

Introduction	3
Parties working jointly on online fraud.....	4
Gal Barak, Uwe Lenhoff, Vlad Smirnoff, Gery Shalon	4
PAYVISION B.V.	5
Payvision as a payment service provider (PSP).....	6
Amount of cash laundered by Payvision for TCOs identified in Austrian criminal records	7
What happened in detail	8
Background on credit and debit card processing	14
Acquiring organizations are the gatekeepers for card payment schemes.	16
Legal Rules for Payment Institutions	17
Banking Regulations Exist to Help Prevent Funding of Criminal Ventures.	17
EBA guidelines for the risk management of Payment Institutions	18
EBA Guidelines on Due Diligence with ML/TF risk when Onboarding a new merchant.....	19
EBA Guidelines on ongoing monitoring of business relationships and transactions.....	21
Rules and regulations of the card networks	21
Obligations of the Acquirers in the underwriting process.....	22
Monitoring obligations according to the card network rules	24
High-risk merchants	24
Payvision’s knowledge and participation in the fraud.....	26
Payvision’s wrongdoings in detail.....	28
Payvision exclusively onboarded sham companies	28
Dozens of different billing descriptors set by Payvision for the card transactions processed	33
False Merchant Category Codes set by PAYVISION for the card transactions processed (MISCODING)	34
RED FLAGS: Some of the public warnings issued by supervisory authorities against the scam websites serviced by Payvision for offering unlicensed financial services in their jurisdictions:	37
Customer complaints and negative reviews on different websites	39



Excerpt: Binary options as a high-risk business area	40
Warnings issued by supervisory authorities worldwide for binary options trading platforms	41
Additional RED FLAGS: Payvision signed a new merchant contract with Gal Barak on July 24, 2018.44	
Remittances to non-related companies on Barak and Lenhoff's instructions	48
Witness statement of Rumen GOGOV.....	49
PAYVISION also provided payment gateway and alternative payment services for Barak and Lenhoff's scam websites and wactively reroutedtransactions.....	50
Cash deposits in bank accounts held by money mules for Barak and Lenhoff's scam websites.....	52
Also, several ING bank accounts showed up in the criminal files:.....	52
Close personal relations between BOOKER/ Barak and Lenhoff	53
Tons of fraud complaints and chargeback requests	57
Payvision also effected refunds for its fraudulent merchants.....	58
Termination of the payment processing contracts by Payvision.....	60
PAYVISION also provided payment services for other transnational criminal organizations offering binary options trading/FOREX/Crypto	62
NOVOX Capital Ltd	62
Binex/Dreamspay.....	64
24 Option	66
Other	67
Legal proceedings against Payvision in the United States	68
Cooperation agreement between Payvision and T1	69
Bank fraud committed by Payvision	72
T1 Payments deregistration as a PayFac results in Payvision as the only accountable PSP.....	75
Miscoding (U.S. bank fraud) committed by Payvision.	76
Payvision processed payment transactions for CBD and KRATOM for at least four years up to May 2021	80
Involvement in sex trafficking.....	85
Payvision's involvement in the Allied Wallet case.....	86
Acquisition of PAYVISION by ING in March 2018.....	87
The role of ING in the in the scamming activities of Payvision.....	88

Transaction laundering schemes and miscoding as a usual part of business activities	91
Aiding and Abetting Breach of Fiduciary Duties	93
Add on: Pending criminal proceedings Rudolf Booker in Austria	94

Introduction

1. Since at least May 2013, the principals of the Payvision companies (specifically Payvision B.V and Acapture B.V.), Amsterdam, Rudolf Booker, and his co-conspirators, have knowingly facilitated illegal payment transactions for transnational criminal organizations (TCOs)¹.
2. Because European banks and financial institutions are unwilling to process illegal transactions, Booker and his co-conspirators used fraudulent methods to avoid these restrictions, enabling transnational criminal organizations to rip off thousands of European victims.
3. So Payvision and the co-conspirators engaged in bank fraud to support transnational criminal organizations like the Wolf of Sofia (Gal BARAK) and Uwe Lenhoff. Knowing they would earn millions of dollars from facilitating Lenhoff and Barak's online fraud, Booker and his co-conspirators favored profit over following the law.
4. To effectuate the Transaction Laundering Scheme, the conspirators, in cooperation with the transnational criminal organizations, arranged for payment processing agreements with phony merchants and miscoded the transactions, thereby deceiving banks (issuing organizations/financial institutions) about the true nature of the financial transactions they were processing.
5. Payvision's management knowingly benefitted financially from assisting, supporting, facilitating, and otherwise providing the most critical service for Barak and Lenhoff's

¹ Organized crime has traditionally been seen as a domestic problem bedeviling a relatively small number of states such as Italy, the United States, and Japan. In the last few years, however, there has been a recognition that the problem is no longer limited to a few states and can no longer be treated as something that falls within a single jurisdiction. The rise of a global market for illicit drugs, the end of the Cold War and the breakdown of the barriers between East and West, the collapse of the criminal justice system in Russia and the other states of the former Soviet Union, the development of free trade areas in Western Europe and North America, and the emergence of global financial and trading systems have fundamentally changed the context in which criminal organizations operate - and encouraged what had been predominantly domestic groups to develop into transnational criminal organizations (TCOs) **Transnational Criminal Organizations: Strategic Alliances**, Phil Williams [The Washington Quarterly](#) 1994

criminal organization to successfully rip off tens of thousands of worldwide innocent retail consumers for the total amount of **154** million Euros (Appendix 1).

6. Payvision has also, for years – before and after the acquisition by ING, until mid of 2021 – offered its collecting and gateway services to fraudulent high-risk merchants for processing payment transactions in business activities such as porn (e.g., MindGeek), gambling, or other cybertrading (24option, Algotechs/BEALGO,...), as well as pharmaceuticals, MLM and drugs (cannabis/Kratom).
7. Payvision acted outrageously and intentionally. Payvision worked with actual knowledge or in reckless disregard.
8. Payvision was a crucial middleman in the chain of payments, which defrauded unsuspecting members of the public, mainly based in Europe.
9. Payvision breached the fiduciary duty via first-hand participation in the commingling of funds and improper transfers on instructions received from the beneficial owners of the scam serviced (like Uwe Lenhoff).

Parties working jointly on online fraud

Gal Barak, Uwe Lenhoff, Vlad Smirnoff, Gery Shalon

10. 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 severe commercial fraud and money laundering. Investigators had identified Lenhoff as the beneficial owner of the scam websites (trading platforms): Option888, ZoomTrader, ZoomTrader, Tradovest, Lottopalace, and Xmarkets. Since 2016, European criminal authorities have received countless complaints from victims about these scam websites.
11. The criminal proceedings against Lenhoff were opened in Vienna and handed over to Saarbrücken, Germany. On 5 July 2020, Lenhoff was found dead in his cell in Saarbrücken.
12. According to the victims' lists in Lenhoff's criminal records, 29,000 victims (mainly European consumers) transferred more than 100 million euros to sham companies owned by Lenhoff for fictitious investments offered and marketed via the scam websites option888, Xmarkets, and ZoomTrader, Tradovest, Tradeinvest90 between early 2013 and January 2019.
13. On 29 January 2019, Gal Barak, an Israeli citizen and close business partner of Lenhoff, was arrested in Sofia, Bulgaria. Barak runs boiler rooms in Sofia, Bulgaria, and was the beneficial owner of the scam websites xTraderfx (formerly CryptoPoint),

OptionStars/OptionStarsGlobal, goldenmarkets, and safemarkets. Here, too, have been countless criminal complaints from aggrieved Europeans since 2013.

14. According to the customer lists in the criminal files of GAL BARAK, more than 35,000 victims (95% are European consumers) have transferred more than 200 million euros to the fraudulent trading websites operated by Barak between the summer of 2016 and January 2019.
15. After more than 24 months of criminal investigations, Gal Barak was found guilty of severe commercial fraud and money laundering by the Criminal District Court of Vienna on 1 September 2020 (122 HV 4/20g).
16. The Austrian Criminal Court considered 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.
17. 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.
18. The money transferred by the victims was converted to the use of the convicted Barak and Lenhoff.
19. The indictment and the verdict for Gal Barak identify the Dutch Payvision group as the primary payment service provider for Lenhoff's and Barak's scam websites for the years 2016 up to January 2019.
20. During the upcoming months, Vlad Smirnoff, Gery Shalon, and Ilan Tzorya (further co-conspirators of Barak and Lenhoff) will be trialed in Austrian and German courts for being also beneficial co-owners of the fraudulent websites operated by BARAK and Lenhoff.

PAYVISION B.V.

21. 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-founders Gijs op de Weegh and Cheng Liem Li.
22. Until 7 May 2020, the Board of Management of Payvision consisted of Rudolf Booker, CEO, Gijs op de Weegh, COO, and Cheng Liem LI, CCO.
23. Payvision is responsible, under Dutch law and otherwise, for the acts of its officers, directors, employees, and agents, including those actions described in this complaint.
24. Rudolf Booker maintained a close business and personal relationship with Uwe Lenhoff. He engaged Uwe Lenhoff to refer more (fraudulent) merchants from the binary options/FOREX industry.

25. The Payvision group consists of Payvision Holding B.V., the 100 % subsidiaries Payvision B.V and its sister company Acapture B.V., and the unique purpose entities Stichting Trusted Third Party Payvision and Stichting Trusted Third Party Acapture.
26. Since early 2012, Payvision B.V. ("Payvision") has been a regulated payment Institution, licensed and supervised as such by the Dutch Central Bank (the Netherlands Bank).
27. Since late 2012, Payvision has also been a member company of Visa Europe and Mastercard.
28. Acapture B.V. ("Acapture") was also licensed as a Payment Institution under the EU Payment Service Directive and regulated by the Dutch Central Bank.
29. To meet the requirements on the security of funds received from payment services, Payvision and Acapture used special purpose entities named Stichting Trusted Third Party Payvision and Stichting Trusted Third Party Acapture. According to the Payvision Annual Report 2018, The Dutch Central Bank included the before-mentioned Stichtings jointly in its supervision.

Payvision as a payment service provider (PSP)

30. To understand the Payvision (initial success) story, one needs to consider the growing importance of payments in recent years as a fast-growing sector in finance, profiting from the rise of cross-border e-commerce and cashless payments.
31. Payvision marketed its payment processing services - (website excerpt summer 2018) - as follows:

"Payvision is one of the world's fastest-growing global card-acquiring networks. Over the past fifteen years, Payvision has built an independent, international acquiring network, serving banks, payment service providers, and their global merchants in the U.S., Europe, Asia and the Pacific Rim.

Payvision offers a global processing platform with 24/7 support, 150+ currencies, a high-end reporting interface, and a robust risk management solution. With the launch of Acapture in 2015, a new, modern, scalable, and data-driven payment solution, Payvision completed its

Payvision completed its omnichannel package to help merchants pay via a fast, secure processing platform for all transactions processed globally transactions more easily. This results in improved authorization rates, reduced fraud, increased security, and higher revenues for merchants.

Payvision was named Best with MPE Berlin 2016, Best Merchant at the 2015 Payments Awards as Best Merchant Acquirer/Processor, and at MPE 2017 Berlin as

best PSP (payment service provider). *Payvision is headquartered in Amsterdam and serves customers in more than 40 countries. Today, Payvision has offices in New York, Utah, Madrid, London, Toronto, Singapore, Tokyo, Hong Kong, and Macau."*²

32. Payvision focused from the beginning on high-risk payment transactions in the card-not-present environment, meaning online transactions that many other payment companies would avoid, such as those related to gambling and pornography.
33. High-risk transactions are often associated with a high risk of fraud, merchant closure, or chargebacks. For these reasons, high-risk transactions come with higher costs for the merchants, higher profits, and higher risk for the payment service providers.
34. Payvision and Acapture offered collecting services, with Payvision offering mainly card transactions and Acapture offering especially alternative payment methods and/or Payment Gateway Services.
35. The relevant excerpt from Payvision's Terms and Conditions reads as follows:
Payvision allows the Merchant to accept payments from its Customers via the agreed Payment Method for goods and/or services sold online, via a call center, or another type of sales channel. Payvision will provide the Merchant with the agreed Services, subject to the terms of the Agreement and these Conditions, which entail that PAYVISION may:
 - *Operate and maintain a gateway and give the merchant access to it;*
 - *Transmit data (including Transaction Data) from the Merchant to the Payment Organizations;*
 - *Collect or receive the Settlement and transfer the Remittance if so agreed between the Parties;*
 - *Provide reporting and reconciliation about Transactions and*
 - *Provide Related Services in connection therewith.*

Amount of cash laundered by Payvision for TCOs identified in Austrian criminal records

36. Based on the information provided by Booker in its statements to the Austrian law enforcement agency as of May 23, 2019, and July 12, 2019, Payvision has already started to work for binary options platforms in early 2013.
37. In total, more than 154 million euros were processed by Payvision for the fraudulent websites Optionbit, OptionStars, OptionStarsGlobal, option888, xmarkets, Tradeinvest90, Tradovest, xtraderfx, safemarkets, goldenmarkets

² www.globenewswire.com

Figures prepared according to Payvision's statements to the Austrian law enforcement agency					
UBO: NOVOX, Tzorya, Gal Barak	card transactions proces:	Chargebacks done	%	Fraud complaints	%
Mai 2013 - 01.08.2017	5 925 841,25	133 441,16	2,25%	k.A.	
Mai 2013 - 01.08.2017	7 708 286,60	k.A.		149 540,76	1,94%
01.09.2015 - 01.12.2017	4 987 218,77	201 982,36	4,05%	k.A.	
Sept 2015- Mai 2017	4 981 347,49	k.A.		125 174,91	2,51%
	23 602 694,11	335 423,52	1,42%	274 715,67	
UBO: Gal BARAK, Gary Shalon, Vlad Smirnov					
Sept 2016 - Sept 2018	28 101 859,97	2 125 984,71	7,57%	1 065 605,74	3,79%
April 2018 - Jan 2019	37 464 887,13	3 894 711,24	10,40%	1 491 477,50	3,98%
July 2018- Jan 2019	4 806 545,28	819 898,78	17,06%	51 485,14	1,07%
Juni 2018- Jan 2019	5 237 486,63	488 080,55	9,32%	87 232,53	1,67%
Total	75 610 779,01	7 328 675,28	9,69%	2 695 800,91	3,57%
UBO: Uwe Lenhoff					
02/2016 - 01/2019	18 272 610,96	613 041,86	3,35%	372 237,76	2,04%
07/2017-01/2019	27 547 372,92	623 811,00	2,26%	353 792,57	1,28%
07/2018 - 01/2019	9 826 550,91	257 787,00	2,62%	58 923,66	0,60%
Gesamt	55 646 534,79	1 494 639,86	2,69%	784 953,99	1,41%
Gesamt	154 860 007,91	9 158 738,66	5,91%	3 755 470,57	2,43%
Note: based on our research the lists provided by Booker as of July 12, 2019 and as of May 23, 2019 are incomplete.					

38. thousands of trustful European consumers transferred their life savings to the transnational criminal organizations around the Hillel brothers, Gery Shalon, Gal Barak, and Uwe Lenhoff, using their credit and debit cards.

What happened in detail

39. Payvision onboarded NOVOX Capital Ltd, a Cyprus company incorporated on 12/08/2011 already in March 2013, a year before NOVOX Capital Ltd got licensed as a Cypriot Investment Firm (CIF) on 04/02/2014, under license number 224/14.
40. NOVOX Capital Ltd. was authorized to operate the following CySEC-approved binary options websites: optionbit. eu, zoomtraderglobal.com, optionstars.com, and optionmerchants.com.

41. The beneficial owners of NOVOX Capital Ltd. were Israelis Israel Bash, Shay Hillel, and Yehoram Hillel³, and according to the Austrian criminal files, Ilan Tzorya.
42. Shay Hillel, Yehoram Hillel, and Tzorya also co-owned Tradologic, the cybertrading software provider for fraudulent websites.
43. The criminal files show that NOVOX Capital Ltd. operated approved and unapproved binary options websites, sometimes differing just by a different ending, like optionbit.eu (CySEC-approved domain) and optionbit.com (unapproved domain) or OptionStars.com/OptionStarsGlobal.
44. NOVOX Capital Ltd. operated optionbit.com (unapproved) and optionbit.eu (approved) resp. optionstars.com (approved), optionstarsglobal.com (unapproved), zoomtrader.com (unapproved), and option888 (unapproved) until the end of 2016.
45. Payvision onboarded NOVOX Capital Ltd before its authorization by CySEC and processed card transactions for approved and unapproved domains. At the time of onboarding, regulators warned about optionbit and zoomtrader, and the web was full of negative postings from victims.
46. In late 2014, Gery Shalon and Vlad Smirnov joined Ilan Tzorya, Gal Barak, and Uwe Lenhoff's organizations and invested in the software company Tradologic.
47. A few months later, U.S. prosecutors charged the Georgia-born Israeli citizen Gery "Gabi" Shalon with a twenty-three count Superseding Indictment (Docket No. S1 15 Cr. 333). Shalon was deported from Israel in 2015 and accused of running what then-US Attorney General Loretta Lynch called "one of the largest thefts of financial-related data in history." He faced 23 counts and was charged with running a scheme that stole client information from JPMorgan Chase & Co. and other companies. He was also accused of running online gambling, stock manipulation, and global money-laundering operations. He was charged with computer hacking, securities fraud, aggravated identity theft, illegal online gambling, illegal money-transmitting business, and money laundering. In April 2017, Shalon pled guilty to all 23 counts and made a plea deal with prosecutors, including forfeiting all seized funds and assets.
48. In 2015, Uwe Lenhoff established option888.com with the help of Ilan Tzorya. In the same year, Gal Barak joined the NOVOX venture and took over the management of optionstars.com and optionstarsglobal.com (still the onboarded merchant for the card

1. ³ Shay Hillel and Yehoram Hillel also operated the payment service provider DCashier (afterward: IM Payments).

payments was NOVOX Capital Limited). In March 2016 Lenhoff bought the domains zoomtrader.com, zoomtraderGlobal.com and zoomtrader.info from Ilan Tzorya.

49. With more and more warnings from different regulators⁴ and complaints on various web forums and CySEC piling up about the brands operated by NOVOX Capital Ltd, CySEC fined NOVOX in Dec. 2016 (announcement date: 19.02.2017).
50. The fine set with € 175.000 split as follows:
- where €70,000 comes for providing investment advice without authorization. The remaining part of the fine is imposed for the following violations:
 - €10,000 for not maintaining proper internal control mechanisms for the approval of advertising materials
 - €20,000 for inadequate outsourcing of activities, such as customer service and call center activities, to third parties.
 - €30,000 for not acting in the best interests of the clients.
 - €30,000 for the dissemination of misleading advertising materials by third parties.
 - €15,000 for providing information that is not suitable for clients.
51. NOVOX asked for a reimbursement of the fine from optionbit, optionstars, and zoom trader, as shown in the criminal files.
52. NOVOX Capital Limited insisted on taking optionstars.com and optionstarsglobal off in September 2016 due to the high number of complaints.
53. According to information in the criminal files, VISA/Mastercard fined Payvision in April 2017 with two chargeback fines totaling 480.000 euros relating to the card transactions for optionbit, optionStars/optionStarsGlobal, and ZoomTrader.
54. Although Payvision must have been aware of the CySEC fine for optionbit, optionstars, and zoomtrader, and although the card companies levied a heavy fine for high chargebacks, Payvision continued to work for NOVOX Capital Limited up to the end of 2017.
55. When NOVOX Capital Limited officially took off the brands optionstars and zoomtrader, Payvision started to onboard pure sham companies set up by Lenhoff (Payific Ltd, Hithcliff Ltd, Celtic PAY Ltd) and Barak, Gery Shalon and Vlad Smirnov (Cool Markets, Optiumcommerce, Matching Blue Consulting, Gpay Ltd).

⁴ Already as of February 2, 2012 the Autorite des Marches Financiers (AMF) issued a warning for the unauthorized website: www.optionbit.com. Warnings for Optionstars and OptionStarsGlobal were issued by the British Columbia Securities Commission as of June 12th, 2016.

56. Neither one of the merchants onboarded by Payvision starting in 2016 was an authorized investment firm nor an authorized money transmitting company.
57. Due to the personal relationship established between Lenhoff and Rudolf BOOKER in late 2015, Payvision changed its role.
58. For the NOVOX Capital Limited organization, Payvision was one of many different acquirers used. Still, with the personal relationship and Lenhoff reselling Payvision's services to BARAK, Shalon, and Smirnov, Payvision became the main acquirer organization for these transnational criminal organizations.
59. The financial flows for the card processing (acquiring) for these TCOs ran through the merchant accounts with Deutsche Bank and ING set up by Stichting Trusted Third Party Payvision.
60. PAYVISION transferred the stolen funds collected bi-weekly, minus its margin and other handling fees (e.g., charge-back fee) and rolling reserves, to the fraudsters' bank accounts with Wirecard resp. With Bulgarian banks.
61. Based on a comparison between the transaction volume provided by Payvision and the collected money shown on the bank statements in Barak's criminal files, **about 20% of the total cash processed by Payvision for the criminal organizations remained with Payvision.**

xtraderfx		
collected GPAY ltd		26 525 720,37
According to Payvision's statement as of May 2019		
2018		
April	681 518,85	
Mai	2 147 500,64	
Juni	2 366 586,55	
Juli	2 963 592,27	
August	6 227 367,93	
September	4 352 203,95	
oktober	5 416 695,44	
November	7 425 109,30	
Dezember	4 791 455,63	
2019		
Jänner	1 092 857,86	
	37 464 887,13	
Chargeback	3 894 711,24	10,40
Fraud	1 491 477,50	3,98
	33 570 175,89	
collected by Gpay ltd.	26 525 720,37	
money with PV	7 044 455,52	20,98%

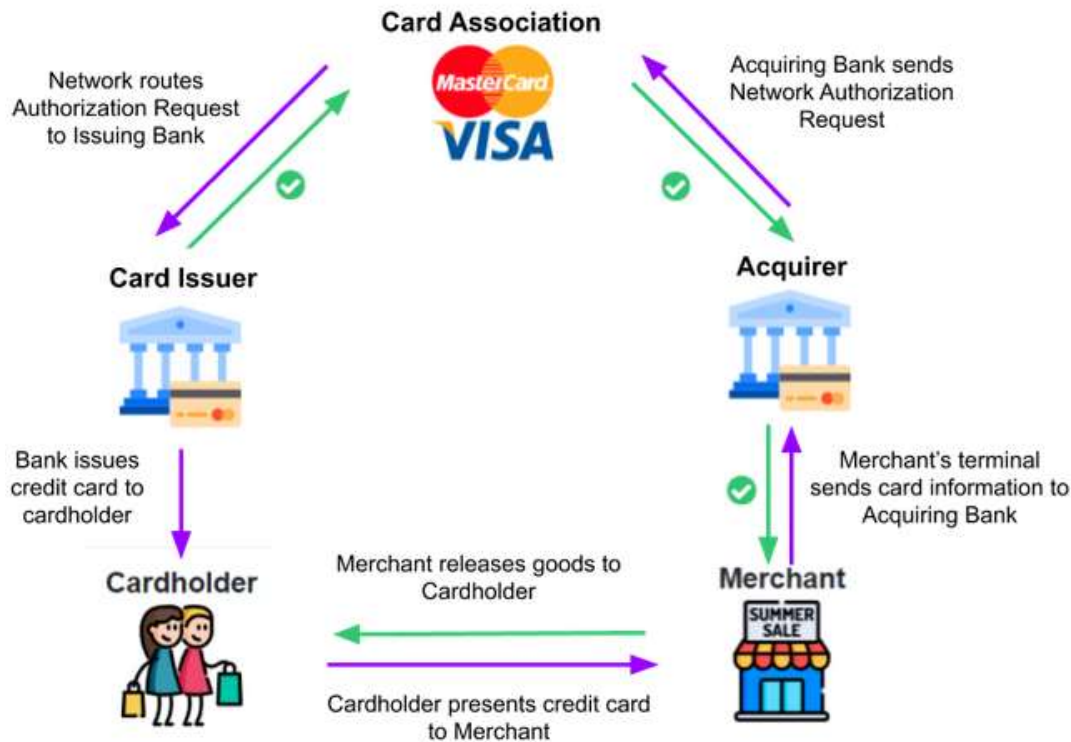
- 62.
63. A snapshot of Gpay Ltd's (sham company used for the intake of the card payments for the scam website xtraderfx and cryptopoint) bank statement as of September 11, 2018, is as follows:

Дата Date	Оп. No Ref No.	Валютен Value Date	Описание на операцията Description of the transaction	Плащания Paid	Постъпления Received
11.09.2018	0120940907		Нареден превод в полза на ONLINE PROSPECT LIMITED по сметка 817588940838 при INVOICE 906/03.09.18 ИЗХОДЯЩ ПРЕВОД	95 689.40	
11.09.2018	0120940907		Такса комуникационни услуги	10.00	
11.09.2018	0120940907		Комисиона за изх. вал. превод	287.07	
11.09.2018	0121055065		Такса получен валутен превод	10.00	
11.09.2018	0121055065		Получен превод от BETTER TELECOM PTY LIMITED LEVEL 1 309 PITT STREET от сметка 00001663044 ВХОДЯЩ ПРЕВОД		3 237.93
11.09.2018	0121108564		Такса получен валутен превод	70.00	
11.09.2018	0121108564		Получен превод от P2P GMBH EUPENER STR. 55A от сметка NL52BUNQ2206949628 PAYMENT ACCORDING THE AGREEMENT		70 000.00
11.09.2018	0121108728		Такса получен валутен превод	200.00	
11.09.2018	0121108728		Получен превод от STICHTING TRUSTED THIRD PARTY PAYVISIONMOLENPAD 2 от сметка NL09DEUT0265137020 MID 75075614 TRADE NAME GPAY 6051 EUR X2 FUNDING DATE 03.09.18 FUNDINGAMOUNT 1,510,783,58		1 277 129.14
11.09.2018	0121108900		Нареден превод в полза на ONLINE PROSPECT LIMITED по сметка 817588940838 при INVOICE 906/03.09.18 ИЗХОДЯЩ ПРЕВОД	95 689.40	

Background on credit and debit card processing

64. With digitalization, the use of payment cards has increased significantly. Credit/Debit cards are the most common and popular method for consumers to make online purchases.
65. Card payments provide consumers with an easy, convenient way of making payments at home and abroad and the no-hassle ability to draw on credit lines.
66. Globally, American Express, Diners Club, MasterCard, and Visa are among the world's leading credit card systems. Specifically, VISA and Mastercard are definitely on the winning side of digitalization. MasterCard and Visa dominate the global payments processing market. The duopoly accounts for over 80% of all EU card transactions in Europe.⁵
67. For online merchants, it is a must to win a PSP, a partner company licensed by a payment card system such as VISA or Mastercard, as a contractual partner (also referred to as an acquirer in the payment card system).
68. The most popular credit card payment networks, VISA and Mastercard, are (at least) a 4-party system:
 - Payer or the cardholder/customer of a merchant
 - Payee/online merchant (often referred to as merchant),
 - payment service provider of the payer (often referred to as **issuer**) and
 - Payment service provider of the payee (often referred to as an **acquirer**).

⁵ <https://www.finextra.com/newsarticle/33339/ecb-chief-says-instant-payments-could-break-visamastercard-duopoly>



Icon Credit: Cardholder Icon, Bank Icon, Merchant Icon

69. The role of the issuer or acquirer is assumed mainly by financial institutions (banks and payment institutions), licensed, regulated, and supervised by national financial supervisory authorities. The issuing and the acquiring organizations acquire member licenses from the card association and thus are obliged to submit to the rules of the card payment networks.
70. The card payment networks (i.e., Visa and Mastercard) provide their members (issuing and acquiring organizations) with the infrastructure (CSM – Clearing & Settlement Mechanism) and the brand.
71. An **issuer (customer's bank) issues** payment cards to customers. The issuer has a contractual relationship with the cardholder and charges their customers for payments they make.

- 72. The merchant **acquiring organization**⁶ negotiates deals with merchants and processes card payments for their onboarded merchants.
- 73. The customer's cash is transferred from the card issuing bank (the customer's bank) to the merchant acquiring bank (the bank of the merchant) via a card association.

Acquiring organizations are the gatekeepers for card payment schemes.

- 74. The acquirers maintain relations with the merchants and give them access to the financial system by providing them with a merchant bank account and the ability to accept card transactions.
- 75. Principally, the acquirer's responsible for administering the acceptance ("approval") of the individual merchant in the payment card system and monitoring the merchants.
- 76. The acquirer handles the authorization and settlement of card payments for the merchant.
- 77. In detail, the acquirer authorizes, processes, and calculates each card transaction during the payment process⁷.
- 78. A merchant derives various advantages from participating in card schemes and, above all, the facilitation of payment transactions. The electronic processing of card payments simplifies accounting compared to cash transactions, increases transparency, and speeds up the sales process.
- 79. Credit card acceptance can also contribute to expanding a merchant's business area. Various goods and services sold via long-distance relationships (Internet, telephone orders, or mail orders) are usually only possible with cards. In addition, credit card acceptance expands the merchant's customer base by allowing low-liquidity customers to use credit cards to conclude sales that would not have been possible without a credit line.
- 80. The acquirer is within the card payment systems to have a direct relationship with the merchants. He advocates the merchant relationship within the card associations,**

⁶ While some merchants deal directly with the Acquirers to conclude the contracts, (usually smaller) merchants can be concluded by intermediaries such as payment processors, payment facilitators, independent sales Organizations (ISO's), and resellers (common on the 'Service providers') Access to the networks. Payment facilitators recruit merchants, and merchants' applications present the acquirer and equip the merchants with the technical necessities of Payment to be able to carry out species transactions. Sometimes these payment facilitators also open merchant accounts with the acquirers themselves and open sub-merchant accounts for small traders. ISOS are commissioned by the acquirers or the Payment Facilitators.

⁷ A contract company is a company (merchant) that undertakes to accept the credit card as a means of payment and concludes a credit card acceptance contract with the acquirer for this purpose. The credit card acceptance contract is the legal basis for credit card payments and contains provisions such as verification obligations of the merchant at the receipt of credit card data, handling of credit card data and amount of fees.

carries out the due diligence and onboarding process, concludes the necessary merchant acceptance contracts, and cooperates with the card association to provide the required technical payment infrastructure.

Legal Rules for Payment Institutions

81. In Europe, the applicable legal rules for organizations engaged in commercial payment instruments (cards), also known as payment institutions, were set for the first time in the European Payment Services Directive 2007/64/EC (PSD1) of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market. This law aims to create a single legal framework for European payment services⁸. All EU member countries had to implement PSD1 up to the end of 2009.
82. The Second Payment Services Directive (2015/2366) was intended to develop further the European internal market for non-cash payments created by PSD2. It will be transposed in all EU countries until January 13, 2018.
83. **The PSD2 requires all payment service providers dealing with card payments to be authorized and regulated.**
84. PSD2 provides for new additional obligations and due diligence requirements of the payment service provider to limit fraud risks as much as possible to protect the payment service users as much as possible.
85. The inclusion of new payment providers within the scope of PSD2 was intended to allow competent authorities to monitor better and supervise the activities of these new players.
86. The 4th Anti-Money Laundering Directive ([Directive \(EU\) 2015/849](#)), as well as the 5th Anti-Money Laundering Directive (Directive (EU) 2018/843), defines payment institutions as obliged parties.

Banking Regulations Exist to Help Prevent Funding of Criminal Ventures.

87. The Anti Money Laundering Rules in the EU require Payment institutions to have adequate anti-money laundering (“AML”) policies and systems. European Union and Dutch require payment institutions to devise and implement strategies reasonably designed to identify and report suspicious activity and block transactions prohibited by law.
88. All regulated institutions are expected to configure systems based on their unique risk factors, incorporating parameters such as institution size, presence in high-risk jurisdictions, and the specific lines of business involved. The institutions have an affirmative duty to ensure that their systems run effectively.

⁸https://www.ris.bka.gv.at/Dokumente/Begut/BEGUT_COO_2026_100_2_508042/COO_2026_100_2_508050.html

89. In addition to having adequate AML controls in place, it is also necessary for payment institutions to monitor their customers to prevent their customers from facilitating criminal activity using the institution's facilities as **part of preventing illegal activity**.
90. **Know Your Customer ("KYC"); customer due diligence is critically important. Financial institutions must collect customer information when establishing new relationships with clients, including as necessary to assess the risks associated with the client. To properly consider these risks, payment institutions must consider relevant factors such as the nature of the client's business, the purpose of the client's accounts, and the nature and duration of the relationship.**
91. Payment institutions must also conduct KYC reviews for each client relationship at intervals proportional to the AML risks posed by the client, including reviewing account activity to determine whether such activity fits with what would have been expected given the nature of the account. Each client's AML risk should also be re-assessed if material new information or unexpected account activity is identified.
92. Payment institutions must also establish criteria for determining when a client relationship poses too high of a risk and must be terminated. A payment institution may be liable under applicable laws if it maintains such a relationship despite repeated indications of the facilitation of improper transactions.

EBA guidelines for the risk management of Payment Institutions

93. EBA has issued appropriate procedures for establishing a risk management framework, risk assessment, control, and other safety measures for payment institutions to be followed by national supervisory authorities and acquirers.
94. The EBA/GL/2017/17 guidelines set out requirements for the definition, application, and monitoring of the security measures to be taken by payment service providers under Article 95(1) of Directive (EU) 2015/2366 to manage the operational and security risk assessments associated with the payment services they provide.
95. The risk appetite defines the overall level and types of risks an institution is willing to take within its risk capacity and in line with its business model to achieve its strategic objectives.
96. The guidelines provide extensive requirements for the risk management of an acquirer, such as under 3.4.

Risk assessments of functions, processes and assets

- 3.4 PSPs should ensure that they continuously monitor threats and vulnerabilities and regularly review the risk scenarios impacting their business functions, critical processes and information assets. As part of the obligation to conduct and provide CAs with an updated and comprehensive risk assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigating measures and control mechanisms implemented in response to those risks, as laid down in Article 95(2) of Directive (EU) 2015/2366, PSPs should carry out and document risk assessments, at least annually or at shorter intervals as determined by the CA, of the functions, processes and information assets they have identified and classified in order to identify and assess key operational and security risks. Such risk assessments should also be done before any major change of infrastructure, process or procedures affecting the security of payment services occurs.
- 3.5 On the basis of the risk assessments, PSPs should determine whether and to what extent changes are necessary to the existing security measures, the technologies used and the procedures or payment services offered. PSPs should take into account the time required to implement the changes and the time to take appropriate interim security measures to minimise operational or security incidents, fraud and potential disruptive effects in the provision of payment services.

EBA Guidelines on Due Diligence with ML/TF risk when onboarding a new merchant

97. On 1 March 2021, EBA, under Articles 17 and 18(4) of Directive (EU) No 2015/859 (EBA/GL/2021/02) and Article 16 of Regulation (EU) No 1093/2020, issued guidelines on due diligence and the factors that credit and financial institutions may have in assessing the risk of money laundering associated with individual business relationships and occasional transactions and terror financing ('The Guidelines on Risk Factors for Money Laundering and Terrorist Financing'), replacing Guidelines JC/2017/37.
98. EBA/GL/2021/02 defines "**risk**" as the likelihood of money laundering and terrorist financing and the associated effects. "**Risk appetite**" means the level of risk an entity is willing to accept. "**Risk Factors**" means variables that, either on their own or in combination with each other, may increase or decrease the GW/TF risk of a single business relationship or occasional transaction. '**risk-based approach**' means an approach based on which the competent authorities and the undertakings identifying, assessing and understanding the GW/TF risks applicable to the latter and implementing anti-money laundering measures or Measures to combat terrorist financing (AGW/BTF measures) which are appropriate for these risks.

99. The guidelines identify extensive and detailed obligations for financial and payment institutions, with Title 1 containing general rules and Title II being sector-specific.
100. General due diligence requirements already require explicit identification of the contractual partner (Know Your Customer check), the identification of the beneficial owner, a risk-based due diligence review, a comparison of customers and transactions with international sanctions lists, and a check as to whether a customer is considered a PEP, the observation of negative news reports current or potential customers are mentioned in them, for the continuous monitoring of customers and whether a customer's AML risk has changed.
101. Enhanced due diligence obligations (EDD) are required if the increased risk is detected; the higher the risk, the more information must be obtained, and the more intensively an ongoing business relationship must be controlled⁹.
102. The guidelines provide explicit instructions on how payment institutions must consider and implement the "risk-based approach" in their organizational processes and structures when carrying out their payment service activities.
103. For example, the company-wide risk assessment guidelines help companies understand where and with which services they are exposed to ML/TF risks. (1.11) ff)
104. The individual risk assessment shall carry out an initial review as part of its customer due diligence measures under Article 13(1)(a), (b), and (c) and Article 15(4) of the Directive.
105. According to 1.24, at least the following risk-oriented measures should be taken during the initial review:
- The identity of the potential customer's identity (beneficial owner) is verified.
 - The purpose and the intended nature of the respective business activity must be determined.
106. When determining the risk factors associated with customers, it is also explicitly required to determine whether the customer has connections to sectors generally associated with an increased ML/TF risk, such as the gambling or binary options industries.
107. Relevant risk factors concerning products, services, and transactions (2.16) are mainly the degree of transparency and complexity of the merchant's products or services. Also, the risk factors connected with sales channels must be checked.

⁹ https://www.pwc.ch/de/publications/2020/handbuch-geldwaeschereigesetz_5.auflage.pdf

EBA Guidelines on ongoing monitoring of business relationships and transactions

108. According to Article 13 of Directive (EU) 2015/859, companies should constantly monitor their business relations with their customers (

109. Ongoing monitoring of transactions has to ensure that the original risk assessment matches the client's risk profile, financial position, and the company's general knowledge of the client to detect unusual or suspicious transactions. A constant update of documents, data, and information on the risk associated with the business relationship is required.

Sector-specific guidelines for payment institutions) are laid out in EBA guideline 11

110. Financial transfer service providers may be exposed to a higher ML/TF risk due to the nature of the payment services offered. This risk results from transactions being processed efficiently and quickly, having a global reach, and often being based on cash.

111. According to 11.5, the following factors can contribute to increased risk.

- The product in question authorizes transactions of large or unlimited amounts,
- The product or service in question has a global reach
- Mass of Cross-border transactions
- The prospective customer's sales channel has a certain degree of anonymity.
- The service in question is provided exclusively online.

Rules and regulations of the card networks

112. In line with the AML/CTF requirements of PSD I and PSD II for payment systems, the card schemes impose extensive rules on their licensees (issuers and acquirers) and demand unconditional adherence to these comprehensive regulations.

113. The designated explicit purpose of the extensive sets of rules is

- prevention of money laundering,
- consumer protection
- reducing the cost and reputational risk associated with chargeback and fraud and
- maintaining the integrity of the financial system.

114. Both card schemes determine the acquirer's responsibility for accepting, validating, and monitoring authorized merchants¹⁰.

¹⁰ <https://usa.visa.com/dam/VCOM/download/merchants/visa-global-acquirer-risk-standards.pdf>

115. So is the **Visa Global Acquirer Risk Standards Guide** designed to help acquirers:

- understand their responsibilities towards the Visa payment system;
- manage and control their relationships with retailers and third-party agents;
- ensure that day-to-day operations and practices comply with Visa Global Acquirer Risk Standards and Visa Rules.

Obligations of the Acquirers in the underwriting process

116. This guide provides extensive minimum requirements for underwriting/onboarding online shops.

117. For example, extensive relevant public and non-publicly available merchant information (**Open Source Intelligence OSINT**) must be collected and validated before a merchant can access the payment card networks.

118. The Acquirer is obliged to carry out comprehensive due diligence before acceptance of a merchant (technical term: onboarding), the level of detail of which also depends on the risk class of the business activities of the potential authorized merchant.

119. A critical review of the onboarding process is intended to prevent pure shell companies from gaining access to the payment card system to carry out fraudulent activities.

120. Furthermore, by carrying out the due diligence, the acquirer is enabled to verify or determine the "correct" merchant category allocation ("MCC").

121. In detail, the onboarding of an online shop requires due diligence with a clear identification of the merchant, a determination of his business activity (as a basis for determining the correct merchant category allocation), and, above all, a determination of the risk associated with the specific transactions of the merchant particular with online shops.

122. Summarizing the following due diligence steps is a must:

- a review of the merchants' companies and business documents,
- check the merchant's website for the correctness of the information and the functionality of the website
- as well as a check for domain ownership and compliance with the information on the website and data provided by the merchant.
- determine whether an illegal or legal activity is being carried out.
- Carry out a check for negative press releases
- Carry out a check for an entry in the MATCH List (Terminated Merchant Files) of the credit card companies

- an examination of the regularity of the company's distribution channels
- If a trader has no history, increased due diligence measures must be taken (enhanced due diligence).

123. The large card networks demand that every processed transaction include detailed information about a single transaction, the place of activity of the merchant (country code);

- A unique number assigned to the respective merchant: MID (Merchant Identification Number), also called authorized merchant number or contractor number.
- The determination of a billing descriptor that is displayed on the customer's credit and debit card receipts. The billing descriptor is set by the acquirer when onboarding the merchant. The customer uses the billing descriptor to identify to whom a payment has been made in a particular transaction.
- A country transaction code
- The merchant category code (MCC) is a four-digit code that describes the type of business receiving the payments, such as 7995 for gambling establishments, 5667 for pornography, 5698 for wig and toupee stores, 7273 for dating and escort services, and 9223 for bail and bond payments. These codes permit other banks and networks to decline transactions on specific countries or merchant codes that reflect high-risk transactions or high-risk locations. **The acquirer sets the four-digit code after the onboarding process is finished.**

124. Illegal transactions under the laws applicable to parties involved may not be executed under the Card Brand rules.

Monitoring obligations according to the card network rules

125. Once merchants have been accepted, acquirers must constantly monitor ongoing transactions for irregularities, high chargeback requests, fraud reports by payment service users, or other indications of prohibited transactions (red flags).
126. Suppose the chargeback requests reach a certain percentage of the total transaction turnover. The acquirers must terminate the contracts and register the authorized merchant for entry in the MATCH list.
127. The MATCH list is a list of merchants who are considered unacceptably risky. Acquirers use this list to identify merchants they don't want to do business with.
128. MATCH is the renamed version of an older, more aptly named list, the Terminated Merchant File (TMF). Mastercard created the list to help acquirers identify high-risk merchants before entering into merchant acceptance contracts.
129. Credit card companies use chargebacks [as an indicator](#) of potentially fraudulent activity. Credit card companies constantly monitor a business' "chargeback ratio" — i.e., a ratio of contested to uncontested transactions. High chargeback ratios result in a business losing access to the credit card system and can potentially tip off authorities to fraudulent or criminal activity
130. When a cardholder and an issuer initiate a dispute (chargeback request), they submit an information packet to the acquirer, who then forwards it to the merchant. The information contained in this package includes the code (e.g., missing goods or fraud) for the chargeback reason.
131. The chargeback rate is a metric that indicates the ratio between the total number of transactions a merchant processes and the total number of chargebacks the merchant receives.
132. Visa and Mastercard each set their acceptable thresholds for chargebacks, and there are several different calculation methods to refer to. For example, in 2019, VISA set its default threshold at 0.9% of monthly transactions.

High-risk merchants

133. Online gaming, multi-level marketing systems, cryptocurrencies/precious metals, dietary supplements, dating / erotic services, binary options, FOREX, all these industries are classified as high-risk business areas due to the high associated risk of fraud both according to the provisions of the EBA guidelines and according to the rules of the card associations.
134. For high-risk customers, both the money laundering regulations and the card schemes company regulations provide enhanced due diligence obligations when onboarding



and constantly monitoring and reviewing ongoing transactions. The card rules even ask for existence verification for the card-not-present business.

135. For online retailers carrying out these types of transactions, it is usually challenging to find an acquirer, as the fraud and reputation risk associated with fraud settlement is considered too high.

136. Acquirers specializing in this business are recorded as high-risk acquirers by VISA/Mastercard.

137. Payment institutions charge higher fees for processing high-risk payment transactions for the higher fraud and associated reputation risk. To illustrate: For settling credit card payments for services from the "normal" trade in goods, fees are 0.05 to the max. 1.5%. In the high-risk credit card billing area, up to 9% is charged (PAYVISION has charged 7%+ for settling binary options transactions).

Payvision's knowledge and participation in the fraud.

138. So the law, and EBA's rules and card rules, required Payvision and its principals to monitor their onboarded merchants for anomalous or suspicious behavior, discovering signs of fraud, money laundering, or misconduct to stop doing business with them and report the red flags.
139. Acquirers should mitigate the risk that one or more of their merchants may be involved in money laundering (and be alert to the risk of collusive merchants) by understanding the types of goods their merchant offers and what activities/transactions are indicative of money laundering in the context of that business
140. Law and the card rules require acquiring organizations to determine the beneficial owner, the source of funds, and the purpose and expect them to monitor transaction activity for every account and identify activity outside expected usage."
141. Among other facts that triggered enhanced due diligence obligations, Payvision knew that binary options have repeatedly presented an opportunity for fraud. They, therefore, should have applied heightened scrutiny when onboarding and monitoring transactions.
142. Payvision breached its know-your-customer and anti-money laundering duties concerning Barak and Lenhoff's entities. They either failed to establish and maintain an adequate due diligence program or failed to execute such a program properly.
143. Because red flags from the online schemes abounded, even ordinary due diligence—not limited to the enhanced scrutiny required—would have revealed suspicious account activities.
144. Payvision's failures to adequately monitor and stop the fraudulent activities of Gal BARAK and Lenhoff, and Payvision's acts and omissions directly in furtherance of this scheme, carried out through Payvision's merchant accounts bank accounts, were the cause of the investment losses of the innocent victims.
145. Barak and Lenhoff's online fraud scheme was not possible without the assistance and collaboration of payment institutions—only these payment institutions and the possibility to accept card payments provided their operation with an appearance of legitimacy and special treatment to the online fraud venture, thereby ensuring its continued operation and defrauding tens of thousands of innocent European consumers. Without Payvision's participation, Barak and Lenhoff's online fraud scheme could not have existed or flourished.
146. Barak and Lenhoff's victims were innocent European consumers who suffered material harm and **were affected socially, emotionally, and mentally**. The financial impact of scams brings stress that can be both intense (from the sheer amount lost) and chronic (long-term as they seek to recover the loss). The stress leads to depression or other disorders such as anxiety and results in the suicide of some of the victims.
147. Lenhoff and Barak needed a reliable Payment Institution that would provide the necessary legitimate appearance for their operation, allow them to open many accounts for illegitimate companies, ignore blatant red flags, enable them to transfer money without questioning, allow

- them access to abundant cash in direct violation of money laundering regulation and otherwise to facilitate the commercial aspect of their online fraud enterprise.
148. From May 2013 through 2019, Payvision was the key Payment Institution participating and playing an essential role in the criminal organizations around the Hillel brothers, Barak, and Lenhoff's ventures.
149. Payvision has knowingly and willfully violated all regulatory rules and the rules and requirements set by the credit card schemes, thereby providing transnational criminal organizations access to the incumbent financial system and enabling them to rip off hundreds of thousands of innocent European consumers. Payvision has purposefully circumvented card network rules and transaction
150. Payvision knowingly participated in Barak and Lenhoff's online fraud scams by (among other things) providing the financial underpinnings for them to have ready and reliable access to resources—including cash—to lure more victims into their scams.
151. Without Payvision's willful assistance, Barak and Lenhoff could not have victimized tens of thousands of innocent European victims.
152. When considering whether to participate in the online fraud venture and before onboarding, Lenhoff resp. Barak, Payvision estimated that it would earn several million euros annually by funding the online fraud venture and handling the card payments of the fraudulent websites.
153. Ultimately, Payvision benefited financially by earning millions of euros (about 20% of 132,2 million euros – 26 million euros for five years) to participate in Barak and Lenhoff's online fraud venture.
154. Throughout its relationship with Barak and Lenhoff, Payvision violated numerous regulations to continue its lucrative venture, facilitating the transnational criminal organization of Barak and Lenhoff.
155. Payvision enabled Barak and Lenhoff to have ready and reliable access to resources, including cash, to finance their transnational criminal organization.
156. Payvision's knowing and intentional payment institutions' law violations allowed Barak and Lenhoff and their various corporations to stay "under the radar" and continue their online fraud operations without scrutiny or interference.
157. Payvision benefitted by receiving things of value from its participation in Barak and Lenhoff's online fraud venture. Among the various items of value it received were 1) connections with Lenhoff, his co-conspirators, and his wealthy friends and associates; (2) additional deposits from the online fraud venture, his co-conspirators, and wealthy friends and associates; (3) the ability to charge above-normal fees to Barak and Lenhoff because he was a "high risk, high reward" customer; and (4) the opportunity to earn financial benefits from the funds that had been deposited with it. Payvision knowingly received these things of value due to its participation in the Barak and Lenhoff online fraud venture and because it was furthering Barak and Lenhoff's online fraud venture.
158. Breaking up transactions to avoid the reporting of transfers of more than 10.000 euros transfers was a usual procedure applied by the scammers, and by Payvision, this "structuring" took place frequently.

Payvision's wrongdoings in detail

159. In specific, Payvision provided the following services to Gal Barak, Uwe Lenhoff, and other criminal organizations

- Acting as a payment gateway provider
- Processed debit and credit card payment processing
- Paid out Ponzi refunds to victims to lure them into making higher and more deposits.

Payvision exclusively onboarded sham companies

160. Rudolf Booker attached a list of Payvision's contracting parties (merchants) for Barak and Lenhoff's scam websites to his written statement to the Austrian law enforcement agency on 23 May 2019. Also, he provided the names of the directors who signed the contracts with Payvision.

Uwe LENHOFF zuzurechnen:

Firmen Geschäftspartner	Verbundene Gesellschaften	Verbundene Plattformen	Offizielle Unterzeichner
PAYIFIC LTD	Keine	www.option888.com www.lottopalace.com www.kuibet.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.optionstarglobal.com	Rumen Gogov
COOL MARKETS OU	Matching Blue Consulting slr	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

161. The criminal investigation revealed that each of Payvision's onboarded merchants to process Lenhoff's resp. Barak's brands were:

- a phony company that has just been created or acquired without any business history;
- without any employees and an actual place of residence;
- without business plans, without any accounting records;
- and with straw men - some of them homeless - as managing directors and beneficial owners;
- the onboarded merchants had no office space and no websites;
- The bank accounts of these inactive companies were all in Sofia, Bulgaria, with the same bank.
- None of these companies had a license as a financial service provider.
- None of these companies had a license to offer resp. to offer binary options (financial instruments) to retail customers.

162. Most websites (=platforms) had offshore companies as official owners that did not coincide with the merchants onboarded by Payvision.

163. For example, New Markets SA, Republic of SAMOA, was the official owner of the website www.optionstarglobal.com from 2016 to 2018. The onboarded merchant for the payment processing for the website www.optionstarglobal.com was the phony online merchant Markets Development EOOD, Bulgaria.

164. The fraud platform www.xmarkets.com was owned by Capital Force Ltd, Republic of SAMOA (Appendix 4)¹¹. The phony merchants onboarded by Payvision for processing the card transactions of the scam website www.xmarkets.com were Celtic PAY Ltd, London resp. Hithcliff Ltd, London.

165. The owning companies displayed on the scam websites and the merchants were changed over time depending on the extent of the negative rating response. in dependence on the number of warnings published about the specific scam website.

166. In the case of the LENHOFF brand "Option888", the operating companies changed when public warnings were published by financial market regulators. Operating companies of this "brand" were Altair Entertainment NV, Netherlands (Curacao), NOVOX Capital Ltd, Capital Force Ltd., Samoa, Celestial Trading Ltd, Seychelles, and Payific Ltd. Malta (ON 912 S 99; ON 167 S 247f).

¹¹ 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.



167. If a new merchant got onboarded by Payvision, the ex-contracting companies were usually deleted from the Companies House register within a few months due to missing reporting requirements. Examples are Hithcliff Ltd and/or Celtic PAY Ltd.
168. The fraudulent schemes were structured with EU sham companies at their core because the ultimate beneficiaries of the payments received from “investors” would not have been able to receive credit card payments themselves. This was because the recipient of the credit card payments (onboarded merchants) needed to be based in the EUR to have a payment processing agreement with an acquiring bank. The Acquiring bank is, in effect, a “middleman” that receives the money from the credit card company of the victims and then forwards the money to the sham companies

169. Payvision used multiple different MIDs for the same merchant, an evident violation of the Card rules.

Merchant (GoldenMarkets)	Acquirer	MID
Matching Blue Consulting S.L.	Payvision	75076380
Matching Blue Consulting S.L.	Payvision	75082164
Cool markets OU	Payvision	75071753

Merchant (SafeMarkets)	Acquirer	MID
Optiumcommerce OU	Payvision	75071662
Optiumcommerce OU	Payvision	75082172

Merchant (XFX)	Acquirer	MID
GPay Ltd	Payvision	75068833
GPay Ltd	Payvision	75075614
GPay Ltd	Payvision	75080101

Merchant (OSG)	Acquirer	MID
Markets Development (Optionstars)	Payvision	75021844
Markets Development (Optionstars)	Payvision	75021828
Markets Development (Optionstars)	Payvision	75021836
Markets Development (Optionstars)	Payvision	75029318

170.

171. The MID is a merchant identification number. It is a unique authorization number provided to the merchant by their payment processing provider. A MID allows the merchant to securely accept credit and debit card payments and process electronic transactions.

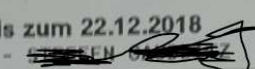
172. Every Merchant MID is utilized to identify a specific business during the MID payment. The merchant's number is transferred to third parties involved in the MID payment

process when the consumer purchases. Merchant ID also verifies the legitimacy of the business to the consumer's issuing bank.

173. Merchant Account ID might seem similar to Merchant ID, but these two banking terms are different. MID is given to each merchant that operates with electronic payments, while Merchant Account ID is issued when the merchant handles various businesses or transaction types within one gateway. For example, sub-brands can have individual merchant account IDs, but one merchant ID is connected to the leading brand.

Dozens of different billing descriptors set by Payvision for the card transactions processed

174. Billing descriptors appear on the card statements of the consumers and are set up when the merchant account is established. The card customer uses it to identify to whom payment was made on a particular transaction.



Buchungs-Datum	Kauf/Beleg-Datum	Leistungsbeschreibung	Ort	Betrag
Abrechnung / Saldenmittlung bis zum 22.12.2018				
MasterCard 5490 06XX XXXX 2357 - XXXX CH 0000				
				in EUR
		Saldovortrag vom 22.11.2018		0,00+
26.11.	23.11.	Safemarkes	TallinnCity EE	2.000,00-
05.12.	04.12.	XXXXXXXXXX	XXXXXXXXXX	XXXXXX

Seite 2 von 2

Einkauf	Text	Belastungen CHF	Gutschriften CHF	Buchung
SALDOUEBERTRAG VON LETZTER SEITE		22'129.70	1'824.15	
01.11.17	OptionStarsGlobal 442080687603 BGR Bankdienstleistungen Umrechnungsdatum: 01.11.17 zum Kurs 1.1840 + 1.75% Bearbeitungszuschlag	EUR 1'000.00	1'204.62	02.11.17

175. The term used is typically the website's trading name rather than the legal name of the owning company so that the customer can easily recognize the payment. The billing descriptor may also be made up of a soft or dynamic descriptor that includes the name of the service provided; this is often used by large companies that offer many services and where the brand of the service is more familiar than the company name.
176. Dozens of different Billing descriptors for card processing were set by Payvision for Barak and Lenhoff's scam websites, an evident sign of irregularities.

177.**OptionStarsGlobal:** OptionStarsGlobal, 442080687603 BG; OptionStarsGlobal, 442080687603 BGR, OptionStarsGlobalFBX*OptionStarsGlobal 442038070647 GBR; OSTARS 442038070647; OSTARS 44203767791

Safemarkets: Safemarkets TallinCity, Safemarkets 10117 TallinCity EST; safemarkes TallinCity EE

Xtraderfx: Cryptopoint 442033183272; Cryptopoint 442033183272 GBR; xtraderfx W3 GAY 442033183272 GBR; Cryptopoint, W3 GAY 442033183272, GBR; xtraderfx,442033183272; xtraderfx/+442033183272; xtraderfx 442033183272 GBR; INTL xtraderfx 00507750420; xtraderfx; VISA xtraderfx;

Option888: Option888, Haslemere; Option888 Gzira MLT; Option888 Gzira MT; Option888 BIRKIRKARA; Option888 BIRKIRKARA 046; Option888, GU27 zLA Haslemere, 6BR; Option888 London

Tradovest: Tradovest 442037691058; Tradovest Doncaster; Tradovest

Tradeinvest90: Tradeinvest90 442080685120

Goldenmarkets: Goldenmrks

False Merchant Category Codes set by PAYVISION for the card transactions processed (MISCODING)

178.A Merchant Category Code (MCC) is a four-digit number used by card payment brands (VISA and Mastercard) to classify a business by the goods or services it provides. The MCC is defined by the acquirer when onboarding the merchant.

179.MCCs are used to categorize, track, and restrict transactions. Issuers rely on the MCC to deny illegal transactions for their customers – if the purchase of the products or services is unlawful in their jurisdiction.

180.In Booker’s statement to the Austrian law enforcement agency as of 23 May 2019 (Appendix 1), he confirmed that he was aware that Barak and Lenhoff offered and sold binary options on the scam websites serviced by Payvision.

181.Booker told the Austrian law enforcement agency that Lenhoff and Barak informed Payvision in March 2018 that they would stop the binary options business in light of the upcoming legislation, which is due to come into force in July 2018¹². They agreed to switch from binary options to crypto trading and CFD products. Under these new

¹² They referred to the ESMA ruling that the offering and marketing of binary options to retail customers was no longer permitted starting with July 1 2018.

terms, according to Booker, Payvision was able to accept to continue processing for Barak and Lenhoff¹³.

182. 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 no mention of binary options in the communication between the clients/victims and the boiler room employees of Barak and Lenhoff. Only investments in financial instruments of various kinds were discussed, offered, and sold.
183. None of Payvision's merchants listed had a license enabling them to operate as a money-transmitting business in the relevant jurisdictions.
184. None of Payvision's merchants listed in the list of merchants provided by Booker had a license to market or sell financial instruments (binary options are classified as financial instruments within the EU) to EU consumers. Also, the operating companies listed on the scam websites –mainly located in offshore countries like the Marshall Islands or the Republic of Samoa – had no licenses to offer or sell financial instruments.

¹³ The criminal files show evidence that no change in the business activity of the different websites took place after June 2018.

Transactionsdaten

<https://b2b.worldline-connect.com/argos/table/select-line.do?sessionId...>

Transactionsdaten

Kartennummer	4263-5401-1500-7337	Acquirer Country	528	NIEDERLANDE
Fild	42635401	Acceptor Country	470	MALTA
		Acq ID	476666	
Iss ID	426354	Mandant		
	COMDIRECT BANK AG PASCALKEHRE 15 QUICKBORN 25451 GERMANY 10034472	Terminal ID	PAYVISION	
		Card Acceptor ID	000103375014336	
		Location/Name	OPTION888	
Txn Code	014213	MCC	6211	WERTPAPIERHÄNDLER, SICHERHEITEN
	eCommerce Standard Authorization Request	Händler Name	OPTION888	
Referenzbetrag	2.000,00 EUR	VU Straße		
Card Exp	2001	VU Stadt	BIRKIRKARA	
Auth Sys Time	07.07.2017 20:32:12	Product Account Id	97467479	
Local Time	07.07.2017 18:32:11			
Req Amount	2.000,00 Euro (978)			
Bill Amount	2.000,00 Euro (978)			
Payout Amt DCC	()			
POS	01	Manuelle Eingabe		
POS PIN	2	Nein, Terminal ohne PIN Tastenfeld		
PIN CHKR	0	Unbekannt		
PIN RES	0	Unbekannt		
PIN# CHKR	0	Unbekannt		
PIN# RES	0	Unbekannt		
Iso Response Code	00	Balance Account	0,00 Euro (978)	
Standin Reason		Unmatched	0,00 Euro (978)	
Auth Code	768684	Credit Available	2.100,00 Euro (978)	
zusätzl. Daten		Credit Limit	2.100,00 EUR Euro (978)	
Resp Code	0	Approved		
ECI	07			
Security Type	31			
Result Type	A			
Result Code	APP_OLW_O			

185. Payvision purposefully classified the services sold by Barak and Lenhoff's scam websites (option888, Tradovest, Tradeinvest90, xtraderfx, goldenmarkets, safemarkets, and OptionStarsGlobal) with 6211 (Security Brokers/Dealers). The MCC 6211 is commonly applied to merchants' accounts of businesses engaged in financial services such as securities, investments, forex, and CFD. Both Mastercard and VISA require that Merchants classified with 6211 are licensed in all jurisdictions; they sell and broker securities, stocks, bonds, commodities, and mutual funds.

Association to Combat Cybercrime against Retail Investors and Consumers
Non-governmental organization to combat cybercrime, ZVR 1493630560, Vienna, Austria
www.efri.io, email : office@efri.io

04.06.18	OptionStarsGlobal 442080687603 BGR Bankdienstleistungen Umrechnungsdatum: 04.06.18 zum Kurs 1.1746 + 1.75% Bearbeitungszuschlag	95	EUR 15'000.00 ✓	17'925.81	05.06.18
04.06.18	OptionStarsGlobal 442080687603 BGR Bankdienstleistungen Umrechnungsdatum: 04.06.18 zum Kurs 1.1746 + 1.75% Bearbeitungszuschlag	96	EUR 15'000.00 ✓	17'925.81	05.06.18
04.06.18	OptionStarsGlobal 442080687603 BGR Bankdienstleistungen Umrechnungsdatum: 04.06.18 zum Kurs 1.1746 + 1.75% Bearbeitungszuschlag	97	EUR 15'000.00 ✓	17'925.81	05.06.18
04.06.18	OptionStarsGlobal 442080687603 BGR Bankdienstleistungen Umrechnungsdatum: 04.06.18 zum Kurs 1.1746 + 1.75% Bearbeitungszuschlag	98	EUR 15'000.00 ✓	17'925.81	05.06.18

186. By miscoding the country of activity and the kind of business activities, Payvision succeeded in deceiving the European banks (issuing banks of thousands of European consumers) about the true nature of the financial transactions they were processing.

RED FLAGS: Some of the public warnings issued by supervisory authorities against the scam websites serviced by Payvision for offering unlicensed financial services in their jurisdictions:

- Already on 2 February 2012, the Autorite des marches Financiers (AMF) issued a warning for the unauthorized website www.optionbit.com.
- As of 10 December 2014, the Gibraltar Financial Services Commission (FSC) from British Columbia issued a warning on www.optionbit.com¹⁴ (the operating company was Top Volume Solutions Limited).
- On 6 December 2016, the Canadian British Columbia Securities Commission warned against Option Stars and OptionStarsGlobal, owned by NOVOX Capital Ltd.
- On 28 December 2016, the Danish FSA warned against Lenhoff's Altair Entertainment N.V., Capital Force Ltd, and **Payific Ltd.**
- Die MSFA (Malta regulator) issued a warning against Altair Entertainment N.V., Capital Force Ltd, and **Payific Ltd.** also as of 28 December 2016.

¹⁴ <https://www.fsc.gi/news/online-binary-options-trading-platforms-5>

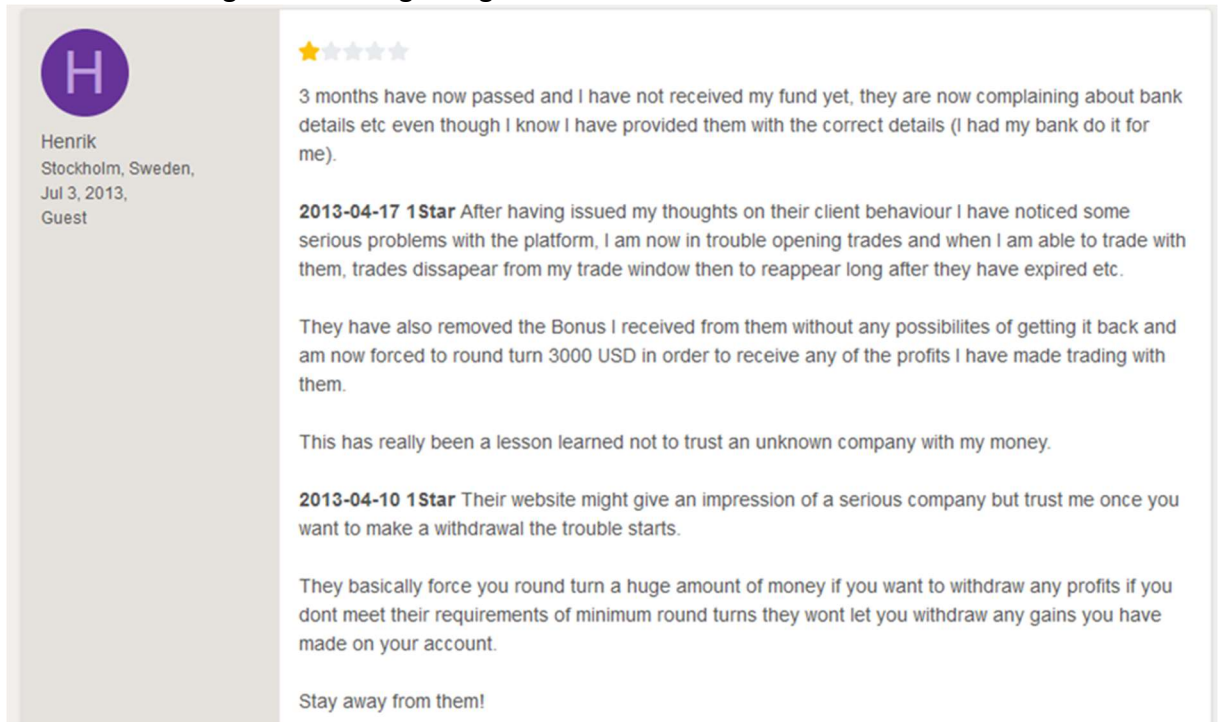
- On December 28, 2016, the Italian CONSOB (Italian regulator) warned against Altair Entertainment N.V. Capital Force Ltd, **Payific Ltd**, for offering unlicensed financial services.
- On 25 November 2017, the Austrian FMA issued a warning for option888 and its operating company Capital Force Limited.
- On February 14, 2018, the UK FCA issued an investor warning against the Xmarkets scheme of LENHOFF for offering unlicensed financial services.
- On April 9, 2018, FCA UK warned against BARAK's AlmaMarket Ltd, UK, and its scheme SafeMarkets for offering unlicensed financial services.
- On January 3, 2018, FCA UK warned against Barak's **OptiumCommerce OU** and its scheme SafeMarkets for offering unlicensed financial services;
- On March 21, 2018, the German BaFin issued an investor warning and a cease-and-desist order against LENHOFF's Capital Force Ltd and its Option888 scheme for offering unlicensed financial services;
- As of 30 March 2018, the Austrian supervisory authority warned against **NEW MARKETS S.A. Republic of Samoa** (OptionStarsGlobal) for offering unlicensed financial services.
- As of 6 April 2018, the Austrian FMA issued a warning for xmarkets.com
- On 9 April 2018, the UK FCA issued a public investor warning against the safemarket scheme;
- On 14 May 2018, the UK FCA issued a public investor warning against BARAK's OptionStarsGlobal scheme for offering unlicensed financial services.
- On 14 May 2018, the UK FCA issued a public investor warning against Barak's **GPay Ltd** and its schemes CryptoPoint, xtraderfx, and XFM;
- On 21 May 2018, the UK FCA issued an investor warning against Lenhoff's Capital Force Ltd and Option888
- On May 25, 2018, the UK FCA issued an investor warning against Barak's **Cool Markets Ltd** and its scheme Golden Markets;
- On June 7, 2018, the UK FCA issued a public investor warning against Barak's **GPay Limited** and its scheme (trading style) xtraderfx;
- On June 13, 2018, the German BaFin issued an investor warning and a cease-and-desist order against Lenhoff's Celestial Trading Ltd and its Option888 scheme;
- On June 13, 2018, The Austrian FMA issued an investor warning against Lenhoff's Celestial Trading Ltd and TradoVest;
- As of 25 June 2018, FCA warned against **NEW MARKETS S.A. Republic of Samoa** (brand OptionStarsGlobal)
- On July 6, 2018, the UK FCA issued a public investor warning against Lenhoff's TradoVest scheme;


- On July 11, 2018, the German BaFin issued an investor warning against Lenhoff's Celestial Trading Ltd and its xmarkets scheme;

187. Merchant/brands/owners matched entries appearing on applicable watch/sanctions list already when Payvision onboarded these merchants. The billing descriptor applied always matched the warnings for the brand in addition.

Customer complaints and negative reviews on different websites

188. Consumer complaints about the fraudulent brands serviced by Payvision since 2013 have been flooding from the beginning.

A screenshot of a 1-star review on a website. On the left, there is a profile section with a purple circular icon containing a white 'H', the name 'Henrik', location 'Stockholm, Sweden', date 'Jul 3, 2013', and the title 'Guest'. To the right of the profile, the review text is displayed. It starts with a 1-star rating (one yellow star, four grey stars) and a paragraph of text. This is followed by a date and star rating '2013-04-17 1Star' and another paragraph. Then, another paragraph follows. This is followed by another date and star rating '2013-04-10 1Star' and a paragraph. Finally, there is a concluding paragraph. The review text describes a negative experience with a company, mentioning issues with funds, trading, and bonuses.

 3 months have now passed and I have not received my fund yet, they are now complaining about bank details etc even though I know I have provided them with the correct details (I had my bank do it for me).

2013-04-17 1Star After having issued my thoughts on their client behaviour I have noticed some serious problems with the platform, I am now in trouble opening trades and when I am able to trade with them, trades dissappear from my trade window then to reappear long after they have expired etc.


They have also removed the Bonus I received from them without any possiblites of getting it back and am now forced to round turn 3000 USD in order to receive any of the profits I have made trading with them.

This has really been a lesson learned not to trust an unknown company with my money.

2013-04-10 1Star Their website might give an impression of a serious company but trust me once you want to make a withdrawal the trouble starts.

They basically force you round turn a huge amount of money if you want to withdraw any profits if you dont meet their requirements of minimum round turns they wont let you withdraw any gains you have made on your account.



Stay away from them!

A circular profile picture with a green background and a white letter 'N'.

Nguyen
Sai Gon, Viet Nam,
Apr 21, 2015,
Guest

★☆☆☆☆

I'm a victim of the Optionbit. anyone can help me to get my money back?
I have funded 500AUD and claim 150% bonus (the bonus is not redeemable). After 2 very success trading, my account balance was 6990 AUD, and the turnover I have traded fulfilled the requirement for withdraw fund. I have submitted a withdrawal request for 6950 AUD, but they decided to close my trading account and transferred 3048.6 AUD to my Netteleer account only.
They told me that I have used abusive trading patterns, so they took almost 4000 AUD from my account.
I have never used abusive trading patterns (never use any kind of robots, trading systems) as they told me. I have sent them emails to give me proof of using abusive trading patterns, but they never reply to me.
Please help me to get my money back from them
Thank you
Nguyen

A small icon of two arrows pointing outwards.ShareA small icon of a thumbs up.Helpful

Excerpt: Binary options as a high-risk business area

189. Binary options are an investment product that enables traders to bet on yes-or-no outcomes. For example, a trader could buy a binary option stating that the price of a particular stock will go up 5% or more in a day. The option has pre-determined payout odds and does not involve the trader taking a direct position in the underlying assets, unlike traditional options contracts. Binary options have no connection to the underlying asset or event
190. Binary options via websites have enjoyed increasing popularity among small investors due to the low capital investment required, their gambling character, and the supposed simplicity of use (there are only two scenarios that investors can bet on: rising and falling prices).
191. A slightly more complex version of a binary option is the “contract for differences” (CFD). Like binary options, CFDs are cash-settled and never result in any delivery of the underlying security. Unlike binary options, the payout or loss on a CFD tracks the price movement of whatever the underlying asset might be. Consequently, the payout or loss on a CFD is uncapped.
192. In the fall of 2013, the United States banned the over-the-counter offering of binary options to its retail investors due to the obvious potential for abuse and the high levels of fraud experienced by small investors.
193. Both binary options and CFDs are illegal in the United States. However, a massive binary options industry in Europe has flourished for over a decade. Many of the firms in the

Association to Combat Cybercrime against Retail Investors and Consumers
Non-governmental organization to combat cybercrime, ZVR 1493630560, Vienna, Austria
www.efri.io, email : office@efri.io

binary options space originated in Israel. By the mid-2010s, the binary options industry employed thousands of people in multiple countries and generated millions of annual revenues.

194. In 2016, a bombshell exposé¹⁵ by Simone Weinglass/Times of Israel revealed that many binary options firms were engaging in consumer fraud. Operating massive call centers (aka boiler rooms) reminiscent of a scene from The Wolf of Wall Street, the firms would cold-call people across Europe and use high-pressure tactics to convince their marks to try trading binary options products. If investors later tried to withdraw their deposited funds, the firms would stall them or, in some cases, simply abscond with the money.
195. After a series of reports by The Times and other media outlets in 2017, the Knesset responded by outlawing Israel's binary options industry¹⁶. However, binary options-style scams flourished throughout Europe, frequently operating out of Eastern European nations with limited regulatory capabilities.

Warnings issued by supervisory authorities worldwide for binary options trading platforms

- In early 2013, the U.S. Commodity Futures Trading Commission (CFTC) warned investors about fraudulent schemes affecting binary options and their trading platforms. These systems include refusal, withdrawal of winnings and refund of funds, identity theft, and manipulation of software to generate lossy trades.
- On September 28, 2017, the Canadian Securities Administrators (CSA) also issued a ban on the marketing, offering, and trading of binary options that have a maturity of fewer than 30 days for retail investors (Multilateral Instrument 91-102 Prohibition of Binary Options), as they usually only run for hours or minutes. This resulted more or less in a total ban on binary options in Canada. The CSA stated that binary options are the leading type of scam Canadian consumers face. The impact of these scams on consumers was increasing sharply. 17 CSA stated binary options were inappropriate for retail investors due to the risky specifications.
- In the Czech Republic, the competent national authority, the "National Central Bank" (CNB), published an opinion in October 2015 to warn retail investors of the risks associated with binary options.

¹⁵ <https://www.timesofisrael.com/the-wolves-of-tel-aviv-israels-vast-amoral-binary-options-scam-exposed/>

¹⁶ <https://www.timesofisrael.com/israel-bans-entire-binary-options-industry-finally-closing-vast-10-year-fraud/>

¹⁷ <https://www.securities-administrators.ca/news/canadian-securities-regulators-announce-ban-on-binary-options/>

- In the summer of 2016, ESMA (European Securities and Markets Authority) issued a warning for highly speculative and risky investments, citing binary options unsuitable for retail investors.
- In August 2016, the Belgian national competent authority, the Financial Services and Markets Authority (FSMA), put into effect the ban on distributing certain specific over-the-counter derivative contracts (including binary options) to retail consumers in Belgium. In addition, the BE-FSMA defined several aggressive or inappropriate distribution techniques, such as cold calling inappropriate forms of remuneration and fictitious gifts or bonuses.
- Since December 2016, providers of investment services have been prohibited by French legislation from providing marketing communications to individuals relating to binary contracts, among other things.
- In Spain, since March 2017, the competent national authority, the "Comisión Nacional del Mercado de Valores" (ES-CNMV), has required investment firms distributing CFDs or Forex products with leverage (leverage) of more than ten to one or binary options to retail clients domiciled in Spain to provide their clients with extensive warnings regarding the complexity, high risk, and cost of these products.
- In Italy, the competent national authority, CONSOB, published a specific communication in February 2017 to warn Italian retail investors of the risks associated with binary options.
- In February 2018, the Portuguese CMVM published a circular requiring investment firms to refrain from providing investment services related to derivatives linked to cryptocurrencies if they do not comply with all information obligations regarding the characteristics of the products to their clients.
- On 10 May 2017, the Hellenic Republic Capital Market Commission HCMC, issued a circular on the provision of investment services in over-the-counter derivative financial instruments (including Forex, CFDs, and binary options) traded via electronic trading platforms, highlighting the susceptibility to fraud of these electronic trading platforms.
- In the Netherlands, the competent national authority, the Autoriteit Financiële Markten ('NL-AFM'), published a consultation paper in February 2017 proposing to subject certain products, including binary options, to an advertising ban due to the high risk of fraud and loss for retail investors.
- The UK-FCA also published a consumer warning on 14 November 2017 about the risks of investing in binary options.
- In December 2016, the Austrian FMA warned about the risks associated with CFDs, rolling spot forex transactions, and binary options.

- On 27 March 2018, ESMA (European Securities and Markets Authority) announced an early ban on the marketing, distribution, and sale of binary options to retail clients, again citing the high risk of fraud and loss for retail investors.
- On 22 May 2018, by Decision (EU) 2018/795, ESMA made use of its direct intervention in the European financial market for the first time and only time to date. Under Article 40, Markets in Financial Instruments Regulation (MiFIR, imposed a (temporary) prohibition on the marketing, distribution, and sale of binary options to retail consumers and provided for restrictions on CFD trading. The emergency measure was justified by increased fraudulent offers in this area and the associated high losses of European private investors, aggressive marketing practices, and misleading marketing communications in the market sector. With effect from 02.07.2018, this ban was implemented by ESMA throughout the EU.
- The ban on distributing, marketing, and selling binary options to retail clients was originally in force from 2 July 2018 to 1 October 2019. Still, it was extended three times by ESMA for three months each.
- Until 1 July 2019, the ban on distributing and offering binary options to retail investors in individual European countries was implemented by the national authorities.

196. Considering the (publicly) well-known high risk of fraud with binary options activities, Payvision had an evident responsibility to assure legitimacy before onboarding new merchants in this business field.
197. Payvision understood the risk associated with doing business with the binary options merchants. Payvision was aware of the general industry warnings. As early as 2014, Payvision knew that binary options merchants were not onboarded by other payment institutions.
198. Payvision's compliance department must have found readily identifiable evidence of red flags of large-scale money laundering.
199. [Searching for red flags, e.g., suspicious addresses](#), and adopting stricter measures to enhance due diligence to combat illegal acts is crucial when serving high-risk merchants.
200. The high-risk classification enhanced transaction monitoring of activity within Barak and Lenhoff's accounts. However, as discussed below, this required monitoring scrutiny was not followed.

Additional RED FLAGS: Payvision signed a new merchant contract with Gal Barak on July 24, 2018

202. On 24 July 2018, Payvision, Gijs op de Weegh signed a new payment processing contract with GPay Ltd, London. Gal Barak signed this contract, although he was not the registered managing director nor the registered beneficial owner of GPay Ltd. The agreement defined new adverse conditions for all scam websites operated by Gal Barak.
203. MCC 6211 is used in this contract, although the products sold are described with "Crypto Trading," pretending that GPay Ltd had a license to offer crypto trading products. (In reality, no change in business activities could be noticed in the second half of 2018, according to the scam victims. The boiler room employees still offered alleged financial investment in shares, forex, crypto, and what so ever).
204. In this new contract, the processing fees were agreed at 7% in combination with additional high fixed costs for fee refunds, refund fees, and call-off fees. The agreement also provided a crucial period for a minimum monthly transaction processing volume of EUR 4 million for the next three years¹⁸ (!) for all Barak (!) operated scam websites).
205. Due to new information from a media report of the Dutch FD published on October 14, 2022, about what was going on within Payvision's compliance department in July 2018, this new contract, signed only five days after Rudolf Booker told his compliance

¹⁸ Everyone in the high-risk business is aware that the the life-time for scam websites is up to one year.

department to "Release all credit," has to be seen in a different light:

For example, there is the British start-up **GPay Ltd.** which trades in cryptocurrency-based binary options through the obscure website Cryptopoint. GPay is eager to become a customer, but Greeuw has a bad feeling about the company with its opaque ownership structure with Bulgarian owner and Israeli contact. GPay provides little financial information. In addition, crypto trading is the subject of numerous court cases against operating startups. In Janner 2018, its verdict is therefore: reject for lack of transparency.

But in April, three months after the takeover of Payvision by ING, the colleagues nevertheless bring GPay on board. For business reasons," one of them explained in an e-mail at the end of June. By then, there was already fire under the roof: in May, the UK regulator FCA issued an official warning: GPay is not licensed for crypto trading and is therefore illegal. Its business model may be fraudulent.

Greeuw and his colleagues switch to escalation mode, but GPay won't show where the money is coming from. Enough is enough for Greeuw. 'We need to terminate them asap,' he emails his team members in late June: 'Alie new transactions and block the funds.' Now all that's left is for the management to give the green light.

Nearly three weeks later, on **July 19, Rudolf Booker** made a judgment: 'Release all credits.' He was Booker is "informed about all issues" with Gpay, his right-hand man informs. We will continue to work with them for the time being," Booker emails. That is enough for Greeuw. A month later he announces. Greeuw did not respond to FD's requests for comment.



INFO@PAYVISION.COM
WWW.PAYVISION.COM



APPENDIX 1

Service Fees and Reporting

Merchant details:

Company name : GPAY LTD
Payvision client number : 323973
Payvision sales office : Amsterdam
Address : Churchfield Road, 47
Postal code : W3 6AY
City : London
Country : United Kingdom
Contact person : Gal Barak
Contact email : Bark.gal@gmail.com

Credit Card processing via **Payvision**. Fees specified herein will be included in the reconciliation report provided by Payvision, or, as the case may be, shall be specified in an invoice as set forth in the Agreement and may be deducted from any Settlements as per the Agreement. All fees are exclusive of Value Added Tax. Notwithstanding anything to the contrary contained in this Appendix or the Agreement, should there be any inconsistency or conflict with respect to (a) any provision of this Appendix and (b) the Agreement, for the purpose of this Appendix, (b) shall prevail over (a).

MCC code	6211
Products sold	Crypto Trading
Descriptor	Cryptopoint
Website(s)	cryptopoint.com
Cards accepted	Visa and Mastercard
Approved monthly volume	EUR 4.000.000,00
Approved highest ticket size	EUR 15.000,00
Discount % (per card type)	<EUR 5.000.000,00 - IC++ 7,00% EUR 5.000.001,00 - EUR 7.500.000,00 IC++ 6,50% EUR 7.500.001,00 - EUR 10.000.000,00 IC++ 6,00% EUR 10.000.001,00 - EUR 12.500.000,00 IC++ 5,50% EUR 12.500.001,00 - EUR 20.000.000,00 IC++ 5,00%
Rolling Reserve	7% rolling reserve for 6 months, 7 days delayed payment
Funding	Weekly
Average transaction amount	EUR 250,00
Processing currency	EUR
Settlement currency	EUR
Annual fee	EUR 500,00
Chargeback fee	EUR 24,00
Pre-arbitration fee	EUR 24,00
Retrieval fee	EUR 5,00
Refund fee	EUR 1,30
PCI-registration platform fee	Included in price (using Payvision/ControlScan PCI-registration platform is mandatory)
PCI non-compliance fee (per month)	EUR 50 (based on PCI compliance status in Payvision/Controlscan platform)
Settlement bank account holder	GPAY LTD
Bank account number	1488911800
IBAN number (and/or bank sort code)	BG30JORT80481488911800
BIC/SWIFT code	JORTBGSF
Settlement bank name	INVESTBANK JSG
Bank address / City / Country	blvd Bulgaria 85, 1000 Sofia, Bulgaria



INFO@PAYVISION.COM
WWW.PAYVISION.COM

PAYVISION
Global Card Processing

67

Additional Terms:

Each of Gpay LTD, Optiumcommerce OU and Cool Markets OU hereby, jointly and severally, commits to process payment transactions with Payvision exclusively for at least three (3) years as of the effective date of the merchant agreement (i.e. DATE July 2018). Gpay LTD, Optiumcommerce OU and Cool Markets OU, jointly and severally, commit to process a minimum monthly volume of EUR 4,000,000.00 with a rampup of 6 months starting July 24th 2018.

In the event Gpay LTD, Optiumcommerce OU and Cool Markets OU process less than the minimum volume commitment measured in any twelve (12) month contract year, the parties will elect that either (i) Payvision shall invoice Gpay LTD, Optiumcommerce OU and Cool Markets OU for the difference between the aggregated volume processed in such contract year and the minimum processing commitment, and Gpay LTD, Optiumcommerce OU and Cool Markets OU shall pay Payvision within ten (10) business days after receipt of Payvision's invoice, or (ii) the prices set forth in each Appendix 1 shall be adjusted accordingly.

Gpay LTD will have the same liabilities and obligations as Optiumcommerce OU and Cool Markets OU in respect of the abovementioned commitments. Gpay LTD confirms it has been given and read a copy of the Appendices 1 of Optiumcommerce OU and Cool Markets OU and covenants with Payvision to perform and be bound by all the terms of such Appendices 1 and named in such Appendices 1 as if Gpay LTD was a party thereto to the intent it shall be bound by and entitled to the benefit of such Appendices 1 as if it were a party thereto and named in such Appendices 1 as an obligor. Additional brands may be added.

On behalf of **PAYVISION**

Date: July 24th 2018
Name: Mr. G. op de Weegh
Title: COO

Signature

On behalf of **GPAY LTD**

Date: 24.07.18
Name: Gal Barak
Title: _____

Signature

Remittances to non-related companies on Barak and Lenhoff's instructions

206. The cash flows of the stolen money traced by the criminal agencies in Austria and Germany revealed that Payvision transferred a substantial part of the remittances (stolen victims' money) to phony companies without any contractual relationship, just on instructions received by Barak and Lenhoff.

207. Booker informed the criminal agencies about some of these transfers in his statement as of May 2019 by talking about transfers to "affiliated companies."

- So Payvision transferred more than 2 million euros of the remittances to the Bulgarian bank account of Rockarage Ltd. in the period 4 October 2017 and 17 April 2019. Rockarage Ltd, an "affiliated company," had its registered office in the Marshall Islands and was displayed as the official "owning company" for the scam website www.safemarkets.com. PAYVISION had no contractual relationship with this company.

9 St 3/20b Beilage M1 387

Rockarage Ltd
BG931ORT80481488922500
Währung: EURO
Zeitraum: 04.10.2017 - 17.04.2019

EINGÄNGE				AUSGÄNGE			
Zeilenbeschriftungen	Daten	Summe	Anz	Zeilenbeschriftungen	Daten	Summe	Anz
STICHTING TRUSTED THIRD PARTY PAYVISIO		2.275.000,00 €	5	ARC SOLUTIONS D.O.O.		941.158,00 €	27
NL09DEUT0265137020		2.275.000,00 €	5	BA391994990010346618		941.158,00 €	27
BINEX GROUP LP		1.600.640,24 €	42	TRANSCONNECTION LIMITED		594.518,62 €	21
GB07CNN00998354100035		1.600.640,24 €	42	023293764838		594.518,62 €	21
OPTIUMCOMMERCE OU		1.386.380,00 €	26	MARINA IVANOVA ANDREEVA		551.500,00 €	24

208. In his statement, Booker missed disclosing additional transfers made to companies under the direct influence of Uwe Lenhoff and Gal Barak. Also, these non-disclosed transfers were done to pure sham companies not based in Europe:

- The cash flows also revealed that Payvision transferred 4.4 million euros from the merchant account to the Bulgarian bank account of Winslet Enterprises EOOD, Bulgaria (BG67STSA93000024171778) between February 2018 and May 2018. The transfers were marked as "profit distribution." Payvision had no contractual relationship with this company.
- Furthermore, it was revealed that PAYVISION transferred 15,3 million euros to a bank account of NEW MARKETS SA, the Republic of SAMOA, from February 2017 to June 2018 based on a scrap of paper (Appendix 10) signed by Rumen Gogov (general manager of the Bulgarian sham company Markets



Development EOOD. NEW MARKETS SA, SAMOA, was founded in 2017 and was displayed on the website www.optionstarsglobal.com as the operating company. Payvision had no contractual relationship with this company.

Witness statement of Rumen GOGOV

209. The Bulgarian Rumen GOGOV was the registered managing director of Markets Development EOOD, the merchant onboarded by Payvision to process the card payments for the scam website OptionStarsGlobal. The total card payment volume processed on behalf of this sham merchant amounted to 28.101.859,97 euros.
210. Already during the criminal investigations relating to Barak, Rumen GOGOV witnessed that he never talked to Payvision and that he does not even know about the business activities of Markets Development EOOD.
211. During civil proceedings in Austria, Rumen GOGOV witnessed again that he never was in contact with Payvision and that he had not signed the paper to transfer the remittances to the company located in the Republic of SAMOA. He does not speak English, nor does he write in English. BOOKER produced this scrap of paper in his interrogation by the Austrian law enforcement, it was not found during the raids at

Barak's offices in Bulgaria.

Prepared for : Payvision

Date: 13-10-2016

Transfer of funds

I am writing this Instruction Letter to you in my capacity as a director of Markets Development Ltd. based in Bulgaria with registered company number 203951019 and with registered address at Vitosha Blvd 66, 1000, Sofia. I hereby would like to request Payvision BV to settle all funds to the bank account of New Markets SA, based in Samoa with registered company 70612 and with registered address at Novasage Chambers, Level 2, CCCS Building, Beach Road, Apia, New Markets SA is a parenting company.

I confirm that the boards of both companies are fully aware of and have authorised this arrangement and I also confirm that the arrangement should stay in place untill revoked or varied in writing by myself or other duly authorised representative of either company.

A handwritten signature in black ink, appearing to be "Rumén Gogov", written over a horizontal line.

Signature

Date: 13-10-2016

Name: Rumén Gogov

Title: Director

PAYVISION also provided payment gateway and alternative payment services for Barak and Lenhoff's scam websites and wactively rerouted transactions.

212.A payment gateway facilitates a payment transaction by transferring information between a customer, a website, and the front-end processor (acquiring bank).

213.When a customer orders a product from a payment gateway-enabled merchant, the payment gateway performs various tasks to process the transaction.

- A customer places an order on the website by pressing the 'Submit Order' or equivalent button or perhaps enters their card details.
- If the order is via a website, the customer's web browser encrypts the information sent between the browser and the merchant's webserver. In between other methods, this may be done via SSL (Secure Socket Layer) encryption. The payment gateway may allow transaction data to be sent directly from the customer's browser to the gateway, bypassing the merchant's systems. This reduces the merchant's Payment Card Industry Data Security Standard (PCI DSS) compliance obligations without redirecting the customer away from the website.
- The merchant then forwards the transaction details to their payment gateway. This is another SSL-encrypted connection to the payment server hosted by the payment gateway.
- The payment gateway converts the message from XML to ISO 8583 or a variant format (format understood by EFT Switches). Then it forwards the transaction information to the payment processor used by the merchant's acquiring bank.
- The payment processor forwards the transaction information to the card association (i.e., Visa/MasterCard/American Express).
- The credit card issuing bank receives the authorization request, verifies the credit or debit available, and then sends a response back to the processor (via the same process as the request for authorization) with a response code (i.e.: approved, denied).
- The processor forwards the authorization response to the payment gateway.
- The payment gateway receives the response and forwards it to the website or whatever interface was used to process the payment. It is interpreted as a relevant response, then relayed back to the merchant and cardholder. This is known as the Authorization or "Auth."

214. Scam websites usually use several different payment service providers with different payment gateways and with different acquirers connected – this is also termed load balancing: a common practice in online commerce, where a merchant's transactions are spread across different banks to also spread the risks of any payment defaults.

215. Payment gateways enable scammers to efficiently route transactions to other acquirers (with different MCCs) and to reroute efficiently declined transactions.

216. Rerouting is necessary when transactions are declined by issuing banks for different reasons, mainly based on the MCC.

217. The more different PSPs and payment gateways, the more victims can be addressed, transactions can be processed, and money can be laundered.

218. Barak engaged the services of Fibonatix, Payvision, Dcashier, and PaymentIQ

219. The below picture is taken from the deposit list of Tradologic's CRM System for the deposits of Barak's victims.

2	NULL	EUR	Mastercard	WaitingForC	4	20.09.2018	Payvision2	1	91	SB.PeterB	NULL	80.151.52.11	14:31,7	0b4bbe12cc
2	NULL	EUR	Credit Card	Confirmed	6	12.10.2017	PaymentIQ	0	106	CK.KarenG	TeleMarketi	54.194.243.1	17:01,6	6a98fa97ecc
2	NULL	EUR	Credit Card	Initialized	1	14.11.2016	Fibonatix	0	73	EricD	NULL	217.6.103.1	40:48,4	792824bf16
2	NULL	EUR	Credit Card	Initialized	1	13.07.2015	DCashier	0	19	amandac	NULL	95.208.96.2	33:48,3	1608184
2	NULL	EUR	Credit Card	Confirmed	6	21.02.2017	PaymentIQ	0	106	Kevin.S	TM-First dep	54.194.243.1	05:51,9	a591853935
2	NULL	EUR	Fee	Confirmed	6	29.09.2017	Adjustment	4	22	General_Poc	NULL	NULL	46:52,2	25f5f66b4fb
2	NULL	EUR	Credit Card	Initialized	1	16.12.2015	DCashier	0	19	EricD	NULL	95.91.225.1	33:34,2	1781208
2	NULL	EUR	Wire Transfe	Confirmed	6	04.07.2017	Manual	2	9	IvanA	TM-First dep	94.26.58.20	12:01,0	f290fe6947
2	NULL	EUR	Fee	Confirmed	6	27.06.2018	Adjustment	4	22	SB.Inactivity	NULL	NULL	16:42,4	757ef8dccaC
2	NULL	EUR	Credit Card	Confirmed	6	22.04.2017	PaymentIQ	0	106	IvanA	TM-First dep	54.194.243.1	32:41,1	fb21a1a2eb
2	NULL	EUR	Fee	Confirmed	6	30.01.2018	Adjustment	4	22	General_Poc	NULL	NULL	08:27,8	0150baa437

Cash deposits in bank accounts held by money mules for Barak and Lenhoff's scam websites

220. In addition to credit and debit card payments, the retail investors were induced by Barak and Lenhoff's boiler room employees to deposit material amounts in bank accounts of money mules held with European banks.
221. The setup and coordination of as many money mules with bank accounts as possible is offered by professional money launderers for criminal organizations and is part of the job description of scam payment service providers.
222. Payment gateway providers establish the connection with these money launderers as a service provider.
223. Several accounts with DEUTSCHE BANK (Payvision had its merchant accounts for xtraderfx as well as OptionStarsGlobal with DEUTSCHE BANK up to the end of 2018) were used in the years 2016 – 2019 for deposits of the victims:

1	CONDESK gmbH	DE79440100460409328468	Postbank	xtraderfx, safemarkets	Dortmund
1	Trustsecure Gmbh	DE42370100500980910505	Postbank	safemarket/xtraderfx	Köln
5	Davis Consulting GmbH	DE11440100460414901469	Postbank	safemarkets/xtraderfx	Nürnberg
3	Securityport GmbH	DE63760100850103092854	Postbank	safemarkets/xtraderfs	Nürnberg
7	Optimum commerce - safemarktes	DE63760100850103092854	Postbank	safemarkets	Nürnberg
8	Gpay limited - xtraderfx	DE63760100850103092854	Postbank	xtraderfx, safemarkets	Nürnberg

Also, several ING bank accounts showed up in the criminal files:

- 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 bank account was used for deposits of the victims of the scam website option stars global (Appendix 17.1).
- As early as July 2016, the Times of Israel reported MoneyNetInt's involvement in binary options fraud. In spring 2017, the Polish Financial Supervisory Authority ("KNF") warned about the activities of MoneyNetInLtd.

- 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 scam schemes (including the scams of Barak).
- 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.
- For Stichting WST Capital Ltd, the US CFTC (Commodity Futures Commission) already issued a warning on April 25, 2017,¹⁹ 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 in 2018 and 2019.

Close personal relations between BOOKER/ Barak and Lenhoff

224. The managing directors of the onboarded merchants had no contact with Payvision. This was revealed, for example, in the interrogation of Rumen Kirilov GOGOV (compare above).
225. All day-to-day communication for the parties to Gal Barak's fraud systems was through a Bulgarian employee of Gal Barak (Boyan@Maevar).
226. An employee of Lenhoff made the day-to-day communication for the contracting companies of Lenhoff's fraud systems.
227. 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, terms of new contracts, and in case too many chargeback and fraud complaints got raised by victims.
228. 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.

¹⁹ <https://cftc.gov/node/221151>

229. Intercepted phone calls prove the close relationship between Booker and Lenhoff.

ÜBERSETZUNG/TRANSKRIPTION VON GESPRÄCH NR 714 vom 22.01.2019

U = UWE (LENHOFF)

R = RUDOLF (BOOKER)

R: Hallo, UWE!
Hi!

U: Nein, Du ich glaube, so ist es viel besser!

R: Ja.
Also, ZOOMTRADER war ja schon unter ähhhhh – ich meine, ZOOMTRADER stand ja schon im Eigentum von ähhhhh – bzw. Du hattest das Merchandise für sie, oder?

U: Für ZOOMTRADER?
Aber doch nicht für GLOBAL!
GLOBAL ist ja schon komplett gelaufen!
GLOBAL ist jenes Unternehmen, das komplett im Eigentum von NOVOX steht.

R: Mhm, ja.

U: Denn damals hast Du einen Vertrag mit NOVOX gemacht und diesen Vertrag auch unterschrieben bzw. anschließend die ???URL an sie geliefert – übrigens auch für die OPTION888. Das war ebenfalls unter deren Domain bzw. deren Unternehmen.

R: Mhm, ja.

230. Due to the successful cooperation, an agent agreement between Payvision and Lenhoff was established in July 2018 and signed on 16 August 2018; Payvision undertook to pay a commission for mediating other fraud platforms to Payvision. Plus, notice that Uwe Lenhoff was already a convicted fraudster in Germany before he started his binary options business. (2x)

231. 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.

232. Book's relationship with mainly Lenhoff was critical to Lenhoff and Barak running their illegal operation through Payvision.

Association to Combat Cybercrime against Retail Investors and Consumers
Non-governmental organization to combat cybercrime, ZVR 1493630560, Vienna, Austria
www.efri.io, email : office@efri.io



233. Payvision built the financial infrastructure that allowed for Lenhoff and Barak's operation to become what it was.

234. Despite multiple convictions for fraud in Germany, Uwe Lenhoff was a reseller for Payvision due to his personal relationship with Booker.

Merchant (GoldenMarkets)	Reseller	Acquirer	MID	Account Status	Sett
Cool markets OU		Payvision	75071753	Active (Hld Pay)	EUR
Matching Blue Consulting S.L.	Uwe Lenhoff	Payvision	75076380	Active (Hld Pay)	EUR
Matching Blue Consulting S.L.	Uwe Lenhoff	Payvision	75082164	Active (Hld Pay)	EUR

Merchant (SafeMarkets)	Reseller	Acquirer	MID	Account Status	Se
Optiumcommerce OU		Payvision	75071662	Active (Hld Pay)	E
Optiumcommerce OU		Payvision	75082172	Active (Hld Pay)	E

Merchant (XFX)	Reseller	Acquirer	MID	Account Status	
GPay Ltd		Payvision	75068833	Active (Hld Pay)	
GPay Ltd		Payvision	75075614	Active (Hld Pay)	
GPay Ltd		Payvision	75080101	Active (Hld Pay)	

Merchant (OSG)	Reseller	Acquirer	MID	Account Status	
Markets Development (Optionstars)		Payvision	75021844	Active (Hld Pay)	
Markets Development (Optionstars)		Payvision	75021828	Active (Hld Pay)	
Markets Development (Optionstars)		Payvision	75021836	Active (Hld Pay)	
Markets Development (Optionstars)		Payvision	75029318	Active (Hld Pay)	

Non-governmental organization to combat cybercrime, ZVR 1493630560, Vienna, Austria

www.efri.io, email : office@efri.io

Tons of fraud complaints and chargeback requests

235. A chargeback is a type of return when cardholders ask their card issuers to dispute a transaction from their card statement. The card issuer will ask the cardholder to explain why they are disputing the charge and will inform the acquirer of the chargeback request.
236. The acquirer has to inform the merchant and has to deal with the chargeback complaint and report back to the other credit card scheme participants about the chargeback request received.
237. So Payvision was informed and involved in each single chargeback notification and complaint.
- On 18. In Dezember 2017, AK Vorarlberg turns to the credit card company for the victim Bernd Lamprecht and filed a comprehensive submission. The letter is accompanied by a statement of facts and contains a reference to criminal proceedings against the operators of the fraud website Option888, which has been pending in Austria since 2016 under AZ 2 UT 87/16 with the Austrian prosecutors.
 - On 12. April 2018, Herfurtner Rechtsanwälte submitted a chargeback application for money **laundering and fraud** for the credit card payments made to the platform option888 London (Billing Descriptor) to the credit card issuing Institute Complete Card AG, Vienna, on behalf of the client Gerhard Brandstätter. The application was accompanied by the criminal complaint prepared by the law firm Herfurtner against the binary options platform Option888 created on xxx. Reference was made to the decision of 23.03.2018 of the BaFin Federal Financial Supervisory Authority for the cessation and settlement of the financial commission business of ²⁰**Capital Force Ltd. ("Option888")**. By decision of 21 March 2018, BaFin has abandoned Capital Force Ltd. – commonly known as "Option888" – based in Apia, Samoa, from the unauthorized finance commission business
 - On 23 May 2018, AK Vorarlberg contacted Card Complete on behalf of the injured party Klaus Böhler (Visa account: 4548 2510 0634 1000) with a request for reimbursement of the transferred capital investment. The letter is accompanied by a statement of facts to the STA and contains a reference to criminal proceedings against the operators of the fraud website Option888, which has been pending in Austria since 2016 under AZ 2 UT 87/16v.
 - On 8. October 2018, the customer Complains to Bringezu with a detailed explanation about the method of fraud and speaks of shelf companies.
 - On 27. November 2018, the customer complains about fraud on the fraud website Xmarkets to his credit card company.
 - On 26. January 2018, Herbert Hilscher applied a chargeback to his credit card organization, but the promised repayment was not received.

20

https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/unerlaubte/2018/meldung_180323_capital_force_ltd.html

- On 13 **February 2018**, Herbert Hilscher – customer of the Option888 platform – submitted a new application for a chargeback. Reason: Suspicion of fraud. The ensuing comprehensive discussion on the requested chargeback procedure reflects the platform's approach to ensuring that every cautious and reasonable reader
- On September 27, 2018, Patrick Ho submitted a Charge Back application. His request contained a single word. SCAM!

238. There have been hundreds of them over the years, and Payvision handled all of them.

239. 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 an agent agreement with Lenhoff in the summer of 2018 for the mediation of other fraud platforms indicates the unscrupulousness of Booker.

240. In March 2017, Payvision got high fines set by VISA/Mastercard to show higher Chargeback ratios than allowed. The penalty set was deducted from the Rolling Reserve (funds withheld).

149

Telegram Backup

Dialog with Trinity (@TrinityUP) *Gabriel SHALON*

[Back to the overview](#)

14 AUG 18
16:33:02 Trinity phone call

21 JAN 19
14:29:55 hi
14:52:41 Hi
16:56:06 Trinity Can you pls explain me
16:56:11 whats the problem with payvision
16:56:16 how come we have such huge gap?
16:56:52 Boyan Yes, I've mentioned to Gal that there will be a mismatch, but I didn't expect it to be that large.
16:57:29 The reason is that without them sending their reports, theres no way for me to know what are the
settled chargebacks
16:58:17 On top of that, our AM in PV told me about 2 CHB fines we received in March 2017, but no-one
informed me about it.
16:58:22 Trinity its looks like they have eat entire balance very worrys
16:58:30 Boyan I started working in the company in April 2017
16:58:55 So, the fine was for 480k euro
16:59:19 And PV deducted the amount directly from our RR balance later on.
16:59:53 In my reports, this amount has not been removed from the RR.
17:02:32 Because no-one informed me of it
17:04:40 Basically, biggest part of the mismatch is coming from this and settled Chargebacks, for which there
were no reports and without reports, there's no way for me to know which CHBs were applied to our balance.
17:20:23 Trinity So hows that possible that 4m wiped?
17:24:39 Boyan The difference is not 4m
17:25:50 I'm not in the office at the moment, but I believe the difference was around 1.2m and most of it is
because of the above reasons.
17:27:34 I know that it's not a small difference, not at all. But since OSG brand had some issues with PV,
they stopped sending reports and as mentioned before, I couldn't provide accurate report.
17:29:31 The total amount, most of it approximation, that I provided to Gal was 4m as total for the 4 brands.
PV double checked it and said that the total is ~3m
17:30:11 Though, today they confirmed that part of these funds will be withheld for 6 months after closing
our accounts with them.

Payvision also effected refunds for its fraudulent merchants.

Association to Combat Cybercrime against Retail Investors and Consumers
Non-governmental organization to combat cybercrime, ZVR 1493630560, Vienna, Austria
www.efri.io, email : office@efri.io

241. Booker and Lenhoff worked with several acquiring companies, but only Payvision was involved in effecting PONZI-refunds for the criminal organization. PONZI-refunds mean refunds to victims done by the scammers to provide evidence that they are “real.” The minor payments were done to victims in case the scammers assumed that the refunds would lead to even more and higher deposits from this victim.
242. Payvision received a list of the to-do Ponzi-refunds and debited the victims’ cards with the amount and deducted the total amount debited from the rolling reserve²¹.
243. In a Telegram chat between Gary Shalon (co-owner of the fraudulent brands) and the guy in charge of the handling of the PSPs’ within Gal Barak’s organization, the procedure gets evident:

informed me about it.
16:58:22 **Trinity** its looks like they have eat entire balance very worrys
16:58:30 **Boyan** I started working in the company in April 2017
16:58:55 So, the fine was for 480k euro
16:59:19 And PV deducted the amount directly from our RR balance later on.
16:59:53 In my reports, this amount has not been removed from the RR.
17:02:32 Because no-one informed me of it
17:04:40 Basically, biggest part of the mismatch is coming from this and settled Chargebacks, for which there were no reports and without reports, there's no way for me to know which CHBs were applied to our balance.
17:20:23 **Trinity** So hows that possible that 4m wiped?
17:24:39 **Boyan** The difference is not 4m
17:25:50 I'm not in the office at the moment, but I believe the difference was around 1.2m and most of it is because of the above reasons.
17:27:34 I know that it's not a small difference, not at all. But since OSG brand had some issues with PV, they stopped sending reports and as mentioned before, I couldn't provide accurate report.
17:29:31 The total amount, most of it approximation, that I provided to Gal was 4m as total for the 4 brands.
17:30:11 PV double checked it and said that the total is ~3m
17:30:11 Though, today they confirmed that part of these funds will be withheld for 6 months after closing our accounts with them.
17:30:32 In the meantime we will have some refunds and there will be new Chargebacks, for sure.
17:31:05 I don't like being the bearer of bad news, but I didn't have much control on either of these.
20:22:17 **Trinity** so i dont understand
20:22:20 how much they owe us ?
20:22:23 wihtout rr ?
20:22:59 **Boyan** I can check tomorrow, it's 21:20 here and my reports are in the office

244.

²¹ A **rolling reserve** is a strategy targeted to take care of the merchant and its financial institution as well as to keep away from the possible loss because of chargebacks. The RR functions as a guard for chargebacks. If the organization is facing the dangers: longer delivery, subscriptions, it means that the higher the rolling reserve which will be figured by the acquiring financial institution. When the RR is used to a certain transaction, the money will be settled in one of the payments within the time interval which stated in the trader’s contract

Termination of the payment processing contracts by Payvision

245. After it became published on the website www.fintelegram.com ("FinTelegram") in the summer of 2018 that Payvision was the primary payment service provider for the scam websites of Barak and Lenhoff, Booker contacted Lenhoff with concern²².
246. The files show that Payvision filed many SARs in the summer of 2018. This indicates that Payvision and Booker were well aware of the illegal nature of their customers' business.
247. Payvision terminated the merchant contracts for the scam websites as of 6, 8, and 23 December 2018, subject to a period of 4 weeks, according to the statements by Barak and Lenhoff, due to negative media coverage.
248. Booker justified the termination with an adverse customer due diligence conducted by Payvision in the 4th quarter of 2018 (an evident lie) in his statement to the Austrian law enforcement agency as of 23 May 2019.
249. Despite the termination of the contracts, telephone calls between Booker and Lenhoff and Booker and Barak took place until the end of January 2019.
250. Booker spoke to Lenhoff a few days before the arrest of Lenhoff (phone call on 22 January 2019) and tried to obtain information on the contractual relationships of previous years to set up his documents.
251. Booker met Lenhoff on 14 January 2019 in London, only ten days before his arrest.
252. When the notice period expired at the end of January 2019 – a few days before the arrest of Lenhoff/Barak – Payvision retained an amount of 4.3 million euros.

²² Interestingly Payvision missed all public warnings from the supervisory authorities about the scamming websites processed by them, but did not miss the mentioning of their name on Fintelegram beginning summer 2018.

253. The e-mail communication in the criminal files shows that Booker promised Barak an early payment of the withheld amount just a few days before he got arrested.

lets	219,100.33	27
	864,158.91	62

09:40:38
14:37:53
14:37:55
16:22:49 **Boyan**
16:45:21 **Gal**

phone call
come for a sec pls
urgently
Let me know once you have 2-3 mins
come

22 JAN 19

16:48:19 **Boyan**
16:48:38
16:48:43
16:48:43 **Gal**
16:48:51
16:48:54
16:49:03 **Boyan**
16:49:14
16:49:21
16:49:43 **Gal**
16:49:48
16:52:57 **Boyan**
16:53:19
16:53:50

When PV replied to one of my mails they mentioned that all balances are on hold for now.
Do you have some other info from them, or you knew about it?
also... Hi *
thats not an issue, i will get the funds its confirmed from owner
we just need to confirm the amounts now
so i can ask how much to sell
Ok
btw, since yesterday, Gabi's with me on Telegram
I've been discussing this with him as well
yes, all good ?
u getting help?
in my kilometric mails with PV, they confirmed that I cannot see all details that show the current outstanding balances.
I am asking them to confirm me with all brands current balances, but in any case any Refunds and / or Chargebacks will change these balances.
In case the owner of PV decides to release all funds, at some point they might ask us to pay them the negativity - just an "FYI"

254. 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.

255. Payvision has not provided an account for the withheld early termination fee. Based on information from the criminal file, PAYVISION withheld an amount of 4.3 million euros, reduced by chargeback fines and chargebacks to about 3 Mio euros:

22 JAN 19

08:23:39 Morning
08:25:00 As per my approximation, without the CHB fine and without reports confirming CHB amounts, the amount I told Gal was 4,072,987.00 EUR for the 4 brands - XFX, Safe, Golden, OSG.
08:25:34 PV confirmed that total amount for these brands is 3,008,608.43 EUR
08:25:56 After the CHBs and CHB fines
11:51:14 **Trinity** Morning
11:51:22 So they owe 3?
11:51:30 **Boyan** Morning, Gabi
11:51:32 Yes
11:52:23 But as I mentioned last night, they will hold part of the funds for 6 months after we end our business relationships.
11:52:52 By then the funds will be lowered. There will be Refunds and Chargebacks.
11:53:14 **Trinity** Noted

256. Booker did not mention these withheld client funds in his statement of 23 May 2019 to the Austrian law enforcement authorities or in his second statement of 15 July 2019.

PAYVISION also provided payment services for other transnational criminal organizations offering binary options trading/FOREX/Crypto

We found evidence that Payvision also provided payment services to the following scams:

NOVOX Capital Ltd

257. 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.

Novox Capital:

Novox Capital was a merchant of Payvision which was brought in by one of our reselling Partners Ms. Maya Har Noy from IM Payments. Via this indirect sales model, the reselling partner introduces Merchants that want to apply for a Merchant account. The reseller is the first point of contact and we do not deal directly with the Merchant, just the reseller.

The initial contact was with Ms. Maya Har Noy from the company IM Payments. Maya Har Noy was later on also working at the company Dcashier which led to the fact that the further day to day communication was done with her as a member of the company Dcashier as well as with other colleagues from Dcashier:

- Svetlina Vitanova
- Nir Ambramov

Later on we got in touch with Novox Capital directly. Some of the contacts at Novox Capital were:

- Shoham Cohen
- May de Vries
- Veronika Dankova
- Elly Hadjigiovanni

Novox Capital was terminated as a merchant at Payvision in November 2017 .

Were these persons also the contact for other companies, Payvision worked with? If so, please provide all information regarding these companies available.

1.

Association to Combat Cybercrime against Retail Investors and Consumers
Non-governmental organization to combat cybercrime, ZVR 1493630560, Vienna, Austria
www.efri.io, email : office@efri.io

258. NOVOX Capital Ltd was a licensed investment company (License Number: 224/14; License Date: 04/02/2014) in Cyprus controlled by three Israelis, Israel Bash, Shay Hillel, and Yehoram Hillel.
259. NOVOX Capital officially operated the five binary options schemes, OptionBit, OptionStars, OptionMerchants, STXoptions, and ZoomTraderGlobal (in 2015, ZoomTrader). Later in 2016, RoyalPIP was also included in this list of its approved domains. As with many licensed investment companies, there is evidence that NOVOX also operated unapproved domains like optionbit.biz; OptionMerchants.
260. Since late 2014 those schemes have received investor warnings from financial regulators in different North American and Europe jurisdictions. In December 2016, for example, the Canadian British Columbia Securities Commission (BCSC) warned against NOVOX Capital and its schemes OptionStars and OptionStarsGlobal. Regulators issued other warnings in the UK, France, Germany, Austria, and Belgium.



Financial Conduct Authority
Regulatory Agencies Introduction

FCA FINANCIAL CONDUCT AUTHORITY
REVOKED

Current Status: **Revoked**

License Type: **European Authorized Representative (EEA)**

Regulated By: **United Kingdom**

License No.: **622514**

Licensed Institution: **Novox Capital Ltd**

Effective Date: **2014-05-06**

Email Address of Licensed Institution: **info@novoxfx.eu**

License Type: **No Sharing**

Website of Licensed Institution: **--**

Expiry Date: **--**

Address of Licensed Institution: **3rd Floor, 60 Regaena Street 1010 Nic...**

Phone Number of Licensed Institution: **00357 22272520**

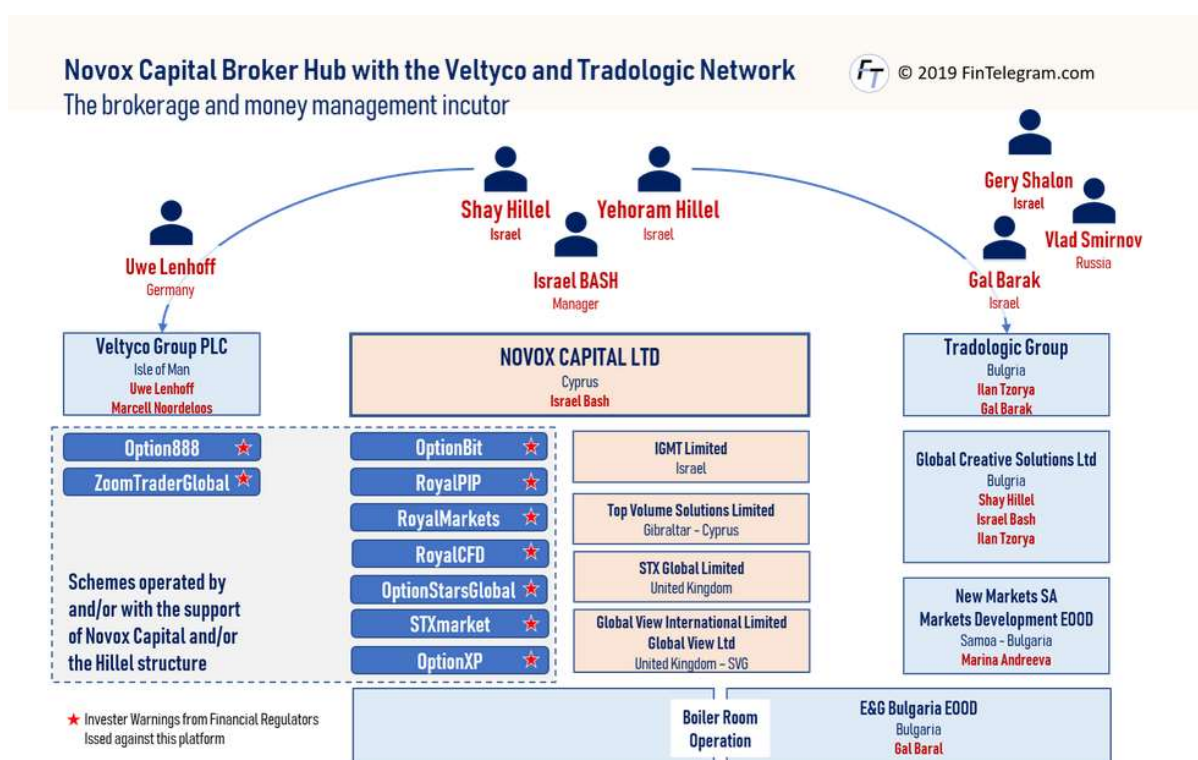
Licensed Institution Certified Documents:

[Annex1](#) [Annex2](#) [Annex3](#) [More](#)

CERTIFICATION CENTER OF WIKIFX

WIKIFX Verification

261. Numerous compliance violations resulted in regulatory penalties. This was also the case at the beginning of 2018 when the Cyprus Securities and Exchange Commission imposed a fine of 175,000 euros.
262. NOVOX Capital and its beneficial owners had a close business relationship with cybercriminal masterminds such as Uwe Lenhoff. In 2016, NOVOX Capital signed a marketing and revenue-sharing deal with Lenhoff's Veltco Group regarding the binary options platform ZoomtraderGlobal.



Binex/Dreamspay

263. Payvision also was a payment service provider 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 Gal Barak's people.

On Mon, Jan 21, 2019 at 1:58 PM Tsanko Arabadzhiev <tsanko.a@service-eng.com> wrote:

This is the list of all companies with contract with Payvision. So we are proceeding with the document you gave me regarding:

Binex
Matching Blue consulting
Optiumcommerce
Fevora

Would you confirm the above 4 or you want more (My idea is to have 1 company per brand, right)?

Regards

Domain	Entity	
binex.ru	Binex Ltd	Contract
cryptopoint	Gpay Ltd	Contract
xtraderfx		

9 St 3/20b

519

	Next Marketing Generation	Contract
goldenmrks	Cool Markets OU	Contract
	Matching Blue Consulting	Contract
safemarkets	Optiumcommerce OU	Contract
	Solvekey OU	applied only
optionstars	New Markets S.A	Contract
	Petit Margarita S.L.	applied only
	Fevora Limited	Contract
gxfx	Softgeeks OU	applied only

264. The scam platform BINEX was closed in the summer of 2018. Police authorities from around the world are investigating this illegal website's activities. One of BINEX's call centers in Kyiv was already searched by the Ukrainian cyber police in August 2018²³. The 60 boiler center employees persuaded more than 15,000 customers in Russia,

²³ <https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-organizatoriv-masshtabnoyi-shaxrajskoyi-onlajn-finansovoyi-birzhi-4169/>

Ukraine, and other countries (mainly Eastern Europe) to transfer tens of millions of dollars in just a few months to the scammers via Payvision²⁴.

24 Option

265. Payvision has also processed credit/debit card transactions from the scam website www.24option.com, operated by Roedeler Ltd, for many years up to March 2020²⁵.



For commodities and indices there is a fixed swap fee for keeping the position open overnight.

6. Deposit Fees

There are no deposit fees charged to the client.

7. Commission Fees

There are no commissions charged to the client.

8. Financing Fees

There are no financing fees charged to the client.

List of Payment Service Provider (PSPs)

Please find below the list of PSP companies in cooperation with their listed country headquarters and supervising authorities:

Name	Country of Establishment	Regulated	Regulatory Authority
Acapture (Payvision Group)	Netherlands, NL	Yes	Dutch Central Bank
eMerchantPay Limited	United Kingdom, GB	Yes	Financial Conduct Authority
Credorax	United States, US	Yes	Malta Financial Services Association (MFSA)
PAYSAFE FINANCIAL SERVICES LIMITED (Neteller)	United Kingdom, GB	Yes	Financial Conduct Authority
PPRO Group (Payment IQ)	United Kingdom, GB	Yes	Financial Conduct Authority
SAFECHARGE	Cyprus, CY	Yes	Central Bank of Cyprus
Wirecard Card Solutions Ltd	United Kingdom, GB	Yes	Financial Conduct Authority

²⁴ <https://www.trafikmarket.com/2019/the-raid-of-the-ukrainian-cyberpolice/>

²⁵ Based on a statement made by Andre Maarten Valkenburg.

266. In the summer of 2018, ARD Germany – one of the biggest broadcasting companies in Germany – published an extensive documentary about the fraud system 24option. The YOUTUBE video is still online https://www.youtube.com/watch?v=cAU4k_3zvaU.

267. 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. A raid and arrests were made in January 2021.

268. Warnings for this binary options platform were issued as follows:

- As of 3 April 2013, the Ontario Securities Commission (OSC), Canada, warned against Rodeler Ltd and the scam website 24Option.
- As of 6 August 2013 British Columbia Securities Commission issued a warning against the binary options trading scheme 24option. 26
- As of 1 August 2016, **France's regulator, the AMF**, has banned the **24Option binaries broker** from operating in France.
- As of 12 June 2017²⁷, The Financial Markets Authority (**FMA**) of New Zealand has published a warning for the binary options trading website 24option.

Other

269. Payvision also processes credit/debit card transactions for the scam website Algotechs/BEALGO from 2017 to 2019.

270. Like Barak and Lenhoff's scam brands, Algotechs had no license to offer financial instruments in Europe.

271. Payvision also miscoded those payment transactions.

²⁶ <https://www.bsc.bc.ca/enforcement/early-intervention/investment-caution-list/2013/24optioncom>

²⁷ <https://atozmarkets.com/news/details-behind-new-zealand-fma-24option-warning/>

Legal proceedings against Payvision in the United States

272. Payvision is accused in numerous pending lawsuits in the United States of contributing to cybercriminal activities (specifically money laundering), electronic communications fraud (access device fraud, wire fraud), bank fraud, and conducting illegal payment transactions in conjunction with the U.S. payment service provider T1 Payments LLC, Nevada (from now on T1):

273. High-risk processing for questionable MLM-Systems:

- Counterclaim and allegation of fraud by **New U Life Corporation**, a California corporation, Case No. 2:19-cv-01816-APG-DJA, regarding an early termination fee (ETF) million USD brought on 10/17/2019 resulting from a payment processing agreement for a multilevel marketing system for healthcare products (pending).
- Action Counterclaim, as well as Fraud Allegation of Beyond Wealth PTE LLC, Utah Case 2:20-cv-01405-JCM, brought on 24 August 2020 regarding a claim in the amount of 4 million USD resulting from a payment processing agreement for a multilevel marketing system (MLM) dated **29 May 2020 terminated on July 22, 2020.**
- Claim, counterclaim, and the allegation of fraud IBUUMERANG LLC, Texas Case 2:21-cv-01611-JCM-VCF, brought on 31 August 2021 concerning a claim in the number of millions of USD resulting from a Multilevel Marketing System (MLM) payment processing contract dated 06/26/2019 terminated on 08/11/2020.
- Action and allegation of fraud GAIA Ethnobotanical LLC, Case 2:22-cv-01046-CDS-NJK. Brought on 2 July 2022 concerning a claim of approximately 0.4 million USD resulting from a payment processing contract for trade in KRATOM (drug) concluded on 12 August 2020 and terminated on 28 May 2021.
- Action and allegation of fraud **First Capital Venture Co.** d/b/a Diamond CBD, Ltd., Case No. A-21- 834626-B (Clark County, Nevada) brought on 14 May 2021 regarding a claim of 0,6 million USD resulting from a payment processing agreement for the trade of cannabis.

274. Court documents show that it was only after the termination of the payment service contracts that it became apparent to T1's US customers that payment processing was done by the Dutch licensed payment service provider Payvision in massive violation of legal obligations and contractual existing credit card regulations

Cooperation agreement between Payvision and T1

275. Based on the court documents, the cooperation between Payvision Amsterdam and T1 Payments LLC, Las Vegas, started on 27 February 2015 and lasted until the summer of 2021. The business relationship developed as follows²⁸:

276. On or about 13 January 2015, T1's CEO, Donald KASDON, applied to become a Payment Facilitator (PayFac)²⁹ of Payvision in a web form application on the Payvision.com website. On the form, Donald Kasdon stated that T1's "worldwide headquarters" was located in the U.S. and provided a phone number with a Las Vegas area code.

277. According to testimony from Payvision employees, Payvision was aware that Donald Kasdon was a resident of Nevada and that T1 was a US corporation. On February 27, 2015, Payvision's CEO Rudolf Booker approved Kasdon's application.

On 11 March 2015, Donald Kasdon incorporated T1 Payments Ltd ("T1UK") in the UK. The managing director and shareholder of T1UK was Donald Kasdon's mother, Debra Karen King.

On 16 April 2015, Payvision entered into a merchant payment processing agreement with the newly formed T1UK.

T1 Payments LLC subsequently used the merchant account set up by Payvision for T1UK to process the transactions of T1's U.S. merchant customers, who also have to open up a sham UK company to get their transactions processed by Payvision. This was done in violation of the legal requirements applicable to Payvision as the payment license granted to Payvision is only valid for processing credit card transactions in the European area but in evident violation of the country coding requirements of the Credit Card schemes.

²⁸ Description is based on the legal files in different US court cases. <https://pcl.uscourts.gov/pcl/index.jsf>

²⁹ A Payment Facilitator is a merchant service provider that simplifies the merchant enrollment process. PayFac operate on a sub-merchant platform where merchants no longer require their own MID but are boarded directly under the PayFac's master MID account. A payments facilitator (or PayFac) allows anyone who wants to offer merchant services on a sub-merchant platform. Those sub-merchants then no longer have to get their own MID and can instead be boarded under the master MID of the PayFac who is sponsored by a bank.

This allows merchant services to be offered in a very elegant and very efficient manner. The PayFac does not have to underwrite all merchants upfront — they are instead, underwriting the merchants essentially as they continue to process transactions for them on an ongoing basis.

278. In his deposition, Kasdon testified that it was "a Payvision rule" that a European (shell) company had to be opened for all US merchants serviced by T1UK during the onboarding process. Payvision employee Joe Emig also confirmed this in his testimony. He stated that Payvision required each merchant to establish a European-based sham company. Accordingly, the US merchants onboarded by T1 routinely instructed T1 to set up UK companies as part of the onboarding process.
279. T1UK was formed by T1 to provide a "straw" company to facilitate payment processing for US high-risk merchants. Debra King was not involved in the formation or management of T1UK (or any of the TI parties) and said in her deposition that she signed documents that her son Donald Kasdon handed her and instructed her to sign. Donald Kasdon exercised complete control over T1UK. T1UK had no employees. It had no actual presence in the United Kingdom. The address for the company was a virtual office, along with hundreds of other companies. T1UK also needed a bank account. The merchants' money was sent directly to the T1 Payments LLC account). T1UK had no staff and no office facilities.
280. Although T1UK was a mere letterbox company with no actual presence in the UK, Payvision entered into payment processing agreements with T1UK. Payvision required Nevada-based T1 Payments LLC to be a guarantor for T1UK's liabilities.
281. On **8 July 2015**, after two months of processing, Payvision terminated its agreement with T1UK due to "multiple incidents involving chargebacks and fraud." After the termination of T1UK, Booker (the then-CEO of Payvision) communicated directly with Kasdon about resuming the processing of merchant transactions through PAYVISION. Booker advised KASDON to incorporate the new company in Guernsey, the Isle of Man, known for its lax financial regulations.
282. On or about 7 December 2016, Kasdon incorporated TGlobal Services Ltd. as an Isle of Man company. Like T1UK, T Global Services Ltd. was solely a shell company that T1 used to facilitate the payment processing of high-risk U.S. merchants through a European acquirer (Payvision). Like T1UK, TGlobal Services Ltd. (TGlobal) was nominally owned by Debra King, also named as a director, but Kasdon controlled the entity.
283. Donald Kasdon is the beneficial owner of T1UK and TGlobal Services Ltd. and did not act as a shareholder or director himself, as his name appears on the MATCH list or Terminated Merchant File (TMF)³⁰ several times.

³⁰ The MATCH list is essentially a blocklist for credit card processing. Businesses on the MATCH list have had merchant accounts terminated previously or deemed a significant risk for payment processors. The MATCH list is the same as the Terminated Merchant File (TMF), an older, more generic term. The MATCH list is used by acquiring banks to screen potential applicants (particularly to see if that applicant has been terminated in the past). They do this to assess and control the risk associated with credit card processing. Essentially, the MATCH list is used by processors to avoid merchants who have been flagged as especially high risk. In addition to Mastercard itself, acquiring banks can add/remove merchants to/from the MATCH database when they have the justification to do so. In fact, only the acquiring bank that put you on the list has the power to remove you from the list. Mastercard can also remove merchants from the list, but it rarely deals with merchants directly. This also makes it difficult for merchants to dispute their addition to the list. Having too many chargebacks, participating in fraudulent activity, or money laundering are all activities that can get you listed. According to Mastercard (SRP, Section 11.2.2), an acquiring bank is required

284. Rudolf Booker authorized KASDON to resume processing with Payvision through the TGlobal Services merchant account with a card processing agreement dated 13 December 2016 (signed by Debra King).
285. In November 2017, Payvision signed a payment service provider contract with T Global Services UK. The merchants' money was remitted from Payvision's merchant account to the bank account of TGlobal Limited LLC in Nevada resp. To any other US bank account named by KASDON.
286. Although there were additional fraud allegations against T1 as early as 2019 (see above) related to U.S. high-risk customers that Payvision processed, Payvision continued to work with Donald Kasdon until at least **the end of May 2021**.
287. By then, for Kasdon, the cooperation with Payvision was critical as he had been in dispute with his previous acquirer VANTIV since the fall of 2016, which then culminated in a court battle in the spring of 2017 as well and resulted in the loss of T1 Payment LLC's authorization as a Payment Facilitator (PayFac/payment services intermediary) with the credit card companies VISA and Mastercard.

The Ibuumerang Case 2:21-cv-01611-JCM-VCF complaint states the following regarding this fallout:

T1 was a Payment Facilitator (registered with VISA and Mastercard) under a March 31, 2016, contract with Vantiv, an industry-leading payment processor processing more than USD 20 billion transactions annually. However, on or about March 14, 2017, Vantiv sued T1 in the United States District Court for the Southern District of Ohio for breach of contract and fraud. Vantiv alleges that in addition to breaching its contract with Vantiv, T1 invented fictitious companies to defraud Vantiv and stole money from merchants by using a ruse to divert funds to T1's bank account that should have gone to the merchants. Specifically, Vantiv alleges that T1 set up two fake merchants by using its bank account as the fake merchant's purported bank account and then submitted hundreds of fraudulent transactions using stolen credit card numbers to fund its account from the accounts of the cardholders whose numbers were stolen. When Vantiv learned of the fraud, it immediately terminated the relationship on or

to put a merchant on the MATCH list if the merchant's account was terminated for any reason on the list, and they must do so within five days of termination. Since the obligation is between the acquiring bank and Mastercard, there's not much you can do to stop the bank. While acquirers must put you on the MATCH list if they terminate you for MATCH list reasons, they're **not** required to refuse to take you as a merchant. The MATCH list indicates the level of risk of doing business with you, and some acquirers and processors have a higher tolerance for risk than others. These high-risk processors have less favorable terms, but they can allow you to continue accepting credit cards. We'll take a closer look at this option in the next section. So long as you remain on the MATCH list, you'll be considered a high-risk merchant even if you wouldn't otherwise qualify as one. If you've been added by mistake or due to PCI non-compliance, remember that you may be able to get off the list.

about February 2, 2017, ending T1's role and causing it to deregister from the card brands as a payment services intermediary.

288. Neither the deregistering of T1 as a payment facilitator nor the fact that Donald Kasdon was the beneficial owner of the UK companies and had multiple entries on the MATCH lists did stop Booker. As with its predecessor T1UK, Payvision insisted on a guarantee from Donald Kasdon and a corporate guarantee with T1 Payments LLC for all liabilities of the British shell company TGlobal Services Ltd. As with the execution of transactions for TIUK, T1 used TGlobal Services Ltd's merchant account with PAYVISION to process the payment transactions of US high-risk merchants.

289. Payvision knew throughout its relationship with the Kasdon companies that it was the Nevada-based T1 that was processing T1's U.S. merchant customer transactions through the TGlobal Services Ltd. merchant account (only T1 had contracted with US merchants under the CPPA) and that it was T1, not TGlobal, that was onboarding and managing the US high-risk merchants onboarding. T1 required all accepted U.S. high-risk merchants to open offices in the United Kingdom as part of their standard onboarding practices.

290. TGlobal Services Limited LLC is a Nevada corporation registered in the name of Kasdon's parent but controlled by Kasdon, according to KASDON.

Bank fraud committed by Payvision

291. On page 19/44 of the complaint Case 2:21-cv-01611-JCM-VCF Ibuumerang LLC, the allegations concerning Payvision are detailed in points 84ff.

87 Third, the Card Brand Rules require the acquirer to have exclusive control over the merchant's funds unless it is a duly registered payment facilitator. See Mastercard Rule 7.2.1 (p. 127), Mastercard Rule 7.3 (p. 130), Mastercard Rule 7.6.2 (p. 132), and Visa Core Rule 1.5.8.2 (p. 105). However, the CPPA provides for T1 to collect and deduct service fees, retain and maintain reserves, and make payments to Ibuumerang directly from the proceeds of Ibuumerang's processing activities. See, e.g., CPPA 5, 7, 6.1, .2, 6.3, 6.4, 6.5, 6.8, 7, 8.1, 8.2, 8.3, 8.4, .5. These transactions violated the Brand Rules.

89 Fifth, the Card Brand Rules prohibit an acquirer from accepting and transmitting to Interchange transactions from merchants, payment intermediaries, or sponsored merchants (i.e., merchants that contract with a payment intermediary outside the acquirer's jurisdiction). The card payment rules also prohibit a payment intermediary from contracting with a sponsored merchant outside the country where the Payment Facilitator and acquiring company are located. This means that T1, as a company based in Las Vegas, Nevada, is only eligible for sponsorship as a registered service provider by an acquirer based in North America. Thus, even if T1 were properly registered adequately a payment facilitator or other type of service provider-which it is not-the Card Brand Rules would prohibit any acquirer in the United Kingdom or Europe from sponsoring T1 as a service provider and accepting transactions from merchants located in the United States and forwarding them to Interchange without violating the Card Brand Rules, which prohibit cross-border acquiring. See Mastercard Rule 5.4, Visa Core Rules 1.5.1.1. and 1.5.1. 3.

90. Sixth, T1 also used tactics designed to circumvent the credit card rules against cross-border processing by establishing foreign front companies for Ibuumerang and other U.S. merchants as a normal part of the merchant affiliation process. The card brand rules define a merchant's location. For example, Visa specifies that a merchant's location must be the country where its original place of business is located, which Visa defines as a fixed location where a merchant's officers direct, control, and coordinate its activities-generally, a merchant's headquarters. See also Mastercard Rule 5.4.

91. T1 Payment arranged for the registration of a U.K. shell company in the name of Ibuumerang and other U.S. merchants to circumvent credit card regulations that require merchants to be located in the same geographic areas as T1 Payment's acquirers.

92. by facilitating UK shell companies for Ibuumerang and other merchants outside the UK and EU, T1 Payments colluded with one or more undisclosed acquirers to create the false appearance that these merchants were based in the UK or EU and therefore eligible for domestic payment processing. Notwithstanding this ploy, however, the Card Brand Rules prohibit undisclosed EU acquirers and payment processors from T1 Payments from opening accounts for Ibuumerang and these merchants.

93. By setting up foreign shell companies to process payments for Ibuumerang and other U.S. merchants abroad, T1 knowingly orchestrated the active evasion of the generally stricter regulatory framework of the U.S. financial system. At the same time, T1 Payments repeatedly assured Ibuumerang that the formation of the UK company was entirely legal and complied with all applicable regulations.

94. *the use of UK shell companies to open accounts for non-UK and EU merchants is the standard operating procedure at T1, so much so that the need to obtain an "EU Corp" in addition to the merchant's actual corporate form is codified in T1 Payments' account opening instructions, MSA and related documentation provided to partners and merchants in the ordinary course of business.*

95. *T1 Payment's plan to circumvent these card brand rules is also evidenced by its instructions to Ibuumerang and other merchants to open a "hot desk" in the United Kingdom, to change their LinkedIn profiles to show an affiliation with the U.K. company, and to change their websites to include the U.K. company and U.K. address instead of the company name and address of the actual U.S. company requesting merchant services, as well as its conduct in redirecting the EU members it created to customer service centers in the United States.*

96. *Defendant PAYVISION acted as the acquiring bank concerning Ibuumerang's settlement activities. Ibuumerang is further informed that even though T1 Payments is not sponsored by PAYVISION and is not registered with the Card Brands as a payment intermediary, PAYVISION permitted T1 Payments to simply establish a sub-account for Ibuumerang under its primary merchant account with PAYVISION to process Ibuumerang's transactions without any contract between Ibuumerang and PAYVISION.*

97. *This conduct constitutes illegal "aggregation," a form of credit card money laundering that violates federal regulations, including the unfairness provision in Section 5(a) of the Federal Trade Commission Act. See, e.g., Federal Trade Commission v. Apex Capital Group LLC, CD. Cal. Case No. CV 18-9573-JFW (JPRx) (Nov. 13, 2018) (processing one company's transactions through another company's merchant account is referred to as "credit card laundering" and is an unlawful practice used to circumvent credit card monitoring programs and avoid detection by consumers and law enforcement.*

98. *Money laundering using credit cards (credit card laundering) may involve opening a merchant account through a "shell company," or it may affect "collecting" transactions from other companies and processing them through a single "funnel account" in the ISO's name, as occurred here. In either case, this is credit card fraud and, therefore, an unlawful business practice. See First Amended Complaint, filed December 21, 2015, in FTC v. E.M. Systems, LLC (M.D. Florida), Case No. 8:15-cv-1417-T-23 EAJ at 58-63 (describing transaction laundering in detail). The U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN") considers such activity to be a variant of money laundering.*

T1 Payments deregistration as a PayFac results in Payvision as the only accountable PSP

292. Acquirers like Payvision may contract with third-party organizations to provide processing-related services to merchants under the acquirer's sponsorship with the Card Brands (such third-party organizations are referred to in the Visa rules as "Third Party Agents," and in the Mastercard rules and hereafter as "Service Providers").
293. A Service Provider is categorized by the Card Brands based on the nature of the Program Services to be performed. For example, an acquirer may sponsor a Service Provider: as an Independent Sales Organization ("ISO") to solicit merchants for payment processing services on its behalf (including application processing, customer service and statement preparation not affording access to account data or transaction data); or, as a Third Party Processor ("TPP") to provide authorization services, clearing file preparing and submission, settlement processing (excluding possession, ownership, or control of settlement funds, which is not permitted), merchant statement preparation, fraud control and risk monitoring, and/or chargeback processing; or, as a Payment Facilitator to contract directly with merchants as an agent of the acquirer, and submit to the acquirer records of valid transactions submitted to the Payment Facilitator by its sub-merchants, timely pay sub-merchants for transactions submitted to the Payment Facilitator by the sub-merchant, and provide recurring education and training to sub-merchants to ensure their compliance with Card Brand Rules.
294. Before an entity commences to perform a Program Service that supports or benefits a member bank's acquiring program, the acquirer must:
- verify that the entity is operating a bona fide business,
 - has sufficient safeguards in place to protect account and transaction data from unauthorized disclosure or use,
 - and complies with applicable laws; and cause such an entity to be registered by the Card Brands as a Service Provider.
 - A Service Provider may perform only the type of Program Service it is registered to perform and must be registered with the Card Brands to perform such a particular category of Program Service before an acquirer or merchant may use its services. See e.g. Mastercard Rule 7.2 (The Program and Performance of Program Service).
295. **According to the Card Brand rules, the acquirer must always be entirely responsible for and must manage, direct, and control all aspects of its Program and Program Services performed by any service providers and establish and enforce all program management and operating policies by Card Brand Rules. An acquirer must not transfer or assign any part of such responsibilities or limit its responsibility to any of**

its service providers. An acquirer must conduct meaningful monitoring of its Service Providers to ensure ongoing compliance by its Service Providers with Card Brand Rules. See, e.g., Mastercard Rule 7.2.1 (Customer Responsibility and Control).

296. A Service Provider must not have access to any account for funds due to a merchant or withheld from a merchant for chargebacks, except Payment Facilitators, as outlined in outlined obligations as Sponsor of sub-merchants.

297. An acquirer must not assign or transfer to a Service Provider an obligation to pay or reimburse a merchant if the obligation arises from the merchant's processing activity. See e.g., Mastercard Rule 7.3 (Access to Merchant Account). Discount rates (or similar charges called by other terms) due to an acquirer from a Merchant must be collected directly by the acquirer, not the Service Provider. See, e.g., Mastercard Rule 7.6.2 (Collection of Funds from a Merchant). 33

298. In summary, Card Brand Rules broadly prohibit any Service Provider from (i) contracting directly with a merchant without the acquirer as a party to the agreement, (ii) handling or having access to the proceeds of the merchant's processing activity, including deducting fees, (iii) holding merchant reserves, and (iv) settling the merchant's account, (i.e., paying the merchant for its transactions). **The only exception is in the case of a registered Payment Facilitator.**

Miscoding (U.S. bank fraud) committed by Payvision.

299. Like with Barak and Lenhoff's illegal business activities, Payvision miscoded the payment transactions are done for the US merchants, thereby deceiving US banks about the true nature of the financial transactions they were processing.

300. According to the remote deposition done with Debra King as of September 2021 for the legal claim of New U Life Corporation used the MCC 5499 (Misc. Food Stores – Convenience Stores and Specialty Markets and other similar services) and 5962 (Direct Marketing, travel, including discount travel club). New U Life Corporation is an aggressive MLM system marketing a questionable Somoderm HGH Gel.³¹³²

301. In the remote disposition of Debra King, the official beneficial owner and director of the contracting partner of Payvision B.V. (T1 Payments Ltd, London, Company number **09484519**, TGlobal Services Ltd, London, Company number **11302654**, and T1 Payments LLC, Nevada) declared - similar to RUMEN GOGOV – that she never had any contact with Payvision B.V. and that she is not aware of any due diligence done (Appendix). As

³¹ <https://besthghdoctor.com/blog/is-hgh-gel-a-scam/>

³² <https://behindmlm.com/mlm-reviews/newulife-review-homeopathic-human-growth-hormone-gel/>



with the merchants onboarded by Payvision for the TCOs, merchants used for the high-risk US sub-merchants only were shell companies with no financial records.



302. for processing the high-risk products of New U Life Corporation

1 says, "Products sold" and it says, "Merchant of Record"?

2 A Uh-huh.

3 Q And then under that it says, "Descriptor" and
4 then the field has been redacted? It's field is
5 completely blacked out?

6 A Yes.

7 Q Do you know what this field said?

8 A I have no clue.

9 Q Do you have any idea why it would have been
0 redacted?

1 A No idea.

2 Q Do you see at the top, it says, "MCC code 5499"
3 and "5962"?

4 A Yes, I see.

5 Q Do you know the categories those MCC codes
6 represent?

7 A No idea.

8 Q Do you know who selected those codes?

9 A No idea.

0 Q And looking towards the bottom of the chart, it
1 says, "Settlement bank account holder Tglobal Services,
2 LLC"; do you see that?

3 A Yeah.

4 Q Does this reflect that the funds will be
5 deposited to a bank account held in the name of Tglobal

Payvision processed payment transactions for CBD and KRATOM for at least four years up to May 2021

303. The following legal claims brought against T1 payments and Payvision in the US evidence that Payvision processed payment transactions for CBD and KRATOM products for US merchants from at least 2017 up to and including May 2021.

- **First Capital Venture Co.** d/b/a Diamond CBD, Ltd., Case No. A-21- 834626-B (Clark County, Nevada) brought on 14 May 2021 a claim for 0.6 million USD resulting from a payment processing agreement entered into on May 2017 for CBD products and lasting until May 2021.
- **Sarah Grauert, and by HANNAVAS Enterprises LLC, Delaware**, Case No. 2:20-cv-00411-KJD-VCF, brought a claim on 27 February 2020 regarding the retention (early termination fee) of 1 million USD resulting from a Payment Processing Agreement for Online Cannabis products stores (<http://www.bionicbliss.com>) (settled 11 September 2020).
- **GAIA Ethnobotanical LLC, Nevada** Case 2:22-cv-01046-CDS-NJK brought on 2 July 2022 a legal claim for approximately 0.4 million USD resulting from a Payment Processing agreement for KRATOM (drug) products entered on 12 August 2020 and **terminated on 28 May 2021**.
- Complaint, Counterclaim, and Allegation of Fraud Onyx & Rose LLC, Case No. 2:20-cv-00008-KJD-NIK filed 07/3/2019 regarding an early termination fee of 204,859.51 USD under a cannabis products payment processing agreement entered into 09/12/2018 (settled 07/09/2020).
- Action, Counterclaim, and allegation of Fraud **PureKana LLC**, Case No. 2:19-cv-01399-KJD-NJK concerning an early termination fee of 1.080 million USD filed on 14 August 2019 resulting from a payment settlement agreement for CBD products entered into on 29 September 29, 2017 (settled on 10 March 2020).
- Lawsuit filed by Michigan Herbal Remedies LLC, Case No. A-20-821474-C, filed 18 September 2020 (no more information available).
- Action and Counterclaim by **Sarah Grauert and by HANNAVAS Enterprises LLC, Delaware**, Case No. 2:20-cv-00411-KJD-VCF brought on 02/27/2020 regarding the retention (early termination fee) of 1 million USD resulting from a Payment Processing Agreement for Online Cannabis Products Stores (<http://www.bionicbliss.com>) (settled 11 September 2020).

304. Like with the other US high-risk merchants, T1 Payments – as an alleged payment facilitator - set up phony companies in Europe for the US merchants' resp. claimants

Association to Combat Cybercrime against Retail Investors and Consumers
Non-governmental organization to combat cybercrime, ZVR 1493630560, Vienna, Austria
www.efri.io, email : office@efri.io



(First Capital Venture Co, Hannavas Enterprise LLC, Delaware, and GAIA Ethnobotanical LLC, Nevada) and processed the card transactions for the sale of on-demand CBD and KRATOM products of US merchants via the Dutch Payvision.

305. According to witness statements of Donald Kasdon as well as counterclaims filed by T1 Payments LLC, Payvision was the one to establish the plan for the transaction laundering scheme.

306. In general, with Marijuana listed as a Schedule I drug by the Food & Drug Administration (FDA) — and therefore being illegal under federal law **all US banks and all credit card associations (Visa, Mastercard, Discover, American Express, etc.) have firm policies against their cards being used for marijuana sales, respectively for all CBD products, even in jurisdictions where it's legal.** The same applies to KRATOM products.

307. So due to current banking regulations and laws, credit card processors (VISA/Mastercard) based cannot provide credit card processing services for CBD, KRATOM, and other Hemp related businesses.

308. Because Credit Card companies do not support marijuana transactions, they do not have marijuana merchant codes. As a result, to process a marijuana transaction through a Credit Card Company, a false merchant code, i.e., a merchant code associated with a different product or product category — would have to be used, so merchant codes for other products — typically referred to as “miscoding” — to get around these rules are used.

309. The US authorities are strict on these rules.

310. In March 2021, Ray AKHAVAN and Ruben WEIGAND were found guilty of bank fraud following a four-week jury trial before U.S. District Court Judge Jed. S. Rakoff.

311. HAMID AKHAVAN, aka “Ray Akhavan,” and Ruben Weigand was charged in May 2020 by the Department of Justice for engaging in a transaction money laundering scheme to deceive United States (issuing) banks and other financial institutions into processing over one hundred million dollars in credit and debit card payments for the purchase and delivery of marijuana products. The court outlined that because many United States banks are unwilling to process payments involving the purchase of marijuana, Ray Akhavan and Ruben Weigand used fraudulent methods to avoid these restrictions and to process hundreds of millions of transactions for CBD products via European payment processing companies.

312. In detail, Ray Akhavan and Ruben Weigand relied on third-party payment processors (the “Payment Processors”) who created — in cooperation — with Ray Akhavan phony offshore corporations and websites (i.e., the phony merchants) and opened offshore merchant accounts. These fake merchants and offshore merchant bank accounts (in combination with misleading MCC) were used to disguise payments made to the US merchants for the purchase of Marijuana products and to deceive United States banks about the true nature of the financial transactions they were processing. Ray Akhavan acted as a merchant-middleman for the retailers that delivered on-demand CBD products and accepted card payments.

Association to Combat Cybercrime against Retail Investors and Consumers
Non-governmental organization to combat cybercrime, ZVR 1493630560, Vienna, Austria
www.efri.io, email : office@efri.io

313. The role of Ray Akhavan as the middleman and merchant between the actual retailers for the drugs (sub-merchant) was taken by T1 payments LLC in the transaction laundering scheme (resp. bank fraud scheme) set up by Payvision B.V and companies like GAIA Ethnobotanicals, Diamond CBD Ltd and Sarah Grauert were the sub-merchants.
314. Ray Akhavan was sentenced to 30 months in prison. Co-defendant RUBEN WEIGAND was sentenced to 15 months in jail for participating in a scheme to deceive U.S. issuing banks and credit unions into effectuating more than \$150 million of credit and debit card purchases of marijuana by disguising those transactions as purchases of other kinds of goods, such as face creams and dog products via European payment processing companies.
315. By the illegal use of phony European companies, an overseas aggregator (T1), and the resulting miscoding of the country, as well as the merchant category code, US merchants can offer and sell CBD and KRATOM online with payment via credit cards processed via Payvision B.V.
316. According to info available on the web,³³ T1 payments were providing services to about 90% of the US Kratom businesses. Hundreds of KRATOM merchants got onboarded by T1payments and Payvision.
317. Payvision stopped processing card transactions for KRATOM merchants in or around May 2021.
- 318.



319. The legal claim brought by **GAIA Ethnobotanical LLC, Nevada**, evidenced the conspiracy between Payvision B.V. and T1 payments LLC by providing different documents evidencing that PAYVISION was the one to orchestrate the bank fraud to the court.
320. In the court case, A FIRST CAPITAL VENTURE CO. versus T1 Payments LLC/Payvision B.V and others, T1 Payments filed a counter statement on 16 March 2022 principally confirming all allegations of First Capital Venture regarding the fraudulent structure for the payment processing for the CBD shop but contested that T1 Payments was the one

³³ (Visa, Mastercard, Discover, American Express, etc.) have firm policies against their cards being used for marijuana sales

to develop the fraudulent design (Case 2:22-cv-01046-CDS-NJK Document 40-17 Filed 09/21/22).

321.:

25 11. T1 Payments LLC denies liability in this case. However, if T1 Payments LLC is
26 liable, T1 Payments LLC alleges through this FATC that Payvision is the true responsible party,
27 and thus responsible for all liability T1 Payments LLC might incur and for additional damages that
28 Payvision caused as alleged herein. Among other things and as alleged more fully below,

4

Case 2:22-cv-01046-CDS-NJK Document 40-17 Filed 09/21/22 Page 5 of 69

1 Payvision: established and implemented the payment processing structure and provided
2 instructions to T1 Payments LLC throughout the course of the relationship of the parties to
3 effectuate and operate the processing that First Capital now claims is unlawful; knew that First
4 Capital was a merchant (indeed, Payvision acquired and transmitted funds from the sales First
5 Capital made); represented to T1 Payments LLC that the payment processing structure and
6 operations required by Payvision would be lawful and comply with card brand rules; represented
7 that Payvision would obtain and effectuate the payment facilitator or other needed registrations
8 with the card brands so that the processing relationship could, according to plaintiff, operate
9 lawfully under applicable card brand rules; always treated the relationship as a compliant payment

322.T1 Payments confirmed that Payvision knew everything about the sub-merchants onboarded and even referred US merchants to them

15. During the entirety of the Payvision relationship, T1 Payments LLC serviced the merchants, and managed merchant onboarding and all aspects of the merchant processing operations for merchants, facts which Payvision knew when it entered the Payment Facilitator Agreement and thereafter. The source of Payvision's knowledge included regular communications to and from T1 Payments LLC during the merchant onboarding process and all other aspects of the merchant processing. Indeed, virtually all of the communications from and to Payvision concerning the subject payment processing were from or to Nevada-based T1 Payments LLC. These communications were continuous, systematic, persistent, and numerous, and along with other facts show that Payvision purposefully availed itself of the benefits and protections of doing business in Nevada. For instance, Payvision:

323.Also, the remote disposition of Joe EMIG, a former employee of Payvision New York, on April 2022 in Case No.: 2:19-cv-01816- -DJA confirms that it was Payvision that orchestrated the business relationship between T1 payments LLC and PAYVISION B.V.

324.The new management Valkenburg was served with the claim Beyond Wealth PTE LLC, Utah Case 2:20-cv-01405-JCM, detailing the complaints in all details on September 2020. By 9 October 2020, the Dutch DNB delivered a devastating report about wilful blindness. Nevertheless, Payvision continued with processing GAIA!

Involvement in sex trafficking

325. Payvision provided payment services to PORNHUB up to October 2020. ING Groep NV, the largest Dutch financial services company, published beginning of November 2020 that it had sold part of its PAYVISION payments business, including cutting ties with online pornography and gambling customers.
326. About 100 Victims of Pornhub's illegal activities are going legally against the beneficial owners of Pornhub (MindGeek and others) and VISA for together monetizing videos of child rapes (Case 2:21-cv-04920-CJC-ADS). Specifically, the lawsuit alleges that VISA, via its bank agents (acquirers like Payvision and Wirecard), recognized MindGeek as an authorized merchant and processed payments to its websites via numerous sham shell companies. The victims claim that VISA provided the payment system to monetize Pornhub's illegal business activities. As VISA via their acquirers (supervised payment institutions like Wirecard or PAYVISION) processed payments for these sites, it profited from MindGeek's alleged sex trafficking enterprise.
327. Kasdon and Amber Fairchild (KASDON's girlfriend and business partner) testified in the US court that Payvision regularly referred high-risk customers to them. Payvision representatives officially turned away high-risk customers from industries prohibited under ING's policies to refer them to T1 Payments. These merchants were prohibited from opening their merchant accounts with Payvision, but via T1 processed transactions under the merchant account of TGlobal Services Ltd.

Payvision's involvement in the Allied Wallet case

328. In its action of 23 May 2019 (2:19-cv-04355-SVW-E), the US FTC (Federal Trade Commission) accused 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 2012³⁴.
329. Allied UK and Allied Inc were registered as Payment Facilitators with Mastercard and VISA.
330. 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.
331. The allegation was that Allied Wallet intentionally accepted merchant applications with false information regarding the business 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.
332. Another allegation by the FTC was that the creation and use of European sham companies to process payments for U.S. merchants in Europe with European payment services 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.
333. 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 basic form of the trader was even specified in the internal checklist of the Allied Wallet after each 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.
334. 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.

³⁴ 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.

Acquisition of PAYVISION by ING in March 2018

335. 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, Amsterdam³⁵. The agreed purchase price amounted to 380 million euros. Thus, the valuation was 12* the annual gross profit earned on sales as of 31 December 2017 (29 million euros). According to various media reports, the founders of Payvision had long been looking for a buyer.
336. 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 colleagues.
337. 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 autumn 2017 must have revealed PAYVISION's high-risk business activities.
338. ING Groep BV was in the middle of a criminal investigation for money laundering during the acquisition of PAYVISION (2017), so ING must have been aware of the explosive use of the traditional financial system by criminal organizations.
339. Nevertheless, ING Groep NV accepted a valuation of 360 million euros for PAYVISION.
340. 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.
341. As of the end of April 2020, Rudolf BOOKER, Gijs op de WEEGH, and Cheng LIEM LI left their board positions.
342. 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 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.
343. As of 8 October 2020, an investigation report submitted by the Dutch Supervisory Authority (DNB) to the management of Payvision B.V. – a licensed Dutch payment

³⁵ <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>

institution in Amsterdam, stated that an on-site audit carried out by DNB had established

- that the company has been in serious breach of the Sanctions Act, the Financial Supervision Act, and the Money Laundering and Terrorist Financing Act (Wwft) since at least 2015,
- that fraud signals were deliberately ignored and some of its customers were deliberately not screened (willful blindness)
- and that furthermore, customer checks and compliance with anti-money laundering regulations were systematically neglected.

344. The DNB report explicitly states that the company's violations are still ongoing at the time of writing, despite a clean-up operation by the new management (meaning Valkenburg and Terpstra).

345. As of November 2021, ING announced the closing down of Payvision as of June 30, 2022.

The role of ING in the in the scamming activities of Payvision

346. ING made several bank accounts available to Payvision, which Stichting Trusted Third Party Payvision³⁶ used as payment accounts³⁷ for the processing of Gal BARAK's fraudulent websites: NL55INGB0654654653194; and NL97INGB0660731428. respectively.

347. ING has been providing payment accounts to Payvision for some time, as can be seen from a judgment of March 15, 2016 by the Dutch court AZ: C/13/604101/KG ZA 16-261 PS/MB. This concerns a dispute between the defendant 2) and its customer LOPOCA Gaming Limited, Malta. The dispute concerned the withholding of customer funds by Payvision, which was contested by LOPOCA. In the course of this legal dispute, Payvision and ING Bank N.V. (where Payvision's payment account is held) were served with an attachment order on March 8, 2016. LOPOCA is an online gaming company that has been the subject of criminal proceedings in several jurisdictions for several years. ING was therefore aware of the quality of Payvision's customers when it acquired the company in January 2018.

348. This also corresponds to the statement in ING Bank's annual report for the 2020 financial year, where it is emphasized on page 175 that ING was aware when purchasing the company that the quality of Payvision's customers would not meet the requirements of ING of defendant 3).

³⁶ These are trust vehicles wholly owned by the PAYVISION Group, which acted as the account holder.

³⁷ According to Section 1 (17) ZAG, a payment account is an account in the name of one or more payment service users that is used for the execution of payment transactions.

349. The payment account provided by ING was used to record the deposits and book the fees and commissions; Payvision only paid out the remaining amount to the criminal organization.
350. Part of the takeover transaction carried out in March 2018 was also the continued provision of bank accounts and support for the payment process³⁸. With the takeover, the third defendant also became a sales partner of Payvision on similar terms to other partners.
351. In accordance with the agreement reached when Payvision was acquired, ING has also provided a bank account at its Romanian branch (IBAN RO15INGB0000999908563122) for **Celtic Pay Ltd** - a shell company used by Uwe Lenhoff to receive card payments from the fraud platforms option888.com, tradeinvest90.com, tradovest.com, xmarkets.com - as of March 2018.
352. Celtic Pay Ltd. was founded on 02.02.2018 in London. The parent company was Celestial Trading Ltd in the Seychelles. From April/May 2018, Celestial Trading Ltd was also the domain owner for the fraud platforms option888.com, tradeinvest90.com, tradovest.com, xmarkets.com.
353. The first warnings from the supervisory authorities were issued immediately after the start of operations:

13.06.2018, geändert am 13.11.2020 | Thema [Unerlaubte Geschäfte](#)

Celestial Trading Ltd. („Option888“): BaFin ordnet Einstellung und Abwicklung des Finanzkommissionsgeschäfts an

Die BaFin hat der Celestial Trading Ltd. (Mahé, Seychellen) mit Bescheid vom 6. Juni 2018 aufgegeben, das unerlaubt betriebene Finanzkommissionsgeschäft einzustellen und abzuwickeln.

Die Gesellschaft betreibt insbesondere Forexhandel im eigenen Namen und für fremde Rechnung; zudem handelt es mit Aktien und sonstigen Finanzinstrumenten im Sinne des § 1 Absatz 11 Kreditwesengesetz ([KWG](#)).

Die Gesellschaft nutzt wie zuvor die Capital Force Ltd. den Namen „Option888“. Die BaFin hat der Capital Force Ltd. bereits mit [Bescheid vom 21. März 2018](#) die Geschäftstätigkeit untersagt.

Der Bescheid ist von Gesetzes wegen sofort vollziehbar.

Aktualisierung vom 13.11.2020:

³⁸ See the consolidated financial



354. Payvision received a total of € 9,439,042.89 in card payments for Celtic Pay Ltd. and forwarded them to the company (transferred from the payment account at ING Amsterdam to the bank account of Celtic Pay Ltd. in Bucharest).

Transaction laundering schemes and miscoding as a usual part of business activities

356. In summary, Payvision – as a licensed and supervised EU payment service provider and licensee of Mastercard/VISA – is required by law and contractual law to install internal systems and procedures to avoid the misuse of the card payment system for money laundering and terrorist financing and to report any suspected money laundering and financing of terrorism by the law.
357. If a payment institution decides to do business with a high-risk client, that institution is required to conduct due diligence commensurate with that risk and to tailor its transaction monitoring to detect suspicious or unlawful activity based on the level of risk identified. Payvision, under the management of Booker, Cheng Liem Li, and Gijs op de Weegh knowingly, intentionally, deliberately, and maliciously failed to do so about its relationship with Barak and Lenhoff.
358. To profiteer from the fees and referrals generated by Barak and Lenhoff, Payvision intentionally, continuously, and outrageously allowed Barak and Lenhoff to use Payvision's services to cover up old crimes and to facilitate new ones.
359. Based on Payvision's activities above, it is evident that the company has deliberately ignored all legal and contractual requirements designed to prevent using the financial system for fraudulent, criminal organizations to achieve higher transaction volumes, revenues, and profits.
360. Payvision's intentional and outrageous participation in Barak and Lenhoff's transnational criminal organization was not a "one-off." On the contrary, its conscious participation fits within a pattern and practice of Payvision profiting by undertaking illegal "high risk, high reward" merchants.
361. It was only through this deliberate, knowing, and willful ignorance that convicted fraudsters such as Barak could steal consumers' life savings on a gigantic scale for years.
362. Among the financial benefits that Payvision received for participating in and facilitating Lenhoff and Barak's TCO venture were the fees for processing the card transactions of their fraudulent brands. But in addition, among the financial benefits that Payvision received for participating in Barak and Lenhoff's fraud venture were referrals of business opportunities from Lenhoff.
363. To effectuate the Transaction Laundering scheme, the principals of Payvision arranged for the stolen money to be disguised as payments to over several phony online merchants to be disguised as payments for licensed financial service providers. Payvision placed high-risk payments into low-risk categories.

364. Booker and his co-conspirators committed bank fraud by deceiving US and European banks about the true nature of the financial transactions they were processing. They also facilitated the online fraud of transnational criminal organizations.
365. By onboarding dozens of phony online merchants, the principals of Payvision masked merchants' identities, thereby facilitating money laundering and circumventing laws banning certain activities like crypto trading.
- 366. The lack of conscience, the ruthlessness and willfulness of PAYVISION, and its multiple involvements in similar fraud structures indicate a clear will to contribute. Since at least 2013, Payvision has knowingly processed payments for numerous merchant clients engaged in fraudulent activities, including merchants subject to law enforcement actions by law enforcement agencies all over Europe and the United States.**
367. Payvision's blatant disregard for banking laws gave transnational criminal organizations a virtual carte blanche to finance their operations.
368. Payvision knew of and substantially aided the Lenhoff and Barak online fraud. Payvision accepted millions of euros of irregular deposits and approved the related-party transfers, atypical lending, and funds commingling that marked Barak and Lenhoff's fraudulent scheme. In connection with providing such material assistance, Payvision was aware of its essential role in the scheme and knowingly acted in furtherance of it.
369. If Payvision had conducted due diligence as required by law, several transnational criminal organizations would not have been able to use the reputation of a financial service provider licensed in the Netherlands to carry out their illegal activities in Europe.
370. If Payvision had carried out proper and careful monitoring of transactions as required by law, Payvision would have noticed at the beginning of the customer relationships that Barak and Lenhoff were carrying out online fraud activities, 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.
371. Payvision's violations were serious and systemic and allowed specific onboarded merchants to launder millions of euros of proceeds from online fraud through Deutsche Bank/ING bank accounts over an extended period. Barak and Lenhoff's criminal files have identified that at least 154 million euros in online fraud proceeds were funneled through the merchant accounts provided by Stichting Payvision with Deutsche Bank/ING.
372. Even after Payvision's compliance department finally requested to stop working for Barak, Booker told them to go on after agreeing on a new processing agreement in July 2018.
373. The 273 SARS notifications made by Payvision, mainly starting in July 2018, according to his statement of 23 May 2019, clearly show that Booker had sufficient evidence of fraudulent activity.

374. With the 273 SARS reports submitted, a targeted attempt was made to cover up the involvement of Payvision in criminal activity.
375. The high number of SARS reports 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.
376. Payvision has demonstrably ignored all red flags, including
- Public warnings from European supervisory authorities on authorized dealers and/or scam websites.
 - Massive chargeback requests from victims,
 - fraud complaints from victims
 - house searches took place as early as summer 2018 (Binex)
 - Ongoing lawsuits
377. Payvision's actions and procedures are contrary to all ethical standards set by the authorities in the Netherlands and the European Union.
378. Up to 15 different Billing descriptors are used for the same website with different merchants and several MIDs for a single merchant.
379. In light of these red flags, in addition to knowing they were facilitating Lenhoff and Barak's TCOs, Payvision should have known that it was facilitating severe fraud ventures.

Aiding and Abetting Breach of Fiduciary Duties

380. At all relevant times, Barak and Lenhoff were the controlling owner and/or CEOs of the fraud entities. Because of Barak and Lenhoff's controlling position, actions, and direct and indirect representations to victims and because they deposited funds into Barak and Lenhoff's control with the understanding that they would act by his promises regarding the use of such funds, Barak and Lenhoff owed investors the fiduciary duties of loyalty and care and to deal honestly and in good faith.
381. Nevertheless, Barak and Lenhoff breached the fiduciary duties they owed to the victims.
382. Through Payvision's knowledge of Barak and Lenhoff's business model and banking activity, Booker and his accomplices knew that Barak and Lenhoff owed fiduciary duties to investors.
383. Booker and his accomplices substantially assisted Barak and Lenhoff's breaches of fiduciary duty while knowing they were breaching those duties. Barak and Lenhoff's breaches of duty were enabled by and would not have been possible but for Payvision's relevant actions and inaction

Add on: Pending criminal proceedings Rudolf Booker in Austria

384. Criminal proceedings are pending against Rudolf BOOKER, born 25. 03. 1975, former board member of PAYVISION B.V. at the Public Prosecutor's Office Wr. Neustadt (4 St 113/22m) on suspicion of attempted extortion (§ 15 StGB § 105 (1) StGB). Rudolf BOOKER, in cooperation with some hired guys (they termed themselves as high-pressure negotiators), tried to press a former business partner (Daniel Mattes /JUMIO) under threat of physical violence to transfer 1 million euros in Bitcoin to a wallet provided by BOOKER.