complaints got raised by victims.
52. It should be noted that neither BARAK nor LENHOFF held an official management or ownership function with any of the merchants or with one of the official owners of the scam websites.
53. Due to evidence of the successful cooperation, a commission agreement between PAYVISION and LENHOFF was established in July 2018, PAYVISION undertook to pay a commission for the mediation of further fraud platforms to PAYVISION (Appendix 14).
54. Interception logs of phone calls between LENHOFF and BOOKER and other records in the criminal case confirm the close personal relationship between the two. 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).

Payments to companies owned by BARAK and LENHOFF without a contractual relationship

55. The financial investigations in the criminal proceedings revealed that PAYVISION transferred EUR 4.4 million from the merchant account to the Bulgarian bank account of Winslet Enterprises EOOD, Bulgaria (BG67STSA93000024171778) between February 2018 and May 2018. The transfers showed the purpose of profit distribution. PAYVISION had no contractual relationship with this company.
56. Furthermore, the financial investigations revealed that PAYVISION transferred EUR 15,3 million to a bank account of NEW MARKETS SA, Republic SAMOA from February 2017 to June 2018 based on a scrap of paper (signed by GOGOV) (Appendix 10). NEW MARKETS SA, SAMOA, was founded in 2017 and was displayed on the website www. OptionStarsGlobal.com as the operating company. 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 except.
57. PAYVISION transferred more than EUR 2 million of client funds to the Bulgarian bank account of Rockerage Ltd. in the period 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 scam website www. safemarkets. com. PAYVISION had no contractual relationship with this company

Business activities of BARAK and LENHOFF

58. In Booker´s statement to the Austrian law enforcement agency as of 23 May 2019 (Appendix 8), he confirmed that he was aware that BARAK and LENHOFF offered and sold binary options on the scam websites serviced by PAYVISION.
59. Gal Barak claimed in his interrogations and the main hearing before the criminal court that he was active in the betting business.
60. According to BOOKER, LENHOFF and BARAK informed PAYVISION in March 2018 that they would stop the binary options business - in light of 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 Barak and Lenhoff.
61. In fact, the Vienna Criminal District Court found that neither the scam websites nor the papers exchanged with the victims ever mentioned binary options. Also, the criminal investigations found that there was no mention of binary options in the communication between the clients/victims and the boiler room employees of BARAK and LENHOFF at all. Only investments in financial instruments of various kinds were discussed, offered, and sold.
62. Since 2016 supervisory authorities have issued warnings against the unlicensed supply of financial services on the various websites owned by BARAK and LENHOFF
63. None of PAYVISION´s merchants listed in Appendix 2 (the list of merchants provided by BOOKER) had a license to market or sell financial instruments.
64. On July 24, 2018, PAYVISION signed a new contract with GPAY Ltd, London[6] (merchant according to Appendix 2 for the scam website www.xtraderfx.com). GAL BARAK, signed this contract, although he was not the registered managing director of GPAY Ltd. [7] In the contract, new adverse conditions were laid down for all scam websites operated by GAL BARAK.
65. In this new contract the handling fees were agreed at 7% in combination with additional fixed fees for fee refunds, refund fees, and call-off fees in this new contract.[8] The contract also provided for a binding period for a minimum monthly volume of EUR 4 million for the next three years (!) for all scam websites operated by BARAK (!) and enabled PAYVISION to charge the companies concerned the difference between the aggregated volume processed in a contract year and the minimum processing obligations (Appendix 12).

Termination of contracts by PAYVISION

66. After it became published on the website www.fintelegram.com ("FinTelegram") in the summer of 2018 that PAYVISION was the main payment service provider for the scam websites of BARAK and Lenhoff, BOOKER contacted LENHOFF with concern.

[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 very 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.

67. The files show that PAYVISION filed a substantial number of SARs beginning with summer of 2018. This indicates that PAYVISION and BOOKER were well aware of the illegal nature of their customers' business.
68. Intercepted phone calls prove the close relationship between BOOKER and LENHOFF (Appendix 15.1. and Appendix 15.2)
69. PAYVISION was forced to terminate the merchant contracts for the scam websites as of 6 and 23 December 2018, subject to a period of 4 weeks, according to the statements by Barak and Lenhoff due to negative media coverage.
70. BOOKER justified the termination with an adverse customer due diligence conducted by PAYVISION in the 4th quarter, in its statement to the Austrian law enforcement agency as of May 23, 2019.
71. Despite the termination of the contracts, telephone calls between BOOKER and Lenhoff and BOOKER and Barak took place until the end of January 2019.
72. BOOKER last spoke to Lenhoff a few days before the arrest of LENHOFF (Appendix 15.1. phone call on January 11, 2019) and apparently tried to obtain information on the contractual relationships of previous years in order to supplement his documents.
73. 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 4.3 million.
74. The e-mail communication included in the criminal files show that Barak was promised by Booker an early payment of the withheld amount just a few days before his arrest (Appendix 16).
75. The agreement between Barak and BOOKER regarding the cleaning up of the company structures (only European operating companies should appear on the scam websites) could no longer be implemented due to the arrest of Gal Barak on 29 January 2019.
76. To date, PAYVISION has not provided an account for this withheld amount.
77. BOOKER did not mention these withheld client funds in its first statement of 23 May 2019 to the Austrian law enforcement authorities (Appendix 10) or in its second opinion of 15 July 2019 (Appendix 11).
78. In summary, PAYVISION appears to have used its position of trust to withhold stolen client funds without authorization and to minimize damage.

Involvement of PAYVISION in other fraud systems

79. In his statement as of July 15, 2019, BOOKER confirmed that PAYVISION had already processed the transactions for the scam platforms of NOVOX Capital Ltd, Cyprus (Optionsbit.com, Optionsxp.com, Optionsmerchants.com) in 2014 and 2015 (compare Appendix 11).
80. PAYVISION also processed the credit and debit card transactions for the scam website Binex (www.binex.ru). In an e-mail communication seized during the house search at the end of January 2019, the scam websites serviced by PAYVISION were listed by the GAL BARAK´s people. (Appendix 13).
81. The scam platform BINEX was closed in the summer of 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 Kyiv was already searched by the Ukrainian cyber police in August 2018. The 60 boiler center employees had been able to persuade more than 15,000 customers in Russia,

Ukraine, and other countries (mostly Eastern Europe) to transfer tens of millions of dollars in just a few months to the scammers via PAYVISION. [9]

82. PAYVISION has also handled credit/debit card transactions from the scam 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.
83. PAYVISION also processed credit/debit card transactions for the scam website AlgoTechs/BEALGO in the years 2017 – 2019 (Appendix 20).

Bank transfers to ING bank accounts of legal and illegal financial agents for BARAK and LENHOFF fraud system

84. 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 fraud website www.optionstarsglobal.com (Appendix 17.1).
85. 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).
86. Leonsky Ltd in Madrid, Spain, a money mule held an account with ING BANK N.V. SUCURSAL EN ESPAA (ES17 1465 0100 9519 0060 4045). This account has been used for several fraud schemes (including the scams of GAL BARAK) (Appendix 18).
87. STICHTING ESCROW ICEPAY (Lottopalace) (ICEPAY B.V., Amsterdam) held an account with ING Bank Frankfurt (DE88 5002 1000 0010 1193 45) and also acted as an illegal payment service provider, the company was used to transfer stolen money for the fraud platform of LENHOFF. (Appendix 19).
88. For Stichting WST Capital Ltd, the US CFTC (CommodityFutures Commission) already issued a warning on April 25, 2017,[10] pointing out that the company is involved in the laundering binary options scams. 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) in 2018 and 2019.

[9] https://www.trafikmarket.com/2019/the-raid-of-the-ukrainian-cyberpolice/
[10] https://cftc.gov/node/221151

EFRI INITIATIVE

PAYVISION's involvement in US legal cases

Beyond Wealth vs T1 Payments and PAYVISION

89. 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 respect of the termination of the payment service contract concluded between Beyond Wealth and T1Payments in the United States District Court in Nevada. 11
90. By written application of 24. August 2020 of Beyond Wealth, PAYVISION B. V. Amsterdam ("PAYVISION") was included in the action as a counterclaim defendant.
91. Beyond Wealth claimed that T1Payments LLC ("T1Payments") in its main capacity as A Payment Facilitator, had lured Beyond Wealth in May 2020 into a merchant agreement for the settlement of credit/debit cards by credibly assuring that they were a Payment Facilitator registered with the credit card companies.
92. Only weeks later, the contractual relationship was terminated and Beyond Wealth found that T1Payments 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 as well as the breach of the rules of the credit card companies.
93. In summary, Beyond Wealth claims that T1Payments was guilty of the activities of an illegal financial agent, bank fraud, and money laundering in cooperation with PAYVISION.12
94. The Beyond Wealth lawsuit describes in great 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 T1Payments was not a Mastercard/VISA-approved Payment Facilitator. T1Payments had a merchant account under his name at PAYVISION and PAYVISION deposited the client funds from the processing activity to the T1Payments bank account at Atlanta Bank in Nevada.
95. 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 to be the contracting parties for Beyond Wealth UK subsidiaries (see below) in order to enable T1 Payments to process the credit card transactions.

[11]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.

[12] Sometimes acquirers may enter into 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).

96. Beyond Wealth LLC was also instructed by T1Payments to set up a UK Beyond Wealth UK to enable Beyond Wealth's business with T1UK and/or TGlobal. Although the Customer Payment Processing Agreement (CPPA) was a direct agreement between the US companies and although transactions were to be processed for US Beyond Wealth customers, the transactions were submitted under the names of the British sham companies.
97. T1 Payments offered the set-up of a British company for Beyond Wealth for a one-time fee of USD 250 and made clear that the set-up of this British shell company was a condition for contracting with T1Payments resp. with the UK sham companies of T1Payments.
98. It was only afterward that Beyond Wealth understood that these shell companies were needed for PAYVISION – a European Payment Institution – to enter into card processing contracts with T1Payments resp. with its British sham companies T1 UK or TGlobal) for the settlement of the transactions of the US company Beyond Wealth.
99. The move, which was a massive breach of the legal rules applicable to PAYVISION 13 and also to the rules of the 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.
100. According to the British company register, T1UK and TGLOBAL were officially inactive companies that only accounted for GBP 1 in assets. Facts that did not disturb PAYVISION when onboarding these merchants.
101. In the legal action against T1 Payments, Beyond Wealth alleges that T1 Payments conspired with PAYVISION to give the impression that T1Payments as well as the merchants were located in the UK and/or the EU and that PAYVISION was, therefore, eligible for onboarding the merchant and processing the card transactions.
102. The credit card companies clearly prohibit T1 Payments from opening Payments Facilitator accounts for Beyond Wealth and these merchants with a licensee like PAYVISION and entering into merchant contracts in their own name as payment Facilitator accounts for Beyond Wealth US.
103. Beyond Wealth states in its lawsuit that the procedure used by T1 Payments to establish British sham companies is described as a standard procedure in T1 Payment's onboarding instructions. In particular, the materials offer the procurement of an "EU Corp".
104. Beyond Wealth claims in the lawsuit that T1 Payments uses the same illegal structure to all its high-risk merchants and that all of these illegal merchant agreements have been settled through PAYVISION for years.
105. A review of Pacer (www.pacer.gov) reveals that there have been dozens of similar lawsuits against T1 Payments in previous years, which apparently did not deter PAYVISION from offering payment processing services to that company up to the end of Mai 2021.
106. In PAYVISION's opinion filed with the US court on 9 November 2020 (document 103-2), PAYVISION confirms that PAYVISION under Dutch law is allowed to process transactions only for merchants in Europe.

[13] 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.

107. The actual Chief Risk Officer of PAYVISION, Maria Alida Johana Ruijters – Terpstra, confirmed in a statement that PAYVISION has never offered services in the state of Nevada, since PAYVISION may legally operate exclusively in the EEA area.

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

109. In order to reinforce the statement submitted, PAYVISION provided as evidence an extract of internal customer documents by appearing as customers of the British T1 Payments companies.

110. PAYVISION does not explain why all payment transactions shown on these internal documents are denominated in USD.

PAYVISION s Engagement at ALLIED WALLET

111. In its action of 23 May 2019 (2:19-cv-04355-SVW-E), the US FTC (Federal Trade Commission) accuses 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, to have knowingly processed payments for numerous companies engaged in fraudulent activities since at least 2012.14

112. Allied UK and Allied Inc were registered as Payment Facilitators with Mastercard and VISA.

113. FTC alleged that Allied Wallet contributed to the fraud of pyramids and various Ponzi schemes, and other fraudulent companies by giving scam websites access to the ability to accept credit and debit card payments.

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

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

116. The creation of British shell companies to set up non-EU merchants was standard procedure at Allied Wallet, the FTC alleges. The need to procure an "EU Corp" in addition to the actual form of the trader was even specified in the internal checklist of the Allied Wallet at the conclusion of each individual dealer contract. As a rule, all these foreign shell companies had no employees, no premises, only straw men as managing directors and owners, and were wealthless.

[14] 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.

117. According to the court documents, both PAYVISION and Wirecard - the now insolvent German fintech - served for years as acquirers for allied wallet constructions and carried out the transactions of US scammers in cooperation with Allied Wallet.

Information from the FINCENFILES

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

119. Deliberate and conspicuous division of large transactions were established for no apparent reason. In just a few months, tens of millions were transferred to customers like Pornhub.15

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

Qualification of non-compliance with legal and contractual regulations

Dutch legislation

120. 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 the use by criminal and terrorist organizations.

121. In accordance with the Payment Services Directive PSD2, as enshrined in the Dutch Civil Code and the Financial Supervision Act (Wet op16het financieel toezicht – Wft), Dutch payment institutions must comply with the Anti-Money Laundering and Terrorist Financing Act (Wwft) and the Sanctions Act 1977 and 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.17

122. 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 actions 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 in order 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, and the activity carried out by the company.

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

124. 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.

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

125. Licensees of credit card companies agree to comply with all rules of the Card Brands.

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

127. Prior to onboarding a new trader (also known as "Merchant") Mastercard and VISA require your license companies, for example, 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.

128. The VISA regulations additionally require the following documents of the trader to be reviewed by the acquirer during the onboarding process:

- 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[18] analysis

129. Both Mastercard and VISA provide high-risk traders with particularly high requirements in terms of customer due diligence and monitoring of ongoing transactions.

130. Credit card companies also impose geographic restrictions on their licensees. For example, licensees may only offer and provide their financial services to companies located within that geographical region "within the authorized "area of use"".

[18] Open Source Intelligence

Non-compliance with legal and contractual obligations by PAYVISION

131. 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 card payment system for money laundering and terrorist financing and to report any suspected money laundering and/or financing of terrorism in accordance with the law.

132. Based on PAYVISION`s activities set out in points 24–128, it is obvious that the company has deliberately ignored all legal requirements and contractual requirements designed to prevent the use of the financial system for fraudulent criminal organizations in order to achieve higher transaction volumes, revenues and profits.

133. 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.

134. 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.

135. If PAYVSISION had carried out proper and careful monitoring of transactions 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 not thousands of European consumers having lost their life savings.

136. The 273 SARS notifications made by PAYVISION mainly starting in July 2018 of 2018 according to his statement of 23 May 2019, clearly show that BOOKER had sufficient evidence of fraudulent activity.

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

138. 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.

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

140. 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 a very high valuation in January 2018.

141. PAYVISION has demonstrably ignored all warning signals, including

- Public warnings from European supervisory authorities on authorized dealers and/or scam websites
- Massive charge-back (rebooking) requests from victims,
- fraud messages from victims
- house searches took place as early as summer 2018.

- Constantly changing contractors, 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 scam websites whose transactions were processed identified as operating and ownership companies established in the Republic of SAMOA or Marshall Islands.
- The fact that the actual beneficial owners of the scam websites did not sign any of PAYVISION`s contractors.

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

143. Without this ignorance of any legal compliance requirements, it is inconceivable that Millions of customer funds from PAYVISION's merchant account were transferred to companies with which PAYVISION had no contractual relationship, on the instructions of GAL BARAK (New Markets SA, SAMOA) and LENHOFF (i.e. Winslet Enterprises EOOD for the purpose of "profit distribution").

144. Contracts were concluded with straw men (some of them homeless) with which no one from PAYVISION had ever spoken.

145. 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 intended to conclude a commission agreement with LENHOFF in the summer of 2018 for the mediation of further fraud platforms indicates the unscrupulousness of BOOKER.

Acquisition of PAYVISION by ING in March 2018

146. Any commercial and legal due diligence in the run-up to 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.

147. 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.

148. Nevertheless, ING Groep NV accepted a valuation of EUR 360 million for PAYVISION.

149. The importance of painting the seriousness and credibility of the scam websites, with a subsidiary of ING, doing the processing and the settlement of credit and debit card transactions for these scam websites is evident. PAYVISION was paid for this advantage by the scam websites in higher margins and long contract retention periods.

.

INTEGRITY and TRUST

150. 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

151. We are deeply convinced that PAYVISION knowingly, and willingly has been an accomplice of criminal organizations for many years.
152. The contribution of PAYVISION, its founders, and its managers, has led to the loss of the life savings of thousands of innocent European consumers who have also lost their confidence in the European financial system.
153. PAYVISION's actions and procedures are contrary to all ethical standards set by the authorities in the Netherlands and the European Union.
154. The lack of conscience, the evident ruthlessness and willfulness of PAYVISION, and its multiple involvements in similar fraud structures indicate that there was a clear will to contribute.

Yours sincerely

Elfriede Sixt Nigel Kimberley