EFRI INITIATIVE

EU-Kommission

Vice President Dubravka Šuica

Rue de la Loi 200

1049 Bruxelles, Belgien

Wien, 18. November 2020

Betreff: Einleitung Vertragsverletzungsverfahren wegen nicht zeitgerechter Umsetzung der EU-Geldwäsche-Richtlinien in den Ländern DEUTSCHLAND, NIEDERLANDE und BULGARIEN iSd Artikel 258 (ex Artikel 226 EGV) des Vertrags über die Arbeitsweise der Europäischen Union

Sehr geehrter Damen und Herren

1. Die European Funds Recovery Initiative (EFRI) wurde 2018 ins Leben gerufen und vertritt mittlerweile 876 europäische Verbraucher, die von internationalen Cyberkriminellen um ihre Lebensersparnisse gebrachte wurden.

2. In den Jahren 2016, 2017, 2018, 2019 und 2020 überwiesen diese 876 Geschädigten insgesamt mehr als **45,9 Mio EUR** über verschiedene Banken/Finanzdienstleister an die Besitzer betrügerischer Webseiten.

3. Anhand von Auswertungen der Finanztransaktionsdaten der Opfer, erstellten wir die beiliegende Follow the Money Auswertung (Beilage 1). Diese Aufstellung gibt wieder an welche Finanzinstitute die 876 europäischen Verbraucher gemäß erhaltener Anweisungen der Scammer ihr Geld überwiesen haben.

4. Von den insgesamt 45,9 Mio. EUR dieser 878 europäischen Verbraucher wurden 36.3 Mio. EUR (76,45%) über Online-Überweisungen und 6,9 Mio. EUR (15,10%) über Kredit/Debitkartenüberweisungen, d.h. über das traditionelle Finanzsystem, an die

Cyberkriminellen überwiesen. Nur 2,9 Mio. EUR (6,35%) gingen an die Betrüger durch direkte Überweisung von Krypto-Währungen.

5. 36,3 Mio EUR wurden somit über Konten reiner Mantelgesellschaften bei europäischen Finanzinstituten mittels Banktransfers abgewickelt. 6,9 Mio EUR wurden von lizenzierten Acquiring Organisationen abgewickelt und in der Folge auf Bankkonten von Mantelgesellschaften – die als Betreibergesellschaften (Merchants) in Vertragsverhältnisse mit den Kreditkartenorganisationen eingetreten sind - ausgezahlt.

6. Diese Mantelgesellschaften, gegründet ausschließlich zum Zwecke der Entgegennahme und der Weiterleitung des illegal erworbenen Geldes an die Betrüger bilden einen integralen Bestandteil der internationalen Cybercrimeorganisationen.

7. Diese Mantelgesellschaften erfüllen Alle die folgenden Kriterien:
    - Gründung erfolgte als Vorratsgesellschaft von Company Buildern oder auch von „Gründungsservices“ von den Acquiring Organisationen.
    - Keine physische Präsenz in den jeweiligen Ländern (eingeschriebene Briefe an die in den öffentlichen Registern eingetragenen Adressen wurden als unzustellbar zurückgeschickt).
    - Diese Mantelgesellschaften haben Geschäftsführer bzw. Eigentümer ohne entsprechenden Wohnsitz oder Aufenthalt im Land des Finanzdienstleisters und auch über eine umfangreiche Internetrecherche lassen sich keine Informationen über diese Geschäftsführer bzw. Gesellschafter finden („Strohmänner“).
    - Keine dieser Gesellschaften hatte Mitarbeiter.
    - Der in den öffentlichen Registern angegebene Geschäftszweck dieser Unternehmen entspricht nicht der ausschließlichen Tätigkeit dieser Unternehmen (illegale Geldeintreibungsunternehmen).
    - Die meisten dieser Gesellschaften wurden kurz vor Erhalt der Zahlungen neu gegründet oder waren kurz zuvor erworbene Vorratsgesellschaften.
    - Keine dieser Firmen hat oder hatte eine Online-Präsenz, obwohl die Mehrheit der Firmen laut öffentlicher Register eine Geschäftstätigkeit hat, die als internetaffin bezeichnet werden kann.

- Die auf die Konten dieser Mantelgesellschaften überwiesene Gelder - Beträge in Millionenhöhe innerhalb kürzester Zeit - wurden in regelmäßigen - vor allem aber sehr kurzfristigen - Abständen
- Die gesamte Lebensdauer diese Gesellschaften ist häufig nur wenige Monate, nach Gebrauch als illegaler Finanzdienstleister werden die Gesellschaften liquidiert oder wegen Vermögenslosigkeit gelöscht.

8. Die massenhafte Kontoführung solcher Mantelgesellschaften bei den europäischen Finanzdienstleistern ist der Schlüssel, um den illegalen Fluss des gestohlenen Geldes zu den Betrügern zu ermöglichen.

9. Aus den Strafakten des in Wien, Österreich wegen schweren Betrugs und Geldwäsche verurteilten Israeli GAL BARAK wird offensichtlich das das gestohlene Geld bevor es an die Offshore Unternehmen die im offiziellen Besitz der Cybercriminellen stehen, überwiesen wird meist noch an Service-Gesellschaften weitertransferiert wird um das Geld als Dienstleistungsentgelt zu legalisieren. Auch für diesen Prozess braucht es unzählige Mantelgesellschaften, die über Konten bei diversen europäischen Finanzinstituten verfügen müssen[1].

Cyberkriminalität im Aufwind

10. die zunehmende Digitalisierung der Gesellschaft im Allgemeinen und die damit verbundene Virtualisierung des Geldes im Besonderen bringt eine neue, massive Bedrohung für die Konsumenten mit sich - die transnationale Cyberkriminalität. Die Kombination modernster Technologien mit neuen Marketingmethoden und einer massiven Disparität in der Technikaffinität der Internetnutzer schafft eine noch nie dagewesene Ökosphäre für Kriminelle was sich in massiv steigenden Zahlen der gemeldeten Cyberkriminalstraftaten wiederspiegelt[2].

11. Unseren Opfern wurde klar, dass, obwohl die Europäische Union versucht, die Digitalisierung voranzutreiben, Bargeld zu eliminieren und die Online-Zahlungsindustrie zu fördern, weder die örtlichen Strafverfolgungsbehörden noch die europäischen Vollzugsbehörden wissen, wie man angemessen gegen Cyberkriminalität

[1] Dazu vgl. Punkt …

vorgeht. Modernste Technologie vermischt mit krimineller Energie erfordert eine entsprechende Ausbildung und Erfahrung der Behörden. Zu diesem Zeitpunkt, da sich die Cybergesellschaft der EU noch am Anfang einer Lernkurve befindet, mussten unsere Opfer einen hohen Preis - ihre Lebensersparnisse - zahlen, um das zu lernen.

12. Der einheitliche Währung im EU-Binnenraum in Kombination mit den Fortschritten im gemeinsamen Zahlungsraum vergrößern die Problematik noch.

13. Die äußerste Notwendigkeit der Bekämpfung und Verhinderung der Nutzung des Finanzsystems für Zwecke der Cyberkriminalität liegt daher auf der Hand und ist eines unserer wichtigsten Ziele.

14. Wir sind davon überzeugt, dass die Verhinderung der Nutzung des europäischen Finanzsystems zum Transfer der gestohlenen Gelder an die Cyberkriminellen einen hohen und vielleicht der einzig wirksamen Beitrag zur Eindämmung der Cyberkriminalstraftaten ist.

15. Die Nutzung des traditionellen Finanzsystems zum Betrug an tausenden und abertausenden europäischen Verbrauchern ist nur möglich, weil offensichtlich in den einzelnen Ländern der Europäischen Union die Richtlinien der Geldwäsche zwar **gesetzlich umgesetzt wurden aber deren Einhaltung in keinster Weise geahndet oder sanktioniert wird.**

16. In der Folge zeigen wir anhand von drei Beispielen das exemplarische Versagen dieser Behörden in drei Ländern: Deutschland: Punkt 17 – 29, Niederlande: PAYVISION Punkt 20 – 29, Bulgarien Punkt 30 – 38 auf.

Deutschland als Geldwäscheparadies

17. Von den insgesamt 36 Millionen EUR wurden 11,6 Millionen EUR (26,21% der gesamten Überweisungen) von deutschen Banken abgewickelt. Hier haben die DB/Postbank (insgesamt 4,5 Mio. EUR) und die Wirecard AG (insgesamt 2,6 Mio. EUR) im Laufe der Jahre eine führende Rolle übernommen.

18. Die Wirecard BANK AG hat sich von der Abwicklungsstelle für Porno, Gaming und binäre Optionen, Forex über die Jahre zu der Hausbank vieler Scammer entwickelt. Es sind also die Betrüger selbst, die die Konten zur Entgegennahme und Weiterleitung illegaler Geldströme führten. Ein Beispiel ist hier die Geldwäscheanzeige einer Korrespondenzbank Ende 2019/Anfang 2020 für das Betrugssystem #24option in Höhe von 220 Mio EURO.

19. Im Falle der DB/Postbank geschah dies über von uns identifizierte 83 (!) Konten illegaler Zahlungsdienstleister über die gestohlene Gelder verschiedenster Betrugssysteme gesammelt und weitergeleitet wurden.

20. Da unsere Initiative nur einen kleinen Teil des Tag für Tag in Europa vor sich gehenden Online-Betrugs repräsentiert, ist davon auszugehen, dass die Wirecard und die DB/Postbank hunderte, wenn nicht tausende solcher Mantelgesellschaften den Transfer gestohlener Gelder ermöglicht hat.

21. Die Aktivitäten der deutschen Wirecard-Gruppe im illegalen Sektor sind seit der Gründung des Unternehmens im Jahr 1999 bekannt. Im Jahr 2017 wurde ein umfassender Bericht über die Geldwäschetätigkeiten der Gruppe veröffentlicht und den zuständigen deutschen Behörden vorgelegt (Zatarra-Bericht). Die Behörden wurden nicht aktive. Immer wieder gab es im Laufe der Jahre Hinweise auf massive Geldwäscheaktivitäten des Unternehmens und Unregelmäßigkeiten in der Rechnungslegung des DAX-Unternehmens. Am 1. Februar 2020 legte die EFRI-Initiative der BAFIN und der zuständigen Staatsanwaltschaft München eine Geldwäscheanzeige mit umfangreichen Anlagen (Anhang 2) vor. Zwei Wochen später informierte ich die Staatsanwaltschaft München über das Vorliegen der Geldwäscheanzeige einer Korrespondenzbank der Wirecard über verdächtige Transaktionen im Zusammenhang mit dem Betrugssystem #24Option (unzählige europäische Opfer) im Ausmaß von 220 Mio EUR. Die Staatsanwaltschaft München unternahm nichts.

22. Auch die Deutsche Bank verfügt über eine lange Liste von Verurteilungen wegen Geldwäsche (siehe auch die Punkte 21.1 bis 21.6 des beigefügten Geldwäsche-Anzeige (Anlage 3), die wir am 27. März 2020 der BAFIN und der Staatsanwaltschaft Frankfurt vorgelegt haben. Die von uns bei der Staatsanwaltschaft Frankfurt eingebrachte Strafanzeige ist immer noch unbearbeitet mangels personeller Ressourcen.

23. Besonders eklatant ist, dass die von den europäischen Finanzmarktaufsichtsbehörden ausgesprochenen öffentlichen Warnungen und Verbote einzelner betrügerischer Unternehmen von den deutschen Finanzdienstleistern bei der Eröffnung von Konten oder der Unterhaltung von Kontoverbindungen in keiner Weise berücksichtigt werden bzw. wurden.

24. Dass auch Warnungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BAFIN) von den deutschen Banken regelmäßig ignoriert werden, zeigt das Beispiel der GRENKE Bank, die ein Konto der FinTechServices GmbH[3] unterhielt und die Annahme illegaler Gelder bis in den Spätsommer 2018 ermöglichte, obwohl die Geschäftstätigkeit als illegaler Zahlungsanbieter der Fintech Service GmbH[4] bereits am 8. Mai 2018 untersagt wurde.

25. Die Bundesanstalt für Finanzdienstleistungsaufsicht - BAFIN hat weder zu unserem Geldwäsche-Bericht über die Wirecard Bank AG noch zu dem Geldwäsche-Bericht der Deutschen Bank/Postbank Stellung genommen. Aufgrund von Medienberichten wissen wir, dass sich die BAFIN für die WIRECARD einfach nicht verantwortlich fühlte - offensichtlich nicht einmal für die Bank.

26. Auch tausende verzweifelte europäische Verbraucher, die seit vielen Jahren bei der Aufklärung des an ihnen begangenen Verbrechens, Hilfe bei der BAFIN suchen, wurden im Laufe der Jahre freundlich, aber entschieden zurückgewiesen.

27. Auf der Grundlage der verfügbaren Analyse der Finanztransfers von lediglich 822 Opfern solcher Betrugssysteme und mit dem Wissen, dass Tausende und Abertausende von europäischen Opfern solcher Betrugssysteme ihre gestohlenen Gelder auf deutsche Konten eingezahlt haben, kann davon ausgegangen werden, dass in den Jahren 2016 bis 2020 Millionen, wenn nicht Milliarden (Lebensersparnisse

[3] Die FinTech Service GmbH ist insofern noch eine Besonderheit, da diese Gesellschaft selbst als „Boiler Room“ tätig war und der Geschäftsführer seit… angeklagt ist von der SEC….

[4]

europäischer Bürger) gestohlener Gelder über deutsche Konten an Cyberkriminelle in offshore Länder geflossen sind.

28. Die BAFIN nimmt offensichtlich ihre Verpflichtungen zur Beaufsichtigung des Bankensektors im Hinblick auf Geldwäsche nicht wahr.

29. Lt der Medienberichterstattung wurde auch das System der Financial Intelligence Unit offensichtlich in Deutschland nie wirksam umgesetzt. Die Nichtbearbeitung von tausenden SARs eingemeldet bei der deutschen Financial Intelligence Unit wurde im Wirecard Skandal evident und ist seit dem Bekanntwerden des Bilanzbetruges und dem Konkurs des Konzerns ein Thema der dt. Medienberichterstattung.

PAYVISION - ein niederländisches FinTech

30. Die in Amsterdam registrierte PAYVISION B.V. ist ein im Jahr 2002 gegründeter Payment Service Provider5 der als Zahlungsdienstleister für Onlineshops auftritt. Zusätzlich ermöglicht PAYVISION B.V. den Onlineshops die Akzeptanz von Kreditkartenzahlungen und trat dabei als Acquiring Partner für die Betreibergesellschaften (Merchants) der Webseiten auf. Die Finanzströme gehen dabei über eigens dafür gegründete Vehikel wie Stichting Trusted Third Party PAYVISION.

31. Alleiniger wirtschaftlicher Eigentümer der PAYVISION ist die ING Groep N.V., Amsterdam, Niederlande. Im Zuge der Umsetzung ihrer FINTECH-Strategie hat die ING Group N.V. im Frühjahr 2018 75% der Anteile an dem Startup PAYVISION zu der Bewertung von 360 Mio EUR übernommen, basierend vor allem auf der „höchst positiven Geschäftsentwicklung“ des Unternehmens. Ende 2019 hat die ING in der Folge auch die restlichen 25% der Anteile an der PAYVISION übernommen und die Gründer ausgekauft.

32. Basierend auf den Aussagen der Beschuldigten UWE LENHOFF und GAL BARAK aus dem Strafakt 9 ST 16/19p-116 sowie aus den Stellungnahmen von Rudolf BOOKER/CEO PAYVISION ist ersichtlich, dass folgende Betrugs-Systeme abgewickelt wurden über PAYVISION als Acquiring Partner:

- Option888, ZoomTraderGlobal, Tradovest, Lottopalace, (mehr als 55 Mio EUR) (2016 – 2019)
- XTraderFX, OptionStarsGlobal, safemarkets, goldenmarkets (mehr als 77 Mio EUR (2016 – 2019)
- EasyTrade, Binäre Optionen (beneficial owners not yet known) (Ausmaß der Zahlungen unbekannt)

[5] Ein Payment Service Providers in unserem Fall meint dabei, dass Payvision die technische Schnittstelle der Webshops zu einer Vielzahl von Zahlungsmöglichkeiten zur Verfügung stellte.

- AlgoTechs/BEALGO (beneficial owners not yet known) (Ausmaß der Zahlungen unbekannt)

- GetFinancial (Ausmaß der Zahlungen unbekannt).

33. Laut den Unterlagen der PAYVISION weisen die dem Uwe LENHOFF zuzuordnenden Gesellschaften und Plattformen einen Gesamtzahlungsvolumen (abgewickelt über die PAYVISION Systeme) in Höhe von 55,6 Mio EURO auf. Die dem Gal BARAK zuzuordnenden Gesellschaften und Plattformen weisen einen Volumen in Höhe von 75,6 Mio EURO auf:

	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**

34. Bei den über PAYVISION an die Betreibergesellschaften der Webshops weitergeleiteten 130 Mio EUR gestohlenen Geldern von großteils europäischen Konsumenten handelt es sich lediglich um die Kredit/und Debitkartenzahlungen dieser Betrugssysteme. Zusätzlich flossen rund 140 Mio EURO an Banküberweisungen unter zu Hilfenahme von illegalen Zahlungsdienstleistern in Europa und Serbien an die Betrüger, sowie weitere 20 Mio EUR an Kryptowährungen. Hinzuweisen ist hier, dass das Gesamtbetrugsvolumen von 290 Mio EURO auf lediglich 8 Online Tradingplattformen erzielt wurde[6].

35. Bei den Betreibern der oben genannten und anderen Betrugs-Webseiten (Scams) handelte es sich immer um Mantelgesellschaften mit Strohmännern als Direktoren (Nominee Directors) und Gesellschafter (Nominee Shareholders). Der Sitz dieser

[6] Es gibt unzählige solcher Tradingplattformen im Web.

Mantelgesellschaften war in Ländern wie SAMOA, Marshall Island, St. Vincent and Grenadines, Seychellen.

36. Es gab bereits ab 2016 veröffentlichte Warnungen verschiedener Finanzmarktaufsichtsbehörden gegen diese Betrugssysteme, der unter der Aufsicht der niederländischen Central Bank stehende Zahlungsdienstleister PAYVISION ignorierte alle diese Warnungen[7], [8].[9],[10],[11].

37. Am 5.Juni 2019 sandte EFRI bereits eine Sachverhaltsdarstellung an die niederländische Central Bank mit der Darstellung des Sachverhaltes und mit der Bitte um Untersuchung des Sachverhaltes und der Information das noch zusätzliche Informationen abrufbar waren. Bis dato keine Reaktion.

38. Am 10. Oktober 2019 sandte EFRI die an die PAYVISION gerichteten Forderungsbriefe wiederum mit dem Angebot mehr Informationen zur Verfügung zu stellen an die niederländische Central Bank – auch hier wiederum keine Reaktion bis zum heutigen Datum.

39. Generell entwickelt sich durch das hohe Ertragspotential von Online Investmentbetrug die Zahlungsdienstleistungsbranche für die Betrugswebseiten mit einem immensen Tempo.

---

[7] https://www.fca.org.uk/news/warnings/gpay-limited-trading-cryptopoint.

[8] Die österreichische Finanzmarktaufsichtsbehörde (FMA) hat mit Bekanntmachung im Amtsblatt zur Wiener Zeitung vom 30. März 2018 mitgeteilt, dass *New Markets S.A. (OptionStarsGlobal)* mit Sitz in Novasage Chambers, Level 2 CCCS Building, Beach Road, Apia, Samoa nicht berechtigt ist, konzessionspflichtige Bankgeschäfte oder Wertpapierdienstleistungen in Österreich zu erbringen. Es ist dem Anbieter daher der gewerbliche Handel auf eigene oder fremde Rechnung (§ 1 Abs 1 Z 7 BWG) sowie die gewerbliche Portfolioverwaltung (§ 3 Abs. 2 Z 2 WAG 2018) nicht gestattet.

[9] CONSOB warning against Option888 and its operators: https://smnweekly.com/2016/12/28/italys-consob-warns-of-ayrex-option888-binary-options-brokers-broker-yard-forex-broker/ (dated **December 28, 2016)**

[10] FCA warns against Option888 and its operators https://smnweekly.com/2016/12/28/italys-consob-warns-of-ayrex-option888-binary-options-brokers-broker-yard-forex-broker/ (**dated May 2018**).

[11] FMA wars against Option888 https://www.fma.gv.at/capital-force-ltd-option888/ https://www.fma.gv.at/capital-force-ltd-option888/ **(dated 25. November 2017**).

BULGARIEN – Ein EU-Scam- und Geldwäsche-Hub

Das Geldwäschesystem der Gal Barak Cybercrime Organisation

40. Am 1. September 2020 erging am Landesstrafgericht Wien im Rahmen der sogenannten Vienna Cybercrime Trials ein erstes Urteil. Der israelische Staatsbürger Gal BARAK wurde als Betreiber und wirtschaftlicher Eigentümer der in Sofia, Bulgarien, angesiedelten Cybercrime Organisation der E&G Bulgaria wegen schweren Betrugs and Geldwäsche schuldig gesprochen.

41. Im Zuge der Ermittlungen zu diesem Strafverfahren wurden von den europäischen Behörden die bulgarischen Bankkonten von mehr als 46 Unternehmen geöffnet.

42. All diese Unternehmen zeigten folgende Merkmale:

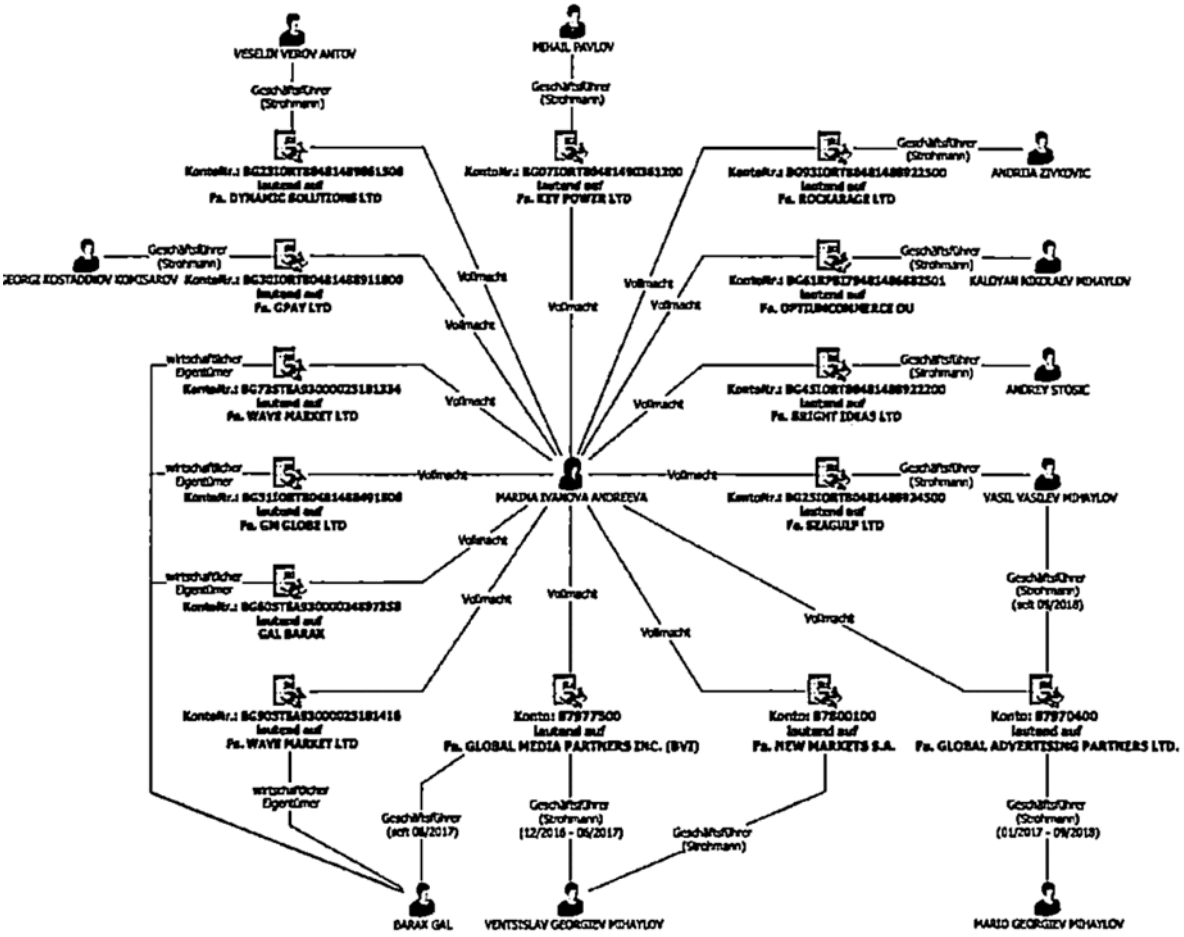
- Es handelte sich mit der Ausnahme der Boiler Room (Call Center) Betreiber und zweier Technologiedienstleister ausschließlich um reine Mantelgesellschaften.
- Nur drei dieser Unternehmen hatte Mitarbeiter.
- Nur bei 11 dieser Unternehmen handelte es sich um in Bulgarien registrierte Unternehmen, der Großteil der Unternehmen waren registriert auf British Virgin Islands, Marshall Islands, Hong Kong, London, SAMOA, Serbien usw.
- All diese Mantelgesellschaften hatten Nominees – meist osteuropäische Staatsbürger - als Geschäftsführer und Eigentümer installiert.
- Alle Geschäftsführer der Mantelgesellschaften erteilten den tatsächlichen wirtschaftlichen Eigentümern (Scammern) eine Handlungsvollmacht (Power of Attorney) für Geldtransaktionen. In den meisten Fällen war Vollmachtnehmer die Frau von Gal BARAK, Marina Barak (vormals Marina ANDREEVA)
- Als Ansprechpartner für Rückfragen aber auch für die Durchführung der Überweisungen beim online-banking war entsprechend beim Großteil der Konten dieser 82 Bankkonten die Telefonnummer von Marina BARAK hinterlegt.
- Aus den Auswertungen der österreichischen Strafbehörden wurde auf Grund von Auswertungen der IP-Adressen ersichtlich das Marina BARAK den Großteil der Konten auch tatsächlich administrierte und die Transaktionen durchführte.

- Tatsächlich verfügungsberichtigt für all die Konten dieser Gesellschaften waren also lediglich die wirtschaftlichen Eigentümer der Cybercrime Organisation

43. Diese 46 Unternehmen hatten mehr als 82 Bankkonten bei bulgarischen Banken, wobei 50 auf die Investbank (IORTBGSF XXX - INVESTBANK PLC, Sofia) 10 auf die DKS-Bank (STSABGSFXXX BIC/SWIFT-Code - DSK BANK AD Bulgaria ... und 11 auf die Eurobank (BPBIBGSFXXX BIC/SWIFT-Code - EUROBANK BULGARIA ...) entfielen.

44. Über die Konten dieser Unternehmen flossen im Zeitraum zwischen 01.01.2016 bis 31.03.2019 insgesamt EUR 200 Mio an gestohlenen Geldern.

Grafisch aufgelöst wurde die Bedeutung von Marina BARAK von den Strafbehörden für die wesentlichsten Bankkonten wie folgt:



45. Ein kritischer Faktor zum Aufbau eines Geldwäschekreislaufes ist der Zugang zu Company Buildern (offshore und in Europa), die eine schier unendliche Anzahl von Mantelgesellschaften mit Strohmännern als Geschäftsführer und nominelle Eigentümer und mit entsprechenden Bankkonten ausstatten und den Betreibern der Scams zur Verfügung stellen.

46. Laut den Aussagen von Alexander Ignatova – einem ehemaligen Call Center (Boiler Room) Mitarbeiter von Gal BARAK bei der Cybercrimeeinheit in Bamberg Deutschland im Juli 2019, gibt es in Sofia, **Bulgarien 60 Call Center** nach dem Beispiel des von GAL BARAKs betriebenen Boiler Rooms.

47. Diese Aussage von Alexander Ignatova stimmt mit unseren Beobachtungen überein, die wir aus den Einmeldungen der bei uns registrierten Opfer erhalten. Es gibt unzählige bulgarische Unternehmen, die in den Dokumenten diverser Betrugsschemata entweder als Betreiber- oder als Dienstleistungsunternehmen aufscheinen. Der Rückschluss, dass Konten bei der bulgarischen Investbank PLC, Sofia oder bei der DKS Bank AD Bulgaria genutzt werden um täglich Millionen, wenn nicht Milliarden an gestohlenen Ersparnissen von hauptsächlich Westeuropäern in offshore Länder zu transferieren, ist naheliegend.

48. Wie kritisch ein gutes „Zusammenspiel“ mit europäischen Banken ist, wird offensichtlich bei Verstehen der Geldwäschesysteme der Betrüger. Es wird jedoch auch offensichtlich, wie wenig wahrscheinlich es ist, dass es sich bei dem Mitwirken, der im speziellen Fall bulgarischen Banken um ein bloßes nicht entsprechendes Anwenden der europäischen Geldwäscherichtlinien handeln kann. Es spricht viel für Vorsatz der involvierten Banken oder auch für reines Inkaufnehmen, dass illegale Gelder im immensen Ausmaß über Konten bulgarischer Banken gewaschen werden.

Verletzung der Umsetzung der 4. und 5 Geldwäscherichtlinien der europäischen Länder

49. Schätzungen zufolge beläuft sich das Volumen der Geldwäschegeschäfte weltweit auf zwei bis fünf Prozent des Welt-Bruttoinlandsprodukts. Das sind 1,9 Billionen EUR, die eingesetzt werden, um Bestechung und Korruption zu finanzieren, kriminelle Machenschaften auszubauen und terroristische Vereinigungen zu unterstützen.

50. Geldwäsche und Terrorismusfinanzierung werden zu fast 70 % über legitime Finanzinstitute abgewickelt. Laut Schätzung des United Nations Office on Drugs and Crime wird jedoch weniger als 1 % des globalen Handels beschlagnahmt und eingefroren."

51. Mit den EU-Geldwäsche-Richtlinien adressiert der europäische Gesetzgeber diese Problematik und will das präventive System verbessern, um Geldwäschepraktiken und Terrorismusfinanzierung noch wirksamer bekämpfen zu können.

52. Sowohl die Bestimmungen der 4. Als auch der 5. EU-Geldwäsche-Richtlinie enthalten präzise und detaillierte Anforderungen an die einzelnen Mitgliedsstaaten zur Sicherstellung einer wirksamen Bekämpfung von Geldwäsche in dem jeweiligen Mitgliedsland.

53. Jedes Mitgliedsland ist aufgrund der Vorschriften der 4. und der 5. EU-Geldwäsche-Richtlinie verpflichtet zeitgereicht (4. Geldwäscherichtlinie bis zum 26. Juni 2017 und 5. Geldwäscherichtline bis zum 20.Jänner 2020) eine entsprechende Struktur zur Bekämpfung von Geldwäsche oder Terrorismusfinanzierung in ihrem Land aufzubauen und deren Wirksamkeit sicherzustellen.

54. Aufgrund der von uns durchgeführten Erhebungen[12] und exemplarischen Darstellung der Problemfelder in lediglich drei europäischen Ländern, wird offensichtlich das die diversen europäischen Länder bis dato weder die Bestimmungen der 4. EU-Geldwäsche-Richtlinie noch die der 5. Geldwäsche-Richtlinie zeitgerecht umgesetzt haben.

[12] Vgl. Appendix 1: Follow the Money evaluation of the EFRI-Initiative.

55. Im speziellen kann beispielhaft für Deutschland im Bezug auf die 4. Geldwäscherichtlinie festgehalten werden:

- Deutschland hat bis dato keine angemessenen Schritte, unternommen, um die für ihn bestehenden Risiken der Geldwäsche und Terrorismusfinanzierung zu bewerten, zu verstehen und zu mindern (Artikel 7 (1) – (4)).
- Deutschland hat bis dato nicht dafür gesorgt, dass die Verpflichteten über Strategien, Kontrollen und Verfahren zur wirksamen Minderung und Steuerung der auf Unionsebene, auf mitgliedstaatlicher Ebene und bei sich selbst ermittelten Risiken von Geldwäsche und Terrorismusfinanzierung verfügen. (Artikel 8)
- Deutschland hat bis dato nicht sichergestellt, dass die Verpflichteten bei Begründung einer Geschäftsbeziehung Sorgfaltspflichten gegenüber Kunden anwenden (Artikel 11 ff)
- Die in Deutschland eingerichteten Meldestelle (Financial Intelligence Unit) ist nachweisbar nicht mit den angemessenen finanziellen, personellen und technischen Mitteln ausgestattet, um ihre Aufgaben erfüllen zu können. (Kapital IV, Abschnitt I, Artikel 32)
- Deutschland hat nicht zeitgerecht sichergestellt, dass die Wirksamkeit ihres Systeme zur Bekämpfung von Geldwäsche oder Terrorismusfinanzierung überprüft werden kann, indem umfassende Statistiken über Faktoren, die für die Wirksamkeit solcher Systeme relevant sind, geführt werden. (Artikel 44)
- Deutschland hat nicht zeitgerecht sichergestellt, dass die zuständigen Behörden eine wirksame Überwachung durchführen und die erforderlichen Maßnahmen treffen, um die Einhaltung der 4. EU-Geldwäsche Richtlinie sicherzustellen (Artikel 48).
- Deutschland hat nicht zeigerecht sichergestellt, dass die politischen Entscheidungsträger, die zentralen Meldestellen, die Aufsichtsbehörden und andere an der Bekämpfung von Geldwäsche und Terrorismusfinanzierung beteiligte zuständige Behörden auch im Hinblick auf die Erfüllung ihrer Verpflichtung nach Artikel 7 über einen wirksamen Mechanismus verfügen, die bei der Entwicklung und Umsetzung von Strategien und Maßnahmen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung die Zusammenarbeit und Koordinierung im Inland ermöglichen (Artikel 49).

ZUSAMMENFASSUNG

56. Anhand der Beispiele Deutschland (DB/Wirecard), Niederlande (PAYVISION), Bulgarien (Investbank,...) wird deutlich, dass das europäische System zur Bekämpfung der Geldwäsche ("AML") und der Terrorismusfinanzierung ("CFT"), das sich in den letzten 30 Jahren etabliert hat, nicht zielführend ist.

57. Die europäischen Finanzorganisationen erfüllen nicht ihren Zweck, ein Torwächter für Finanzkriminalität zu sein.

58. Ahnungslose europäische Verbraucher werden damit zu leichten Opfern von Cyberkriminellen.

59. Im Namen und im Auftrag der 876 europäischen Opfer von Cyberkriminellen beantragen wir die Einleitung von Vertragsverletzungsverfahren gegen die Länder DEUTSCHLAND, BULGARIEN und die NIEDERLANDE.

60. Gleichzeitig bitten Sie, die volle Rückerstattung der von den Opfern erlittenen Schäden zu fordern. Wir sind überzeugt, dass Banken und Finanzorganisationen nur dann stoppen werden, Betrüger zu unterstützen, wenn Sie für die Unterstützung von Betrügern haftbar gemacht werden können.

Mit freundlichen Grüßen

Elfriede Sixt Nigel Kimberly

(Vorstand der EFRI-Initiative)

Beilage 1: Follow the Money evaluation of the EFRI-Initiative

Beilage 2: WIRECARD Geldwäscheanzeige vom 1. Februar 2020

Beilage 3: Deutsche Bank/Postbank Geldwäscheanzeige vom 28. April 2020