Vorab per e-mail: Johannes.Windisch@justiz.gv.at; guenter.goessler@justiz.gv.at

Wirtschafts- und Korruptionsstaatsanwaltschaft

Dampfschiffstraße 4

A-1030 Wien

Vorab per e-mail: poststelle@gensta-ba.bayern.de

Generalstaatsanwaltschaft Bamberg

Zentralstelle Cybercrime Bayern (ZCB)

Dr. Nino Goldbeck

Wörthstraße 7a

D-96052 BAMBERG

Wien, 30. April 2021

Referenz: Strafanzeige gegen Rudolf BOOKER, Gijs OP DE WEEGH, Cheng LIEM LI ehemalige Geschäftsführungsmitglieder der PAYVISION Holding B.V. und PAYVISION B.V. Molenpad 2, Amsterdam wegen Beitragstäterschaft zum schweren gewerbsmäßigen Betrug (§ 263 dStGB, § 148 öStGB) und Geldwäsche (§ 261 dStGB, § 165 öStGB)

Sehr geehrte Damen und Herren,

Allgemeines

1. Die *European Funds Recovery Initiative (EFRI)* ist eine Opferschutzorganisation i.S. der Richtlinie 2012/29/EU des europäischen Parlaments und des Rates vom 25. Oktober 2012 („Opferschutzrichtline). Wir unterstützen Opfer von Cyberkriminalität bei der Aufarbeitung, des an ihnen begangenen Verbrechens, kooperieren mit Strafverfolgungsbehörden und vertreten die Interessen der Opfer bei der Einforderung von Schadenersatzansprüchen.
2. EFRI, als Verein in Wien, Österreich, gegründet im Frühjahr 2019, vertritt inzwischen mehr als 988 europäische Verbraucher, die von Cyberkriminellen um mehr als EUR

55,8 Mio in Form von Investmentbetrug auch bezeichnet als Boilerroom scams betrogen wurden.

3. Der Schaden, der tausenden europäischen Verbrauchern – hauptsächlich älteren Menschen – durch die verschiedensten Arten von Investmentbetrug und Boilerroomscams zugefügt wird, ist momentan gigantisch und wird auf rund 1 Milliarde EUR pro Monat geschätzt.
4. Unschuldige europäische Verbraucher vertrauen auf die Zusagen und Versprechungen Cyberkrimineller hinsichtlich vorteilhafter Veranlagungsmöglichkeiten, überweisen ihre Lebensersparnisse und müssen nach Monaten erkennen, dass sie Opfer skrupelloser internationaler krimineller Organisationen geworden sind.
5. Diese Art von Betrug geht in Europa seit mehr als 10 Jahren vor sich und stellt durch die daraus resultierenden mannigfaltigen finanziellen und mentalen Konsequenzen wie Altersarmut, Depressionen, Vereinsamung, psychische und körperliche Folgeerkrankungen, eine Bedrohung für unsere Gesellschaft dar.

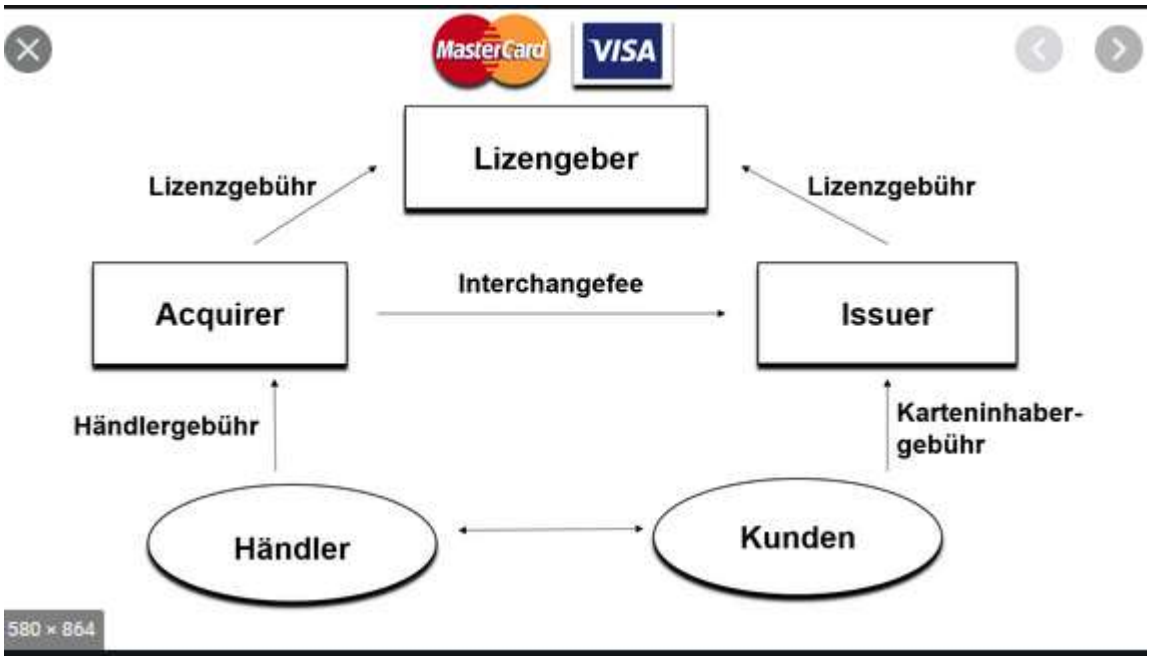
Zahlungsdienstleister als kritische Erfolgsfaktoren für diese Art von Cyberkriminalität

6. Kritischer Erfolgsfaktor für diese Art von Online-Betrugssystemen ist neben ausgeklügelten Softwaretools, aggressivem Marketing, betrügerischen Affiliate-Kampagnen und skrupellosen Call Center Mitarbeitern vor allem die Zusammenarbeit mit regulierten bzw. lizenzierten europäischen Finanzdienstleistern.
7. Diese europäischen Finanzdienstleister sind unabdingbar, um das Geld der Opfer entgegenzunehmen, zu waschen und schlussendlich an Offshore-Bankkonten unter der Kontrolle der Betrüger zur Anweisung zu bringen.
8. Erst durch die Zusammenarbeit mit regulierten Finanzdienstleistern erhalten die Betrugswebseiten die benötigte Seriosität, um tausende europäischer Kleinanleger davon überzeugen zu können ihre Lebensersparnisse an die Online-Betrugswebseiten, die Großteils Betreibergesellschaften in Destinationen wie British Virgin Islands oder Marshall Islands aufweisen zu überweisen.

Rechtliche Verhältnisse der PAYVISION

9. Basierend auf Unterlagen der von uns vertretenen Opfer sowie aufgrund diverser Erkenntnissen in strafrechtlichen und zivilrechtlichen Ermittlungsverfahren in Europa und in den USA, ist einer der europäischen Zahlungsdienstleister, der von diversen internationalen kriminellen Organisationen über viele Jahre hinweg, als Zahlungsdienstleister und Acquirer für Kredit- und Debitkarten Zahlungen genutzt wurde, die niederländische PAYVISION B.V. (in der Folge „PAYVISION“).
10. PAYVISION B.V. Molenpad 2, 1016 GM Amsterdam (KVK-Nummer: 3707811) ist ein niederländisches Unternehmen mit beschränkter Haftung, das 2002 von Rudolf BOOKER und seinem Mitbegründer Gijp op DE WEEGH gegründet wurde.

11. Bis zum 7. Mai 2020 bestand der Vorstand von PAYVISION aus Rudolf BOOKER, CEO, Gijp op DE WEEGH, COO und Cheng Liem LI, CCO.
12. Zur PAYVISION Gruppe gehören neben der PAYVISION B.V., die PAYVISION Holding B. V. gegründet am 24-5-2012: KVK-Nummer: 55358942 und die ACAPTURE B.V; KVK-Nummer 58184082 (heute Cetler B.V.) gegründet am 20-6-2013.
13. Weiters sind die Spezialverhikel **Stichting Trusted Third Party PAYVISION** und **Stichting Trusted Third Party ACAPTURE** Teil der Konzerngruppe.



14. Am 29. Januar 2018, gab Rudolf HAMERS – der damalige CEO der ING Groep B.V. bekannt[1], dass die ING Groep NV (in der Folge ING) – eine der größten Banken der Niederlande - eine Vereinbarung über den Erwerb einer 75%-Beteiligung an PAYVISION, Amsterdam abgeschlossen hatte. Der vereinbarte Kaufpreis betrug EUR 380 Mio. Die erreichte Bewertung betrug somit das 12-fache des erzielten Jahres-Bruttoergebnisses auf den Umsatz zum 31.12. 2017 (EUR 29 Mio). Die Gründer von PAYVISION hatten lt. diverser Medienberichte lange nach einem Käufer gesucht.
15. Im November 2019 erklärte sich ING bereit, den verbleibenden Anteil von 25 % an PAYVISION in drei Tranchen zwischen November 2019 und April 2020 basierend auf der ursprünglichen Bewertung von EUR 380 Mio, mit einer zusätzlichen Zahlung von EUR 90 Mio zu erwerben.

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

16. Im Mai 2020 verließen Rudolf BOOKER, Gijs op de WEEGH and Cheng LIEM ihre Vorstandsposten.
17. Im Geschäftsbericht der ING zum 31. Dezember 2020 (veröffentlicht im März 2021) wird auf Seite 65 berichtet, dass im Geschäftsjahr 2020 eine Abschreibung in Höhe von EUR 260 Mio auf Firmenwerte (mehr als EUR 200 Mio davon entfallen auf PAYVISION lt. Analystenberichte) durchgeführt wurde. Auf Seite 175 des Geschäftsberichts wird weiters ausgeführt, dass bereits bei der Akquisition der PAYVISION erkannt worden wäre, dass die Art der Kunden der PAYVISION (Porno und Gambling wird im spezifischen angeführt) nicht zu den Aktivitäten der ING passen würde und daher bereits 2018 damit begonnen wurde, diese Art von Kunden abzubauen. (Beilage 1 und 2).

Geschäftstätigkeit der PAYVISION

18. PAYVISION ist ein Zahlungsdienstleistungsunternehmen, das von der niederländischen Zentralbank (De Nederlandsche Bank (DNB)) gemäß der Europäischen Zahlungsdienstrichtlinie (PSD2) als solches lizenziert wurde und unter deren Aufsicht steht.
19. Darüber hinaus ist PAYVISION ein Lizenznehmer der Kreditkartenunternehmen (MasterCard/VISA). Dadurch kann PAYVISION sowohl für die Card-Present als auch in der Card-Not-Present-Umgebung als Acquirer fungieren und Kreditkarten- und Debitkarten Zahlungen für Betreiber von Onlinewebseiten (Händler) auf von PAYVISION[2] für die Händler geführten Bankkonten entgegennehmen und in der Folge an die Händler auszahlen.
20. Wie in der Folge ausgeführt wird, hat sich PAYVISION so wie WIRECARD, dass inzwischen insolvente deutsche FinTech, - bedingt durch die höheren erzielbaren Margen – von Gründung an, auf das Geschäft mit Hochrisiko-Händlern[3] konzentriert.

---

[2] Bzw. von ihren Konzerngesellschaften Stichting Trusted Third Party PAYVISION und Stichting Trusted Third Party ACAPTURE.

[3] Die Kreditkartenunternehmen klassifizieren bestimmte Geschäftsvertikale aus underwriting-Sicht als "hohes Risiko". Einige Händler werden als "hohes Risiko" eingestuft, weil sie anfälliger für Zahlungskartenbetrug und Rückbuchungen sind. Andere können als "hohes Risiko" angesehen werden, weil sie in Branchen tätig sind, die einem hohen Maß an Kontrolle durch Regulierungs- und Durchsetzungsbehörden ausgesetzt sind und daher ein höheres Maß an regulatorischen und Reputationsrisiken für Mastercard und VISA und Zahlungsdienstleister darstellen. Häufige "Hochrisiko"-Kategorien sind: Adult Entertainment, Feuerwaffen, Alkohol/Harter Alkohol, Tabak/eCig/VAPE, Nutraceuticals, Auktionswebseiten, Apotheken, Multi-Level-Marketing. Wetten, Lottery Tickets, Casino. binäre Optionen, Forex. Viele Akquirer bzw. Payment Service Provider arbeiten aufgrund der Art der verarbeiteten Transaktionen bzw. auch aufgrund des hohen Reputationsrisikos nicht mit Hochrisiko-Händler. Daher sind Hochrisiko-Händler bereit höhere Margen zu zahlen an Acquirer, die bereit sind, ihre Transaktionen zu verarbeiten. Skrupellose Zahlungsdienstleister und Acquirer nutzen dieses Abhängigkeitsverhältnis aus, indem sie betrügerische und rechtswidrige Taktiken anwenden, um gesetzliche Anforderungen zu umgehen, um Betrüger und Betrüger unterstützen zu können.
Damit verstößt der skrupellose Zahlungsdienstleister nicht nur gegen Gesetze und Card Brand Rules, sondern erleichtert auch betrügerische Geschäfte und ermöglicht es Betrügern, unschuldige Menschen abzuzocken, die von der Integrität der Zahlungsdienstleister ausgehen.

21. PAYVISION hat seit Jahren – vor und nach dem Erwerb durch ING bis heute – für Unternehmen aus den sogenannten High-Risk-Bereichen wie Porno (zB. PORNHUB), Gambling oder Trading (Binäre Optionen, Forex, CFD) Transaktionen abgewickelt.
22. Zusätzlich hat sich PAYVISION jedoch auch unter Verletzung der dem Unternehmen als reguliertem Zahlungsdienstleister auferlegten rechtlichen Bestimmungen (vor allem zum Thema Geldwäsche), aber auch unter Verletzung der Auflagen der Kreditkartenunternehmen an seine Lizenznehmer, an der Durchführung von Betrugssystemen internationaler kriminelle Organisationen wie BARAK und LENHOFF beteiligt und hat diesen den Zugang zum Finanzsystem ermöglicht.
23. PAYVISION hat vorsätzlich, wissentlich und willentlich auch für andere skrupellose Finanzdienstleister Dienstleistungen erbracht, wie T1 Payments LLC (siehe Punkt 88f) und Allied Wallet (Punkt 109ff).
24. Unsere Behauptung, dass PAYVISION am vielfachen Betrug an europäischen aber auch US-Konsumenten wissentlich und willentlich beteiligt war und dass es den Betrügern nur durch die vorsätzliche Mithilfe der PAYVISION gelang über Jahre hinweg zigtausende Konsumenten um ihre Lebensersparnisse zu bestehlen, kann wie folgt nachgewiesen werden:

- Informationen aus den Strafakten von LENHOFF/BARAK beim Straflandesgericht Wien (730 Js 1545/18).
- Aussagen vom exCEO des Unternehmens Rudolf BOOKER in obigen Strafakten.
- Einzahlungsbestätigungen (Banktransfers und Kreditkartenabrechnungsnachweise) für andere Betrugssysteme.
- Informationen aus öffentlichen Unterlagen über in den Vereinigten Staaten anhängige Rechtsfälle, in die PAYVISION involviert ist.

Beitragstäterschaft PAYVISION für die Betrugssysteme von Gal BARAK und Uwe LENHOFF

25. Am 29. Januar 2019 verhafteten die österreichischen und deutschen Strafverfolgungsbehörden LENHOFF, einen deutschen Staatsbürger. Er wurde des schweren gewerbsmäßigen Betrugs und der Geldwäsche beschuldig. Lenhoff war von den Ermittlungsbehörden als wirtschaftlicher Eigentümer folgender Betrugswebseiten (Handelsplattformen) identifiziert worden: Option888, ZoomTrader, ZoomTrader, Tradovest, Lottopalace, Xmarkets. Seit 2016 gab es unzählige Strafanzeigen geschädigter Europäer bei den Strafbehörden Europas zu diesen Betrugswebseiten.
26. Das Strafverfahren gegen LENHOFF wurde in Wien eröffnet und anschließend nach Saarbrücken übergeben. Am 5. Juli 2020 wurde LENHOFF tot in seiner Zelle/Haftanstalt in Saarbrücken aufgefunden.

27. Laut den Kundenlisten in den LENHOFF Strafakten haben 29.000 Opfer (hauptsächlich europäische Verbraucher) mehr als EUR 60 Mio an die betrügerischen Systeme Option888, Xmarkets und ZoomTrader in den Jahren 2015 bis 2018 überwiesen.
28. Ebenfalls am 29. Januar 2019 wurde Gal BARAK, israelischer Staatsbürger und enger Geschäftspartner von LENHOFF, in Sofia, Bulgarien, verhaftet. BARAK betrieb Callcenter in Sofia Bulgarien und war darüber hinaus der wirtschaftliche Eigentümer der Betrugswebseiten (Handelsplattformen) xTraderFX (früher CryptoPoint), Option Stars/OptionStarsGlobal, Goldenmarkets und Safemarkets. Auch hier gab es unzählige Strafanzeigen von geschädigten Europäern bereits seit 2016.
29. Nach den Kundenlisten, die in den Strafdateien der GAL BARAK enthalten sind, wurden von mehr als 35.000 Opfern (95% sind europäische Verbraucher) für die betrügerischen Systeme der GAL BARAK insgesamt mehr als EUR 120 Mio überwiesen
30. Nach mehr als 24 Monaten dauernden strafrechtlichen Ermittlungen wurde Gal BARAK vom Straflandesgericht Wien am 1. September 2020 (122 HV 4/20g) wegen schweren gewerbsmäßigen Betrugs und Geldwäsche für schuldig befunden.
31. Das österreichische Strafgericht (Urteil liegt den Adressaten vor) sieht es als erwiesen an, dass die Gelder der Tausenden unschuldigen europäischen Kunden nie für Investitionen verwendet wurde, wie von den Betrugswebseiten bzw. den Call Center Mitarbeitern versprochen wurde.
32. Der nachvollzogene Geldfluss weist vielmehr nach, dass die erhaltenen Gelder über verschiedenen Layer in Mantelgesellschaften gewaschen wurden und schließlich auf Offshore-Konten der Betrüger gelandet sind.
33. Die Anklage sowie das Urteil iS Gal BARAK, identifiziert die niederländische PAYVISION als Hauptzahlungsdienstleister für die Betrugswebseiten von LENHOFF und BARAK für das Jahr 2015 bis Jänner 2019.
34. Nach Angaben der österreichischen/deutschen Strafverfolgungsbehörden im Strafverfahren gegen BARAK (wirtschaftlicher Eigentümer der Betrugssysteme (=Betrugswebseiten) wie xtraderfx, safemarkets, goldenmarkets, Cryptopoint, Optionstars/Optionstarsglobal) und LENHOFF (wirtschaftlicher Eigentümer der Betrugswebseiten xMarkets, Option888, Lottopalace) hat das Unternehmen PAYVISION im Zeitraum von Herbst 2015 bis Januar 2019 mehr als EUR **131,2 Mio** an Kredit- und Debitkarten Zahlungen der Opfer dieser Systeme verarbeitet.

Total stolen money processed by PAYVISION2)

	Sum Transaktionen	Anz Transaktionen	Sum Chargeback	Anz Chargeback	Sum Fraud	Anz Fraud
Payific ltd	18.272.610,96 €	73.665	613.041,87 €	667	372.237,76 €	650
Hithcliff ltd	27.547.372,92 €	36.848	1.059.749,17 €	1.162	353.792,57 €	631
Celtic Pay ltd	9.826.550,91 €	12.104	378.170,62 €	344	58.923,66 €	174
Zwischensumme	**55.646.534,79 €**	**122.617**	**2.050.961,66 €**	**2.173**	**784.953,99 €**	**1.455**
Markets Development	28.101.859,97 €	26.843	2.125.984,71 €	1.252	1.065.605,74 €	971
Cool Markets	1.750.215,06 €	1.427	104.127,50 €	50	18.382,05 €	28
Optiumcommerce	4.806.545,28 €	4.868	819.898,78 €	310	51.485,14 €	103
Matching Blue Consulting	3.487.272,43 €	2.684	384.003,55 €	204	68.850,48 €	83
Gpay ltd	37.464.887,13 €	34.195	3.849.711,24 €	2.242	1.491.477,50 €	1.144
Zwischensumme	**75.610.779,87 €**	**70.017**	**7.283.725,78 €**	**4.058**	**2.695.800,91 €**	**2.329**

35. Tausende und abertausende von gutgläubigen europäischen Konsumenten überwiesen mittels ihrer Kredit- und Debitkarten ihre Lebensersparnisse an die kriminellen Organisationen von LENHOFF und BARAK. Die Firmen von LENHOFF und BARAK waren bei PAYVISION als Merchants registriert, PAYVISION selbst war ein lizenzierter Acquirer für die Kreditkarten-Netzwerke.

36. Die Finanzströme für die Kartenverarbeitung (Acquiring) liefen über Konten speziell eingerichtete Vehikel wie Stichting Trusted Third Party PAYVISION und Stichting Trusted Third Party ACAPTURE bis 2018 über Deutsche Bank Konten und nach der Übernahme durch die ING über Konten der ING Bank.

37. Die PAYVISION überwies zweiwöchentlich die eingenommenen Kundengelder abzüglich ihrer Marge und sonstiger Bearbeitungsgebühren (z.B. Charge-Back Gebühren usw. an die Konten der Betrüger.

38. Obige Zahlen enthalten nicht die Bank-Transfers, die durch Überweisungen von Opfern auf Anweisung von Call Center Mitarbeitern der Betrugssysteme an illegale Finanzagenten ausgestattet mit Bankkonten bei verschiedenen ING Tochter-gesellschaften getätigt wurden.

Mantelgesellschaften als ausschließliche Vertragspartner von PAYVISION

39. RUDOLF BOOKER legte seiner schriftlichen Stellungnahme an die österreichische Polizei vom 23. Mai 2019 (Appendix 8) eine Liste der Vertragspartner von PAYVISION für die Betrugswebseiten bei und lieferte auch die Namen der Geschäftsführer, die die Verträge mit PAYVISION unterzeichnet haben (Appendix 2).
40. Lt. dieser Auflistung (Appendix 2) hatten mehrere Betrugswebseiten (im Papier als Plattformen bezeichnet) jeweils ein und dasselbe Unternehmen als Vertragspartner der PAYVISION, das Kredit-/Debitkarten Zahlungen von Kunden für diese Plattformen entgegennahmen. Die von BOOKER als Vertragsgesellschaften beschriebenen Unternehmen hatten ihren offiziellen Sitz in einem europäischen Land.

41. Weiters gab es lt. dieser Aufstellung auch „verbundene[4] Gesellschaften“, die in der Folge – ohne ein Vertragsverhältnis zu PAYVISION – zu haben, Kundengelder auf Anweisung von BARAK und LENHOFF überwiesen bekamen. Diese Gesellschaften hatten ihren Sitz teilweise in Offshore-Ländern wie beispielsweise Marshall Islands, Britisch Virgin Islands und SAMOA.
42. Lt. den Aufstellungen im Strafakt wurde von PAYVISION auch noch an andere Gesellschaften, die nicht in der Aufstellung von BOOKER enthalten sind, Kundengelder auf Anweisung von LENHOFF und BARAK hin überwiesen (vgl. weiter unten). Auch diese – nicht aufscheinenden Gesellschaften – hatten ihren Sitz nicht in Europa, sondern in Ländern wie Marshall Islands und British Virgin Islands.
43. Der Großteil der Betrugswebseiten (=Plattformen) wiesen als Betreiber und Eigentümer Offshore-Gesellschaften auf, die nicht mit den Vertragspartnern der PAYVISION übereinstimmten.
44. Beispielsweise wurde die New Markets SA, SAMOA als Eigentümerin der Webseite www.optionstarsglobal.com (Appendix 3) für 2016 bis 2018 angezeigt. Vertragspartner der PAYVISION war die Markets Development EOOD, Bulgarien.
45. Die Betrugsplattform www.Xmarkets.com wies die Gesellschaft Capital Force Ltd, Republik SAMOA, als Eigentümerin (Appendix 4) auf[5].Vertragspartner der PAYVISION war die Celtic PAY Ltd, London für die Abwicklung der Transaktionen der Kunden der www.xmarkets.com oder auch die Hithcliff Ltd, London.
46. Die Erhebungen im Strafverfahren zu den Vertragspartnern von PAYVISION ergaben folgenden Sachverhalt:
    - Bei jedem einzelnen der Vertragspartner von PAYVISION handelte es sich um
    - ein gerade gegründetes oder erworbenes Unternehmen ohne Historie,
    - ohne Mitarbeiter und
    - ohne Businesspläne, ohne Rechnungslegung
    - und mit Strohmännern - zum Teil Obdachlose - als Geschäftsführer und Eigentümer
    - keine Büroräumlichkeiten und keinen Internetauftritt
    - Bankkonten der offensichtlich inaktiven Gesellschaften waren vorwiegend in Sofia, Bulgarien bei ein und denselben Banken.
    - Keines dieser Unternehmen hat eine Lizenz als Zahlungsdienstleister oder als Finanzdienstleister.
    - Die auf den Betrugswebseiten ausgewiesenen Eigentums- und Betreibergesellschaften sowie auch die Vertragsgesellschaften von PAYVISION wurden in Abhängigkeit vom Ausmaß der negativen Bewertungen zu den einzelnen Betrugswebseiten geändert.
    - Kam es zu einem Wechsel des Vertragspartners der PAYVISION, wurden diese exVertragsgesellschaften meist innerhalb weniger Monate wegen fehlender

[4] Der Begriff „verbundene“ Gesellschaft wird in diesem Zusammenhang von BOOKER nicht erläutert.
[5] Der Grund für die Verwendung der Offshore-Gesellschaften liegt in der Erhöhung der Schwierigkeit für die Opfer, die nach Realisierung des Betrugs versuchen an die Eigentümer und Betreiber der Betrugswebseiten heranzutreten.

Unterlagen aus dem Register des Companies House gelöscht. Beispiele dafür sind (vergleiche Appendix 5) Hithcliff Ltd und/oder Celtic Pay Ltd (Appendix 6).

- Gegen viele der von BOOKER als Vertragspartner von PAYVISION ausgewiesenen Gesellschaften, ebenso wie gegen manche der auf den Betrugswebseiten ausgewiesenen Eigentumsgesellschaften gab es seit 2016 Warnungen europäischer Aufsichtsbehörden.[6]

Enges persönliches Vertrauensverhältnis zwischen BOOKER/ BARAK und LENHOFF

47. Die unterzeichneten Geschäftsführer und offiziellen Vertragspartner der PAYVISION hatten keinerlei Kontakt zu PAYVISION. Das ergab beispielsweise die Einvernahme von RUMEN Kirilov GOGOV (Appendix 9). GOGOV war eingetragener Geschäftsführer der Markets Development EOOD, Sofia, Bulgarien und damit Vertragspartner der PAYVISION für die betragsmäßig erfolgreichste Betrugswebseite von Gal BARAK. (Appendix
48. Die gesamte day-to-day Kommunikation für die Vertragsgesellschaften der Betrugssysteme von GAL BARAK lief über einen bulgarischen Mitarbeiter von Gal BARAK (Boyan @Maevar).
49. Die gesamte day-to-day Kommunikation für die Vertragsgesellschaften der Betrugssysteme von LENHOFF lief über einen Mitarbeiter von LENHOFF.
50. BOOKER hatte direkten Kontakt zu BARAK und LENHOFF, in diesen Gesprächen wurden die wesentlichen Punkte, wie neue Vertragsunternehmen und Konditionen neuer Verträge besprochen.
51. Anzumerken ist, dass weder BARAK noch LENHOFF eine offizielle Geschäftsführungs- noch Eigentumsfunktion bei einem der Vertragspartner oder auch bei einem der offiziellen Eigentumsgesellschaften der Betrugswebseiten innehatten.
52. Aufgrund der erfolgreichen Zusammenarbeit wurde im Sommer 2018 eine Provisionsvereinbarung zwischen PAYVISION und LENHOFF abgeschlossen, PAYVISION verpflichtete sich zur Zahlung einer Provision für die Vermittlung weiterer Betrugsplattformen an die PAYVISION (Reseller Agreement - Appendix 14).
53. Abhörprotokolle von Telefonaten zwischen LENHOFF und BOOKER und sonstige Aufzeichnungen im Strafakt bestätigen die enge persönliche Beziehung zwischen den beiden, es gab persönliche Einladungen zu Geburtstagsfeiern, gemeinsame Skiurlaube und gemeinsame sonstige Interessen (grauer Kapitalmarkt) zwischen dem Betrüger und dem CEO von PAYVISION (Appendix 15.1 und Appendix 15.2).

[6] (Appendix 7ff). (FMA warnte vor Capital Force Ltd (Option888) zum 25. November 2017; FMA warnte vor New Markets S.A (OptionStarsGlobal) am 20 März, 2018; FCA warnte vor GPAY Ltd als CryptoPoint ab dem 14. Mai 2018; FCA warnte vor der Betrugswebseite xtraderfx (betrieben von der Gpay Limited) ab dem 7. Juli 2018, FCA warnte vor sicheren Märkten einen Handelsstil von OptimumCommerce OU ab dem 3. Januar 2019)

Zahlungen an Gesellschaften im wirtschaftlichen Eigentum von BARAK und LENHOFF ohne eine Vertragsbeziehung

54. Die Finanzermittlungen im Rahmen des Strafverfahrens ergaben das PAYVISION im Zeitraum vom Februar 2018 bis Mai 2018 auf Anweisung von LENHOFF an das bulgarische Bankkonto des Unternehmens Winslet Enterprises EOOD, Bulgarien (BG67STSA93000024171478) EUR 4,4 Mio vom Sammelkonto der Kundengelder überwies. Die Transfers zeigten den Zweck "Gewinnausschüttung". Mit dieser Gesellschaft hatte die PAYVISION keine Vertragsbeziehung.
55. Weiters ergaben die Finanzermittlungen, dass PAYVISION von Februar 2017 bis Dezember 2017 auf der Grundlage einer Aktennotiz (unterschrieben von einem Strohmann) (Appendix 10) EUR 10,2 Mio an NEW MARKETS SA, SAMOA überwiesen hat. NEW MARKETS SA, SAMOA, wurde 2017 als Betreibergesellschaft auf der Webseite www.OptionStarsGlobal.com angezeigt. Zum 30. März 2017 warnte die österreichische Aufsichtsbehörde vor NEW MARKETS SA (siehe Appendix 7). PAYVISION hatte keine Vertragsbeziehung mit dieser Gesellschaft.
56. PAYVISION überwies im Zeitraum 4. Oktober 2017 und 17. April 2019 mehr als EUR 2 Mio Kundengelder auf das bulgarische Bankkonto der Rockerage Ltd. (Anlage 2.1). Rockerage Ltd, ein als "verbundenes" (?) Unternehmen auf der BOOKER-Liste aufscheinendes Unternehmen, hatte seinen eingetragenen Sitz auf den Marshall-Inseln und war die Betreibergesellschaft für die Betrugswebseite www.safemarkets.com.

Geschäftstätigkeit von BARAK und LENHOFF

57. BOOKER gab in seiner Stellungnahme vom 23. Mai 2019 (Appendix 8) an, dass auf den Plattformen von BARAK und LENHOFF binäre Optionen angeboten wurden.
58. Gal Barak behauptete in seinen Einvernahmen sowie in der Hauptverhandlung vor dem Strafgericht, dass er im (Finanz)-Wettgeschäft tätig sei.
59. Lt. BOOKER hätten LENHOFF und BARAK PAYVISION im März 2018 mitgeteilt, dass sie das Geschäft mit binären Optionen stoppen würden - im Lichte der neuen Gesetzgebung, die im Juli 2018 in Kraft treten sollte. Um konform zu sein, drückten sie ihre Absichten aus, von binären Optionen zum Krypto-Handel und CFD-Produkte zu wechseln. Unter diesen neuen Bedingungen – laut BOOKER – konnte Payvision akzeptieren, die Verarbeitung für die Plattformen fortzusetzen.
60. Tatsächlich stellte das Wiener Straflandesgericht fest, dass weder auf den Betrugswebseiten noch im Vertragswerk mit den Kunden, eine Erwähnung von binären Optionen zu finden war und auch in der Kommunikation zwischen den Kunden/Opfern und den Call Center Mitarbeitern von BARAK und LENHOFF binäre Optionen nicht erwähnt wurden, sondern immer nur von Investitionen in Finanzinstrumente verschiedenster Art gesprochen wurde.

61. Auch die Aufsichtsbehörden warnten vor einem unlizenzierten Angebot von Finanzdienstleistungen auf den diversen BARAK und LENHOFF gehörenden Webseiten.
62. Keines der Vertragsunternehmen der PAYVISION die in Appendix 2 (von BOOKER bereitgestellte Liste der Vertragspartner) aufgeführt sind, hatten eine Lizenz für die Vermarktung oder den Verkauf von Finanzinstrumenten.
63. Am 24. Juli 2018 schloss PAYVISION einen neuen Vertrag mit GPAY Ltd[7], London ab (Vertragsunternehmen lt. Appendix 2 für die Betrugswebseite www.xtraderfx.com), unterschrieben hat GAL BARAK, obwohl er nicht eingetragener Geschäftsführer der GPAY Ltd war,[8]. Im Vertrag wurden für die gesamten von GAL BARAK betriebenen Webseiten (die lt. Vertrag nun Cryptotrading betrieben) neue Regelungen festgelegt.
64. Die Bearbeitungsgebühren wurden mit bis zu 7% in Kombination mit zusätzlichem fixem Gebühren für Gebührenrückerstattungen, Rückerstattungsgebühren und Abrufgebühren in diesem neuen Vertrag vereinbart[9]. Der Vertrag sah auch eine verbindliche Frist für ein monatliches Mindestvolumen von EUR 4 Mio für die nächsten drei Jahre (!) vor für alle von BARAG betriebenen Betrugswebseiten vor (!) und ermöglichte PAYVISION, den betreffenden Unternehmen die Differenz zwischen dem in einem Vertragsjahr verarbeiteten aggregierten Volumen und den Mindestverarbeitungsverpflichtungen in Rechnung zu stellen (Appendix 12).

Aufkündigung der Verträge durch PAYVISION

65. Nachdem auf der Webseite www.fintelegram.com („FinTelegram“) ab Sommer 2018 bekannt wurde, dass PAYVISION der hauptsächliche Zahlungsdienstleister für die Betrugswebseiten von BARAK und Lenhoff war, wandte sich BOOKER besorgt an LENHOFF.
66. Die Akten zeigen, dass PAYVISION nach den Artikeln auf FinTelegram umfangreiche Geldwäsche-Meldungen iVm den Artikeln machte. Dies weist darauf hin, dass PAYVISION und BOOKER die illegale Natur der Geschäfte ihrer Kunden sehr wohl bewusst war.
67. Abgehörte Telefonate belegen das Naheverhältnis zwischen BOOKER und LENHOFF (Appendix 15.1. und Appendix 15.2)
68. In der Folge war PAYVISION gezwungen – lt. Aussage von BARAK und LENHOFF aufgrund der negativen Medienberichterstattung – die Händlerverträge für die Betrugswebseiten zum 6. und 23. Dezember 2018 unter Einhaltung einer Frist von 4 Wochen zu kündigen.
69. BOOKER begründete die Kündigung mit einer von PAYVISION durchgeführten Customer Due Diligence im 4. Quartal, in seiner Stellungnahme vom 23. Mai 2019.

[7] Zu diesem Zeitpunkt hatte die FCA bereits am 14. Mai 2018 vor der GPAY Ltd als Cryptopoint https://www.fca.org.uk/news/warnings/gpay-limited-trading-cryptopoint und am 7. Mai 2018 vor der GPAY Ltd als xtraderfx gewarnt. https://www.fca.org.uk/news/warnings/xtraderfx

[8] Im Strafverfahren gab BARAK an, den im britischen Handelsregister eingetragenen Geschäftsführer der Gpay Ltd nicht zu kennen.

[9] Die vereinbarten Konditionen sind sogar für die Hochrisiko-Branche sehr hoch und zeigen einerseits das Abhängigkeitsverhältnis von BARAK und andererseits das Machtverhältnis von PAYVISION.

70. Trotz Kündigung der Verträge fanden in der Folge noch Telefonate zwischen BOOKER und LENHOFF und BOOKER und GAL BARAK bis Ende Januar 2019 statt.
71. Mit LENHOFF sprach BOOKER nachweisbar zuletzt wenige Tage vor der Verhaftung von LENHOFF (Appendix 15.1. Telefonanruf am 11. Jänner 2019) und versuchte offensichtlich noch Informationen über Vertragsverhältnisse der Vorjahre zu erhalten, um seine Unterlagen zu ergänzen.
72. Bei Auslauf der Kündigungsfrist Ende Januar 2019 – wenige Tage vor der Verhaftung von LENHOFF und BARAK – behielt PAYVISION einen Betrag von EUR 4,3 Mio ein.
73. Die bei den Hausdurchsuchungen in Sofia, Bulgarien beschlagnahmte E-Mail-Kommunikation zeigt, dass BARAK noch wenige Tage vor seiner Verhaftung eine baldige Auszahlung des zurückbehaltenen Betrages versprochen wurde (Appendix 16).
74. Die zwischen BARAK und BOOKER getroffene Vereinbarung auf Auszahlung des Geldes in Abhängigkeit von der Bereinigung der Gesellschaftsstrukturen (nur europäische Betreibergesellschaften sollten auf den Betrugswebseiten aufscheinen) konnte bedingt durch die Verhaftung von GAL BARAK am 29. Jänner 2019 nicht mehr umgesetzt werden.
75. Bis dato erfolgte seitens PAYVISION keine Abrechnung für diesen einbehaltenen Betrag.
76. BOOKER ist weder in seiner ersten Stellungnahme vom 23. Mai 2019 gegenüber den österreichischen Strafverfolgungsbehörden (Appendix 8) noch in seiner zweiten Stellungnahme vom 15. Juli 2019 (Appendix 11) auf diese einbehaltenen Kundengelder eingegangen
77. Inzwischen weiß PAYVISION nachweislich, dass es sich bei den einbehaltenen Kundengeldern um gestohlenes Geld handelt.
78. Zusammengefasst hat PAYVISION offenbar seine Vertrauensposition genutzt, um gestohlene Kundengelder unberechtigt einzubehalten und Schadensminimierung auf der Seite PAYVISIONS zu betreiben.

Involvierung von PAYVISION in andere Betrugssysteme

79. In seiner Stellungnahme vom 15. Juli 2019 informierte BOOKER die österreichische Staatsanwaltschaft darüber, dass PAYVISION bereits 2014 und 2015 die Transaktionen für die Betrugsplattformen der NOVOX Capital Ltd, Zypern (Optionsbit.com, Optionsxp.com, Optionsmerchants.com) abgewickelt hatte (Stellungnahme Booker vom 15. Juli 2019: Appendix 11).
80. PAYVISION verarbeitete auch die Kredit- und Debitkarten Zahlungen für die Betrugswebseite Binex (www.binex.ru). In einer in der Hausdurchsuchung Ende Jänner 2019 sichergestellten E-Mail-Kommunikation werden die Betrugswebseiten welche von PAYVISION abwickelt werden, von den Leuten von GAL BARAK aufgelistet. (Appendix 13). Die Betrugsplattform BINEX[10] wurde im Sommer 2018 geschlossen. Die Aktivitäten dieser illegalen Webseite werden von Polizeibehörden aus verschiedenen

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

Teilen der Welt untersucht. Eines der Call Center von BINEX in Kiew wurde bereits im August 2018 von der ukrainischen Cyberpolizei durchsucht Die 60 Mitarbeiter des Call Centers hatten in wenigen Monaten mehr als 15.000 Kunden in Russland, der Ukraine sowie in anderen Ländern (meist Osteuropa) zu Überweisungen zur Veranlagung in diverse (fiktive) Finanzinstrumente in mehrstelligen Millionenbeträgen überreden können.

81. PAYVISION hat auch Kredit-/Debitkarten Zahlungen der Betrugswebseite www.24option.com, betrieben von der Roedeler Ltd, abgewickelt (Appendix 21). In Köln, Deutschland läuft ein Strafverfahren gegen dieses langjährige Betrugssystem. Die britischen und die zypriotischen Aufsichtsbehörden untersagten der Rodeler Ltd im Juni 2020 die Geschäftstätigkeit.
82. PAYVISION verarbeitete auch Kredit-/Debitkarten Zahlungen für die Betrugswebseite AlgoTechs/BEALGO in den Jahren 2017 – 2019 (Appendix 20)

Banküberweisungen auf ING-Bankkonten von legalen und illegalen Finanzagenten für BARAK und LENHOFF Betrugssystem

83. Offenbar kam es durch BOOKER auch zur Eröffnung von Bankkonten für illegale Finanzdienstleister, die von verschiedenen Betrugsplattformen genutzt wurden bei verschiedenen ING-Banken.
84. MoneyNetInt Ltd, London – ein von Financial Conduct Authority (FCA) lizenziertes E-Geld- und Zahlungsinstitut (Referenz Nr. 900190)) – hatte ein Konto bei der ING Bank ,,L'ski Spéka Akcyjna" (PL73105000861000009030701412). Das Konto wurde für Einzahlungen der Opfer der Betrugsplattform www.optionstarsglobal.com verwendet. (Appendix 17.1)
85. Bereits im Juli 2016 berichtete die Times of Israel über die Beteiligung von MoneyNetInt Ltd, am binären Options Betrug. Im Frühjahr 2017 erließ die polnische Finanzaufsichtsbehörde ("KNF") eine Warnung zu den Tätigkeiten der MoneyNetInLtd (Appendix 17.2).
86. Leonsky Ltd in Madrid, Spanien, ein illegaler Finanzagent und hatte ein Konto bei der ING BANK N.V. SUCURSAL EN ESPAA (ES17 1465 0100 9519 0060 4045). Dieses Konto wurde für mehrere Betrugssysteme verwendet (einschließlich der Betrügereien von GAL BARAK). (Appendix 18)
87. STICHTING ESCROW ICEPAY (Lottopalace) (ICEPAY B.V., Amsterdam) hatte ein Konto bei der ING Bank Frankfurt (DE88 5002 1000 0010 1193 45) und fungierte auch als illegaler Zahlungsdienstleister, das Unternehmen wurde verwendet, um gestohlenes Geld für die Betrugsplattform von LENHOFF zu überweisen. (Appendix 19)
88. Für die Stichting WST Capital Ltd, veröffentlichte die US CFTC (Commodity Futures Commission bereits eine Warnung im 25. April 2017[11] über das und wies darauf hin, dass das Unternehmen in die Zahlungsabwicklung von binären Optionen involviert ist. Die Stichting WST Capital Ltd, hatte ein Konto bei ING Bank NL75INGB0006984998, und wurde verwendet, um gestohlenes Geld an die wirtschaftlichen Eigentümer des

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

Betrugssystems AlgoTechs / BEALGO (vergleiche im Detail Appendix 19) 2018 und 2019 zu überweisen.

EFRI INITIATIVE

PAYVISIONs Involvierung in US-Rechtsfällen

Beyond Wealth vs T1 Payments and PAYVISION

89. Am 28. Juli 2020 begann der Rechtsstreit (2:20-cv-01405-JCM-VCF) zwischen der Beyond Wealth PTE LLC, UTAH ("Beyond Wealth")– einem US Multilevelmarketing (MLM)-Unternehmen – und der T1 Payments LLC – einem Payment Facilitator[12]) in Bezug auf den unberechtigten Einbehalt von mehr als USD 4 Mio Gebühr bei Beendigung des zwischen Beyond Wealth und T1 Payments abgeschlossenen Zahlungsdienstleistungsvertrag vor dem United States District Court in Nevada.
90. Mit Schriftsatz vom 24. 08. 2020 der Beyond Wealth wurde PAYVISION B. V. Amsterdam ("PAYVISION“) als Gegenanspruchs-Beklagte in die Klage aufgenommen.
91. Beyond Wealth behauptete, dass T1 Payments LLC ("T1 Payments") in seiner behaupteten Eigenschaft als Payment Facilitator, Beyond Wealth im Mai 2020 in einen Händlervertrag für die Abwicklung von Kredit-/Debitkarten Transaktionen gelockt hätte, indem sie glaubhaft versicherten, dass sie ein bei den Kreditkartenunternehmen registrierter Payment Facilitator seien.
92. Nur Wochen später wurde das Vertragsverhältnis aufgelöst und Beyond Wealth musste feststellen, dass T1 Payments kein registrierter Payment Facilitator war und die Fähigkeit von T1 Payments, die Transaktionen von Beyond Wealth zu verarbeiten, von der niederländischen PAYVISION (Counterclaim-Defendant) und der Verletzung von rechtlichen Verpflichtungen der Bestimmungen der Kreditkartenunternehmen abhängig war.
93. Zusammengefasst behauptet Beyond Wealth, dass T1Payments sich der Tätigkeit des illegalen Finanzagenten, des Bankbetrugs und der Geldwäsche im Zusammenwirken mit der PAYVISION schuldig gemacht hätte[13].
94. Die Klage der Beyond Wealth beschreibt sehr detailliert, wie PAYVISION alle Transaktionen der Beyond Wealth verarbeitete, indem es ein Unterkonto für Beyond Wealth unter dem Master-Händlerkonto von T1 Payments eröffnete. Einen Vertrag zwischen Beyond Wealth und Payvision gab es nicht, obwohl T1 Payments kein von Mastercard/VISA zugelassener Payment Facilitator war. T1 Payments hatte ein Händlerkonto unter seinem Namen bei PAYVISION und PAYVISION hat die

[12]Ein Payment Facilitator steht in direktem Kontakt zum Händler und verwaltet im Auftrag der Subhändler das Händlerkonto beim Acquirer. Die Abrechnung über einen Zahlungsvermittler eignet sich in der Regel für junge Unternehmen mit noch kleineren Umsätzen.

[13] Manchmal können Acquirer Verträge mit Drittorganisationen abschließen, um Händlern im Rahmen der Acquirer Sponsoring mit den Kartenverbänden (solche Drittorganisationen Waren in den Visa-Regeln als "Drittagenten" und in den Mastercard-Regeln und im Folgenden als "Dienstleister" bezeichnet werden. Ein Dienstanbieter darf nur den Typ des Programmdienstes ausführen, für den er registriert ist, und muss bei den Karten registriert sein. Assoziation vor einen Erwerber oder Händler kann seine Dienste in Anspruch nehmen (siehe z. B. Mastercard-Regel 7.2 (Programm und Leistung des Programmdienstes).

Kundengelder, die aus der Verarbeitungstätigkeit stammen, an das T1 Payments Bankkonto bei der Atlanta Bank in Nevada eingezahlt.

95. Darüber hinaus behauptet Beyond Wealth, dass T1 Payments zwar ein US-Unternehmen mit Sitz in Nevada ist, die britischen Mantelgesellschaften der T1 Payments (T1 UK und/oder TGlobal) jedoch - gemäß erhaltener Anweisungen von T1 Payments - Vertragspartner von Beyond Wealth werden mussten, um T1 Payments zu ermöglichen, die Kreditkartentransaktionen durchzuführen.
96. Beyond Wealth LLC wurde von T1 Payments weiters angewiesen, ebenfalls eine britische Beyond Wealth UK zu gründen, um das Geschäft von Beyond Wealth mit der britischen Gesellschaft der T1 Payments zu ermöglichen. Obwohl es sich bei der Vereinbarung über die Abwicklung von Kundenzahlungen (Customer Payment Processing Agreement, CPPA) um eine direkte Vereinbarung zwischen den US-Firmen handelte und obwohl Transaktionen von US-Kunden der Beyond Wealth abgearbeitet werden sollten, wurden die Transaktionen unter den Namen der britischen Mantelgesellschaften eingereicht.
97. T1 Payments war bei der Gründung der britischen Beyond Wealth behilflich bzw. es war für Beyond Wealth offensichtlich, dass die T1 Payments im Zusammenwirken mit PAYVISION seinen Hochrisiko-Kunden einen eigenen Gründungsservice (Incorporationservice) anbot. Die Gründung britischer Unternehmen war gegen eine Gebühr von 250 USD Bedingung für den Abschluss einer Händlervereinbarung bei T1 Payments.
98. Erst im nach hinein, verstand Beyond Wealth, dass diese Mantelgesellschaften benötigt wurden, damit PAYVISION – ein europäischer Zahlungsdienstleister – Verträge mit diesen britischen Gesellschaften (T1UK oder TGlobal) für die Abwicklung der Transaktionen der US-Gesellschaft Beyond Wealth abschließen konnte.
99. Das diese Vorgangsweise mehrere massive Verstöße gegen die gesetzlichen für PAYVISION anwendbaren Regelungen[14] und auch gegen die regionalen Vorgaben der Kreditkartenunternehmen darstellte, wurde Beyond Wealth erst klar, nachdem sie erfuhr, dass T1 Payments über keine aufrechte Registrierung als Payment Facilitator verfügte und PAYVISION – ein europäischer Zahlungsdienstleister die Transaktionen zur Verarbeitung entgegennahm
100. Laut dem britischen Firmenbuch handelte es sich bei T1UK und TGLOBAL um offiziell inaktive Unternehmen sind, die nur 1 GBP an Vermögenswerten auswiesen. Tatsachen, die PAYVISION beim Vertragsabschluss nicht störten.
101. Beyond Wealth behauptet in der Klage gegen T1 Payments, dass T1 Payments sich mit PAYVISION verschworen habe, um den Anschein zu erwecken, dass sich die Händler im Vereinigten Königreich bzw. in der EU befanden und somit für eine Akzeptanz des Händlervertrages durch PAYVISION in Frage komme.

[14] Als europäischer Zahlungsdienstleister darf rechtlich PAYVISION nur Transaktionen mit Unternehmen im EWR-Raum abschließen und durchführen. Die Mastercard-Regel 5.1 (S. 59) sieht analog zu den entsprechenden VISA-Regelungen vor, dass Acquirer und Händler in derselben Jurisdiktion angesiedelt sein müssen.

102. Die Kreditkartenunternehmen verbieten es T1 Payments eindeutig als nicht bei den Kreditkartenunternehmen akzeptierter PAYMENT FACILITATOR Konten für Beyond Wealth und diese Händler bei einem Lizenznehmer zu eröffnen und Händlerverträge in eigenem Namen abzuschließen.
103. Beyond Wealth gibt in seiner Klage an, dass die von T1 Payments angewandte Vorgangsweise der Gründung britischer Mantelgesellschaften als Standardverfahren in den Onboarding-Anweisungen von T1 Payment beschrieben ist. Im speziellen wird In den Materialien die Beschaffung einer "EU Corp" angeboten.
104. Beyond Wealth behauptet in der Klage, dass T1 Payments ein- und dieselbe illegale Struktur, bei allen seinen High-Risk-Händlern anwendet und dass alle dieser rechtswidrigen Händlerverträge seit Jahren über die PAYVISION abgerechnet werden.
105. Eine Durchsicht des US – Klagsregisters (www.pacer.gov) ergibt, dass es dutzende ähnliche Klagen gegen T1 Payments in früheren Jahren gab, was offensichtlich PAYVISION nicht davon abhielt Zahlungsabwicklungdienstleistungen für dieses Unternehmen seit 2015 und 2016 anzubieten
106. In der am 9. November 2020 beim US-Gericht eingereichten Stellungnahme von PAYVISION ein (Dokument 103-2), wird bestätigt das PAYVISION nach niederländischem Recht nur für europäische Händler in Europa tätig werden darf.
107. Der Chief Risk Officer von PAYVISION, Maria Alida Johana Ruijters – Terprstra, bestätigte, in einer eidesstaatlichen Aussage, dass PAYVISION niemals Dienstleistungen im Bundesstaat Nevada angeboten hat, da PAYVISION rechtlich ausschließlich im EWR Raum tätig sein darf.
108. In den von PAYVISION weiters vorgelegten Unterlagen wird deutlich, dass PAYVISION seit vielen Jahren eine enge Beziehung zu T1 Payments und seinen britischen Mantelgesellschaften unterhält.
109. Um der vorgelegten Stellungnahme Nachdruck zu verschaffen, legte PAYVISION als Beweis einen Auszug aus internen Kundendokumenten vor, indem die britischen T1 Payments Gesellschaften als Kunden aufscheinen.
110. PAYVISION erklärt dabei nicht, warum alle durchgeführten Transaktionen, die auf diesen internen Dokumenten angezeigt werden, auf USD lauten.

PAYVISION s Engagement bei ALLIED WALLET

111. In ihrer Klage vom 23. Mai 2019 (2:19-cv-04355-SVW-E) wirft die US FTC (Federal Trade Commission) den Unternehmen Allied Wallet Inc, Nevada, Allied Wallet Ltd, UK, GT Bill LLC, Nevada, GT Bill Ltd, UK, sowie den wirtschaftlichen Eigentümern Ahmad Khawaja, auch bekannt als Andy Khawaja, und Mohammad Diab vor, dass diese Unternehmen und ihre wirtschaftlichen Eigentümer seit mindestens 2012 wissentlich Zahlungen für zahlreiche Unternehmen verarbeiten, die betrügerischen Aktivitäten nachgehen[15].

[15] Unter diesen Kunden der Allied Wallet befinden sich auch Unternehmen, die bereits Ziel diverser Strafverfolgungsmaßnahmen der FTC, der Securities Exchange Commission ("SEC") und sonstiger Strafverfolgungsbehörden waren.

112. Allied UK und Allied Inc sind als Payment Facilitator mit Mastercard und VISA registriert.
113. FTC behauptete, dass Allied Wallet zum Betrug von Pyramidensystemen, diversen Ponzisysteme und sonstiger betrügerische Unternehmen beitrug, indem Allied Wallet ihnen den Zugang zur Möglichkeit der Entgegennahme von Kredit- und Debitkarten Zahlungen gab.
114. Der Vorwurf lautet das Allied Wallet vorsätzlich Händleranträge mit falschen Angaben hinsichtlich der Geschäftstätigkeit abgeschlossen hätte um gemeinsam mit ihren betrügerischen Wiederverkäufern, Thomas Wells, und dessen Unternehmen Priority Payout die Vorgaben der Kreditkartenunternehmen hinsichtlich Kunden Due Diligence und Transaktionsüberwachung zu umgehen.
115. Ein weiterer Vorwurf der FTC ist, das durch die Gründung und Nutzung europäischer Mantelgesellschaften, um Zahlungen für US-Händler in Europa mit europäischen Zahlungsdienstleistern wie Wirecard oder PAYVISION, statt in den USA zu verarbeiten, Allied betrügerischen US-Händlern ermöglicht hat, sich dem allgemein strengeren regulatorischen Rahmen des US-Finanzsystems zu entziehen.
116. Die Gründung von britischen Mantelgesellschaften, um Hochrisiko Nicht-EU Händler einzurichten, sei Standardverfahren bei Allied Wallet gewesen, so der Vorwurf der FTC. Die Notwendigkeit, eine "EU Corp" zusätzlich zur tatsächlichen Unternehmensform des Händlers zu beschaffen, sei sogar in der internen Checkliste der Allied Wallet beim Abschluss jedes einzelnen Händlervertrages vorgegeben gewesen. All diese ausländischen Mantelgesellschaften hatten in der Regel keine Mitarbeiter, keine Räumlichkeiten, lediglich Strohmänner als Geschäftsführer und Eigentümer und waren vermögenslos.
117. Aus den Gerichtsunterlagen ergibt sich, dass sowohl PAYVISION als auch Wirecard, dass inzwischen insolvente deutsche Fintech, über Jahre hinweg als Acquirer für die Konstruktionen von Allied Wallet dienten und die Transaktionen der US-Hoch-Risiko Händler durchführten.

Informationen aus den FINCENFILES

118. Lt. der durch den FinCEN-Leak an die Öffentlichkeit geratenen Unterlagen der Geldwäscheaufsichtsbehörde FinCEN war PAYVISION jahrelang auf dem Radar FinCEN und mehrerer amerikanischer Banken, weil sie verdächtige Transaktionen von Kunden abgewickelt hatte, die nicht in den traditionellen Bankenkreislauf landen hätten sollen. Jahrelang bediente das Unternehmen Hochrisiko Kunden aus der Porno-, Glücksspielindustrie und sonstigen Sektoren, die von traditionellen Banken oft abgelehnt werden, weil sie anfällig für Betrug sind.
119. Wobei eine vorsätzliche und auffällige Zerteilung großer Transaktionen ohne ersichtlichen Grund feststellbar war. In nur wenigen Monaten wurden zig Millionen an Kunden wie die Pornoseite Pornhub überwiesen[16].

[16] Laut dem Bericht Het Financieele Dagblad vom xx

Qualifizierung der Nichtbeachtung gesetzlicher und vertraglicher Vorschriften

Niederländische Gesetzgebung

120. Zweck und Sinn der europäischen Geldwäscherichtlinien, der entsprechenden nationalen Gesetzgebungen sowie der vertraglichen Auflagen der Kreditkartenunternehmen an ihre Lizenznehmer ist es das herkömmliche Finanzsystem vor der Nutzung durch kriminelle und terroristische Organisationen zu schützen.

121. Im Einklang mit der Zahlungsdienste Richtlinie PSD2 [17], wie sie im niederländischen Bürgerlichen Gesetzbuch und dem Finanzaufsichtsgesetz (Wet op*het financieel toezicht – Wft*) verankert ist, müssen sich die niederländischen Zahlungsinstitute an das Gesetz zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (Wwft) und das Sanktionsgesetz von 1977 sowie an die Aufsichtsverordnung gemäß dem Sanktionsgesetz von 1977 (Sw) halten. Das niederländische Finanzministerium gab die „Allgemeine Leitlinien zum Gesetz zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (Wwft) und zum Sanktionsgesetz (Sw)" heraus. Die DNB hat ab Dezember 2019 Leitlinien zur Klärung der verschiedenen Verpflichtungen aus dem Wwft und der Sw herausgegeben und Instrumente zur Erfüllung dieser Verpflichtungen zur Verfügung gestellt.[18]

122. Die vom niederländischen Finanzministerium und der De Nederlandsche Bank (DNB) veröffentlichten Leitlinien zum Gesetz zur Bekämpfung der Geldwäsche, zur Terrorismusfinanzierung (Wwft) und zum Sanktionsgesetz unterstreichen die Aufforderung an niederländische Finanzinstitute, die Verantwortung für die Aufdeckung von Finanz- und Wirtschaftskriminalität zu übernehmen. Integrität wird als Voraussetzung für ein solides Finanzsystem angegeben, und die Aufsicht der DNB befasst sich mit der Integrität der niederländischen Finanzinstitute. Nach den Leitlinien ist die Integrität der Finanzinstitute eine der Säulen des Vertrauens und somit eine Voraussetzung für ein ordnungsgemäßes Funktionieren der Institutionen. Abschnitt 3.10 und Abschnitt 3.17 des Finanzaufsichtsgesetzes enthält die gesetzlichen Anforderungen zur Überwachung des ethischen Betriebsmanagements. Die wichtigste Voraussetzung ist, dass die Institutionen vermeiden müssen, sich an Handlungen zu beteiligen, die gegen das Gesetz verstoßen oder von der Gesellschaft als unangemessen angesehen werden, und dass sie die Integrität ihrer operativen Verwaltung schützen müssen. Gemäß den Richtlinien der DNB (veröffentlicht im Dezember 2019) muss ein ethisches Betriebsmanagement von Finanzinstituten gewährleistet sein; daher sei es wichtig, dass die Institutionen wissen, mit wem sie Geschäfte machen. Die Wft und der Wwft verlangen daher von den Instituten, ein angemessenes Customer Due Diligence (CDD)-System zu betreiben, um ihre Kunden zu kennen und Geschäftsbeziehungen mit Personen zu vermeiden, die das Vertrauen

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

in die Institution beschädigen könnten. Das Hauptziel der Wft und des Wwft ist es, dass das Institut weiß, mit wem es Geschäfte macht, die vom Unternehmen ausgeführte Tätigkeit und das die Geschäftsbeziehung kontinuierlich überwacht (und alle ungewöhnlichen Transaktionen meldet) wird - in einem dem Risiko angemessenen Umfang.

123. Es muss sichergestellt werden, dass Kriminelle daran gehindert werden, die Erträge aus ihren Verbrechen zu waschen, und dass Terroristen und sanktionierte Einrichtungen nicht in der Lage sind, die finanziellen Mittel zu erhalten, um ihre Aktivitäten aufrechtzuerhalten und Anschläge zu starten, und dass Einzelpersonen nicht in der Lage sind, von korrupten Praktiken zu profitieren.

124. Finanzinstitute dienen als erste Verteidigungslinie gegen illegale Finanztransaktionen in dem heutigen schnelllebigen, vernetzten Finanznetz. Nach EU-Recht und niederländischem Recht müssen diese Institutionen Strategien und Systeme zur Verhinderung und Aufdeckung illegaler Finanztransaktionen entwerfen und auch umsetzen.

Regeln der Kartenkartenunternehmen, die Lizenznehmer (Acquirer) einzuhalten haben:

125. Lizenznehmer der Kreditkartenunternehmen verpflichten sich alle Regeln einzuhalten, die die Kartenkartenunternehmen ihren Partnern – einschließlich aller Acquirer und Payment Service Provider, Payment Facilitator usw. für die Verarbeitung von Kartenzahlungen vorschreiben

126. Hauptzweck der von den Kreditkartenunternehmen auferlegten umfangreichen Bestimmungen ist es – ähnlich den gesetzlichen Regelungen - Betrug zu verhindern, die Transparenz der Zahlungsflüsse zu erhöhen und die Einhaltung der Gesetze zur Bekämpfung der Geldwäsche zu erhöhen und somit insgesamt das Risiko für das Finanzsystems zu verringern.

127. Vor dem Onboarden eines neuen Händlers (auch als „Merchant“ bezeichnet), fordern Mastercard sowie VISA von Ihren Lizenzunternehmen beispielsweise die unbedingte Identifizierung des wirtschaftlichen Eigentümers (UBO (ultimate beneficial owner)) sowie eine detaillierte Überprüfung des Zweckes und der Art der Geschäftsbeziehung. Die Partnerunternehmen sind weiters verpflichtet die Quelle der verarbeiteten Finanzströme zu überprüfen und die laufende Geschäftsbeziehung kontinuierlich zu überwachen.

128. Die VISA Regelungen erfordern zusätzlich während der Onboarding-Phase die Durchsicht folgender Dokumente des Händlers vom Acquirer:

- Rechtliche Unterlagen
- Beschreibung der Geschäftstätigkeit
- Rechnungslegungsberichte und Businesspläne
- Berichte von Ratingagenturen usw.
- Einkommensteuererklärungen
- Eine physische Inspektion der Geschäftsräume des potenziellen Vertragsunternehmens

- eine Durchsicht des Webauftritts
- und eine gründliche OSINT[19] Analyse

129. Sowohl Mastercard als auch VISA sehen für Hochrisiko-Händler speziell hohe Anforderungen hinsichtlich der Customer Due Diligence und der Überwachung der laufenden Transaktionen vor.

130. Kreditkartenunternehmen auferlegen ihren Lizenznehmer auch geografische Einschränkungen. So dürfen die Lizenznehmer ihre Finanzdienstleistungen nur „innerhalb des autorisierten "Nutzungsgebiets" an innerhalb dieser geografischen Region angesiedelten Unternehmen anbieten und erbringen.

[19] Open Source Intelligence

Nichteinhaltung der gesetzlichen und vertraglichen Verpflichtungen durch PAYVISION

131. Zusammenfassend ist bzw. war PAYVISION – als lizenziertes Zahlungsdienstleistungsunternehmen und Lizenznehmer von Mastercard/VISA – gesetzlich wie auch vertragsrechtlich verpflichtet, interne Systeme und Verfahren zu installieren, um zu vermeiden, dass das Finanzsystem für Geldwäsche und der Finanzierung des Terrorismus verwendet wird und jede vermutete Geldwäsche und /oder Finanzierung des Terrorismus nach dem Gesetz zu melden.

132. Basierend auf den unter Punkt 24 – 128 dargestellten Aktivitäten von PAYVISION ist offensichtlich, dass das Unternehmen alle gesetzlichen Vorschriften, und Vorgaben und Auflagen, die eine Nutzung des Finanzsystems für betrügerische kriminelle Organisationen verhindern sollen, vorsätzlich ignoriert hat, um damit höhere Transaktionsvolumina, Umsätze und Gewinne zu erzielen.

133. Nur durch diese vorsätzliche, wissentliche und willentliche Ignoranz konnten verurteilte Betrüger wie BARAK über Jahre hinweg Konsumenten in einem gigantischen Ausmaß um Ihre Lebensersparnisse bestehlen.

134. Hätte PAYVISION eine ordnungsgemäße und sorgfältige Kunden Due Diligence wie gesetzlich gefordert durchgeführt, hätten BARAK und LENHOFF nicht das Renommee eines in den Niederlanden lizenzierten Finanzdienstleisters nutzen können, um Ihre kriminellen Aktivitäten in Europa durchzuführen.

135. Hätte PAYVSISION wie gesetzlich gefordert eine ordnungsgemäße und sorgfältige Überwachung der laufenden Transaktionen durchgeführt, hätte PAYVISION bereits zu Beginn der Kundenbeziehung (Herbst 2015) gemerkt, dass BARAK und LENHOFF Betrugshandlungen durchführen und das hätte zur Konsequenz gehabt, dass der Betrug von BARAK und LENHOFF viel früher beendet worden wäre und nicht tausende europäische Konsumenten ihre Lebensersparnisse verloren hätten.

136. Die von BOOKER in seiner Stellungnahme vom 23. Mai 2019 angemerkten 273 SARS Meldungen die PAYVISION die BOOKER an die holländische FIU übermittelt hat, zeigen eindeutig, dass BOOKER genügend Hinweise auf betrügerische Aktivitäten hatte.

137. Mit den abgegebenen 273 SARS Meldungen erfolgte ein gezielter Versuch, der Vertuschung der Involvierung von PAYVISION in die kriminelle Aktivität.

138. Die hohe Anzahl der abgegebenen SARS Meldungen zeigt eindeutig, dass BOOKER wusste, was vor sich ging bzw. genügend Hinweise auf ein betrügerisches Vorgehen hatte und dass er wusste, dass er die Geschäftsbeziehung hätte, sofort beenden müssen.

139. Ein hohes Umsatzvolumen und die Darstellung eins hohen Wachstumes war für die Gründer und Vorstände der PAYVISION von Gründung des Unternehmens (2002) an offensichtlich wichtiger als die Einhaltung rechtlichen und ethischer Vorschriften.

140. Die Vorgangsweise von PAYVISION ist auch damit motiviert gewesen, dass der Hauptgesellschafter und CEO BOOKER seine Anteile an dem Unternehmen PAYVISION zu einer sehr hohen Bewertung im März 2018 an die ING Group N.V. verkaufen wollte.

141. PAYVSISION hat nachweisbar alle Warnsignale wissentlich und willentlich ignoriert, darunter
    - Öffentliche Warnungen europäischer Aufsichtsbehörden zu Vertragshändlern und/oder Betrugswebseiten
    - Massive Charge-Back (Rückbuchungs-) Anfragen von Opfern,
    - vorgetragene Betrugsmitteilungen von Opfern
    - stattgefundene Hausdurchsuchungen bereits im Sommer 2018.
    - Ständig wechselnde Vertragsunternehmen, bei denen es sich allesamt um neu gegründete Mantelgesellschaften handelte, die über keinerlei Finanzzahlen, keine Internetpräsenz, keine Mitarbeiter, keine Räumlichkeiten verfügten und deren Geschäftsführer und Eigentümer reine Strohmänner (teilweise ohne Wohnsitz) waren
    - dass auf den Betrugswebseiten, deren Transaktionen abgearbeitet wurden, Betreiber- und Besitzgesellschaften mit Sitz auf SAMOA oder Marshall Islands angegeben waren.
    - Die Tatsache, dass die tatsächlichen wirtschaftlichen Eigentümer der Betrugswebseiten für keines der Vertragsunternehmen von PAYVISION zeichnete.
142. Es bestand eine enge persönliche Beziehung zwischen den tatsächlichen wirtschaftlichen Eigentümern der Betrugswebseiten und dem Gründer und CEO der PAYVISION, die darin resultierte, dass BOOKER die Compliance Abteilung der PAYVISION offensichtlich immer wieder überstimmte.
143. Ohne dieses Ignorieren jeglicher rechtlicher Compliance Anforderungen ist nicht vorstellbar, dass
    - Millionen von Kundengeldern vom Sammelkonto der PAYVISION an Unternehmen, mit denen PAYVISION keinerlei Vertragsverhältnis hatte, auf Anweisung von GAL BARAK (New Markets SA, SAMOA) und LENHOFF Winslet Enterprises EOOD mit dem Zweck „Gewinnausschüttung“ transferiert wurden.
    - Verträge mit Strohmännern (zum Teil Obdachlose) abgeschlossen wurden, mit denen niemand von PAYVISION jemals gesprochen hatte.
144. Die Tatsache, dass über Jahre hinweg hunderte Betrugsbeschwerden bei PAYVISION zu den Betrugssystemen von BARAK und LENHOFF eingegangen sind und trotzdem BOOKER beabsichtigte noch im Sommer 2018 eine Provisionsvereinbarung mit LENHOFF zur Vermittlung weitere Betrugsplattformen abzuschließen, weist auf die Skrupellosigkeit von BOOKER hin.

ING Akquisition von PAYVISION durch die ING im März 2018

145. Jede kommerzielle und rechtliche due Diligence im Vorfeld der Übernahme von PAYVISION durch eines der größten Bankinstitute der Niederlande, die ING Groep NV im März 2018, musste die hochriskanten Geschäftsaktivitäten von PAYVISION aufgedeckt haben.

146. ING Groep BV war im Zeitraum des Erwerbs von PAYVSISON (2017) mitten in einem strafrechtlichen Ermittlungsverfahren wegen Geldwäsche, musste sich also der Brisanz der Nutzung des traditionellen Finanzsystems durch kriminelle Organisationen bewusst gewesen sein.
147. Nichtsdestotrotz wurde von der ING Groep NV eine Bewertung von EUR 360 Mio für PAYVISION akzeptiert.
148. Der Bedeutung des Anstrichs der Seriosität und der Glaubwürdigkeit für die Betrugswebseiten, dadurch dass ein Tochterunternehmen der ING die Abwicklung der Kredit und Debitkarten Transaktionen für diese Betrugswebseiten übernahm, lies sich PAYVISION von den Betrugswebseiten in höheren Margen und langen Vertragsbindungsdauern entgelten.

.

INTEGRITY und TRUST

149. Integrität der Finanzdienstleistungsunternehmen wird als Voraussetzung für ein solides und sicheres globales Finanzsystem angegeben. Nach den Richtlinien des niederländischen Finanzministeriums und der DNB ist die Integrität der Finanzinstitute eine der Säulen des Vertrauens und somit eine Voraussetzung für das ordnungsgemäße Funktionieren der Institutionen. Abschnitt 3.10 und Abschnitt 3.17 des niederländischen Finanzaufsichtsgesetzes enthalten die gesetzlichen Anforderungen für die Überwachung des ethischen Betriebsmanagements. Die wichtigste Voraussetzung ist, dass die Institutionen vermeiden müssen, sich an Handlungen zu beteiligen, die gegen das Gesetz verstoßen oder von der Gesellschaft als unangemessen angesehen werden, und dass sie die Integrität ihrer operativen Verwaltung schützen müssen.

Zusammenfassung

150. Wir sind zutiefst davon überzeugt, dass PAYVISION wissentlich, willentlich und unter Außerachtlassung aller gesetzlichen und vertraglichen Auflagen zur Tathandlung diverser internationaler krimineller Organisationen über viele Jahre hinweg einen substanziellen Beitrag leistete.
151. Der Tatbeitrag von PAYVISION, seiner Gründer und Manager hat zum Verlust der Lebensersparnisse tausender europäischer Konsumenten geführt, die gleichzeitig auch ihr Vertrauen in das europäische Finanzsystem verloren haben. Die Handlungen und die Vorgangsweise von PAYVISION verstößt dabei gegen alle ethischen Standards, die von den Behörden in den Niederlanden und der Europäischen Union festgelegt wurden.
152. Die gezeigte Gewissenlosigkeit, Skrupellosigkeit und Vorsätzlichkeit der PAYVISION und ihre mehrfache Involvierung in ähnlichen Betrugsstrukturen (Vgl. T1Payments (Punkt 88-108) und Allied Wallet (Punkt 109-115) lässt eindeutig darauf

schließen, dass der ehemaligen Geschäftsführung der PAYVISION der stattfindende Betrug an vielen europäischen Konsumenten bewusst war und der eindeutige Wille zur Beitragshandlung vorlag.

Privatbeteiligtenanschluß/Ädhaseionsverfahren

153. EFRI vertritt 69 österreichische und 108 deutsche Geschädigte der Betrugssystemen von GAL BARAK mit einem Gesamtschaden von EUR 1,4 Mio (Österreich) und von EUR 1,9 Mio (Deutschland).
154. EFRI vertritt 16 österreichische und 21 deutsche Geschädigte der Betrugssystemen von LENHOFF mit einem Gesamtschaden von EUR 1,8 Mio (Österreich) und von EUR 0,3 Mio (Deutschland)
155. EFRI vertritt 4 österreichische (Schaden EUR 69.974) und 4 deutsche Geschädigte des Betrugssystems AlgoTechs/BEALGO (EUR 78.730)
156. In Vertretung und im Auftrag der von uns vertretenen Geschädigten treten wir dem Strafverfahren gegen den Vorstand der PAYVISION als Privatbeteiligte bei bzw. stellen einen Adhäsionsantrag.

Mit freundlichen Grüßen

Elfriede Sixt Nigel Kimberley