An die zuständige bezirksspezifische Staatsanwaltschaft:
Deutschland -
Staatsanwaltschaft München II
Generalstaatsanwalt Stephan Necknig
Leiter der Abteilung VI - Wirtschaftsstrafsachen
Seidlstraße 21
80097 München
Deutschland
Telefon: +49 (0)89 5597-6000
E-Mail: stephan.necknig@sta-m2.bayern.de
poststelle@sta-m2.bayern.de

9. August 2021

Betreff[1]

Strafanzeige gegen den Vorstand sowie den Chief Compliance Officer der HSBC Holdings PLC und HSBC Hong Kong [2] (im Folgenden "HSBC[3]") wegen Bildung einer kriminellen Vereinigung (bzw. Bandenkriminalität) mit transnationalen kriminellen Organisationen und damit Beihilfe zum Finanzbetrug (und nachfolgender Geldwäschestraftatbeständen) an tausenden unschuldigen europäischen Verbrauchern.

Allgemein

1. Die *European Funds Recovery Initiative (EFRI)* ist eine Opferschutzorganisation im Einklang mit der Richtlinie 2012/29/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2012 ("Opferschutzrichtlinie"). Wir unterstützen Opfer von Cyberkriminalität bei der Bewältigung der gegen sie begangenen Straftaten, kooperieren mit Strafverfolgungsbehörden in ganz Europa und handeln im Namen der Opfer bei der Geltendmachung von Schadenersatz.
2. EFRI, ein eingetragener Verein mit Sitz in Wien, Österreich, gegründet im Frühjahr 2020, vertritt mittlerweile mehr als 1.052 europäische Verbraucher, die im Zeitraum 2016 – 2020 von Cyberkriminellen um ihre Lebensersparnisse von insgesamt 59,2 Millionen Euro betrogen wurden.
3. Der Schaden, der Tausenden von europäischen Kleinanlegern - hauptsächlich älteren Menschen - durch verschiedene Arten von Onlinefinanzanlagebetrug/Boilerroom Scams zugefügt wird, ist in

[1] HSBC Holdings PLC, 8 Canada Square, London E14 5 HQ, Großbritannien

[2] HSBC Hongkong, 1 Queen's Road Central, Hongkong

[3] gemeint ist der HSBC-Konzern

den letzten Jahren stark gestiegen und beläuft sich innerhalb der EU auf mindestens 1 Mrd. EUR Schaden monatlich.[4]

4. Unschuldige europäische Kleinanleger werden durch Versprechungen hochprofessionell handelnder Cyberkrimineller hinsichtlich vorteilhafter Anlagemöglichkeiten getäuscht. Im Vertrauen auf ein funktionierendes europäischer Rechtssystem überweisen die europäischen Kleininvestoren ihre Lebensersparnisse und stellen nach Monaten fest, dass sie Opfer skrupelloser transnationaler krimineller Organisationen (TCO) geworden sind.
5. Diese Art von Betrug hat in den letzten 10 Jahren drastisch zugenommen und stellt aufgrund der daraus resultierenden vielfältigen Folgen wie Altersarmut, Depressionen, soziale Isolation, psychische und physische Folgen eine ernsthafte Bedrohung für die Gesellschaft dar.
6. **Die Nutzung des etablierten Finanzsystems ist** für die Cyberkriminellen unabdingbar. Neben ausgefeilten Software-Tools, aggressivem Marketing, betrügerischen Affiliate-Kampagnen und skrupellosen Call-Center-Mitarbeitern ist der kritische Erfolgsfaktor für diese Art von Finanzkriminalität die Zusammenarbeit mit dem etablierten Finanzsystem, die erforderlich ist, um an die gestohlenen Gelder zu gelangen.
7. Die Nutzung des etablierten Finanzsystems ist unerlässlich, um das Geld der Opfer entgegennehmen zu können, es zu waschen und es letztendlich auf Bankkonten unter der direkten Kontrolle der TCOs transferieren zu können.
8. Ohne den Erhalt der illegalen Erträge, die zur Finanzierung der kriminellen Aktivitäten unabdingbar sind, ist das Lebenselixier der kriminellen Organisationen nicht aufrechtzuerhalten.
9. Als Gatekeeper für das Finanzsystem spielen Banken eine immens wichtige Rolle im kollektiven Kampf gegen Finanz- und Wirtschaftskriminalität.
10. Durch die Anwendung einer angemessenen Sorgfaltspflicht gegenüber Kunden sind Banken verpflichtet, die Nutzung des Finanzsystem durch kriminelle Aktivitäten, für die Sicherheit ihrer Kunden und der Gesellschaft aufzudecken und zu verhindern.
11. Banken sind die erste Verteidigungslinie gegen Geldwäscher und andere kriminelle Organisationen, die das globale Finanzsystem nutzen wollen, um ihre kriminellen Aktivitäten voranzutreiben.
12. Banken sind verantwortlich dafür, die in ihren Finanzsystemen verarbeiteten Transaktionen mit angemessener Sorgfalt zu überwachen, die Herkunft der Gelder zu ermitteln und damit die Unterstützung kriminellen Aktivitäten zu verhindern.

Zahlungen an die HSBC

13. EFRI vertritt 145 (63+82) europäische Kleinanleger, die mehr als 13,7 Millionen EUR ihrer Lebensersparnisse (1,9+11,5+1,3) an HSBC [5] Bankkonten krimineller Organisationen überwiesen haben.

[4] https://www.fca.org.uk/publication/research/quan-study-understanding-victims-investment-fraud.pdf

[5] Die Hang Seng Bank ist ein Hauptmitglied der HSBC-Gruppe und die HSBC-Geschäftsführung ist Teil des Verwaltungsrats der Hang Seng Bank (Quelle: Hang Seng Bank Jahresbericht 2019). Die HSBC-Gruppe besitzt 62,14 % der Hang Seng Bank (Quelle: Yahoo Finance, Wikipedia).

14. 63 Opfer des von Russen betriebenen Blue Trading Betrugssystems (auch als "Blue Trading Fraud" bezeichnet) haben 1,9 Mio. EUR auf das Konto der Firma Vilardes Group Ltd, 62-76 Park Street, London SE1 9DZ (GB10HBUK40127882816886, HBUKGB4BXXX), bei der HSBC PLC UK im Zeitraum von Februar 2018 bis Februar 2019 überwiesen (siehe **Anlage A1** für Details zu den beteiligten Opfern und dem überwiesenen Geld).
15. 82 Opfer[6] verloren ihr Geld durch einen von Briten in Südostasien betriebenen Boilerroom scam (auch als "Investment Scam Asia" (ISA) Fraud-System bezeichnet). 30 dieser Opfer haben von Juli 2017 bis März 2020 10,5 Millionen Euro auf 33 verschiedene HSBC Hong Kong Bankkonten von Zweckgesellschaften überwiesen, die als illegale Zahlungsdienstleister (Money Mules) fungierten. Zusätzliche 1,3 Mio. Euro wurden von 5 Opfern zwischen November 2017 und November 2018 auf 6 Konten der Hang Seng Bank überwiesen.
16. Die Einzelheiten der Überweisungen der europäischen Opfer auf Bankkonten der HSBC Hong Kong und Hang Seng Bank sind in **Anlage A2** (A2_a: Überweisungen an HSBC; A2_b: Überweisungen an die Hang Seng Bank) dargestellt.

Der Blue Trading Betrug

17. Der Blue Trading Forex und Crypto Investment Betrug wurde über einen Zeitraum von 2,5 Jahren von Januar 2017 bis April 2019 betrieben und hat mehrere tausend europäische Verbraucher um geschätzte 165 Mio. EUR betrogen. Ein globales Netzwerk von Briefkastenfirmen ausgestattet mit Bankkonten bei internationalen Großbanken wie der Deutschen Bank, und der HSBC wurde genutzt um das gestohlene Geld entgegenzunehmen, zu waschen und an die Betrüger weiterzuleiten. Ermittlungsverfahren zu diesem Betrugssystem laufen in mehreren Ländern.

[6] Der Schaden der 82 Opfer beträgt über 20 Millionen EUR.

Der ISA-Betrug

18. Angeblich sehr erfahrene Broker, die vorgeben, aus New York oder London anzurufen,[7] überzeugen gutgläubige vermögende europäische Privatanleger, materielle Geldbeträge an ausschließlich asiatische Banken (vor allem die HSBC HK) bestimmt für Investitionen in Hongkonger Technologieunternehmen zur Anweisung zu bringen.

19. In Hongkong ansässige Technologieunternehmen werden als Investitionsmöglichkeiten in die vielversprechende asiatischen High-Tech-Wirtschaft beworben.

20. Sogenannte (Trading) Unternehmen (in der Folge „Tradinggesellschaften“) – reine Briefkastenfirmen – die ausschließlich für die Vereinnahmung des Geldes von den europäischen Opfern gegründet und verwendet werden – weisen dabei folgende Merkmale auf:

    - Die meisten dieser Tradinggesellschaften wurden kurz vor Nutzung durch das Betrugssystem, neu gegründet, die Gründung sowie der Registrierungsprozess erfolgt durch Hong Kong Company Builders (TCSPs).
    - Alle Trading- sowie "vielversprechenden" Technologieunternehmen haben ihren Sitz in den Büros des Hongkonger Company Builders.
    - Die registrierten Geschäftsführer und wirtschaftlichen Eigentümer sind Festlandchinesen ohne Wohnsitz in Hongkong – wir haben erfahren, dass Festlandchinesen, die ihre Identität verkaufen, kontinuierlich von Hongkonger Company Buildern rekrutiert werden.
    - Alle diese Handelsunternehmen und vielversprechenden Technologieunternehmen haben keine Mitarbeiter und keine Historie.
    - Ihr Geschäftszweck, wie er im Handelsregister von Hongkong eingetragen ist, stimmt nicht mit den tatsächlichen Aktivitäten dieser Handelsgesellschaften überein, die ausschließlich als illegale Zahlungsdienstleister agieren.
    - Die Betrüger benutzen hochprofessionelle Marketingmaterialien, um Investoren anzuwerben **(Anlage A3:** Prospekt der Zijing Mining Corp HKEX: 2899, die von einer betrügerischen Brokerfirma namens Osaka Matsui Management gesendet wurden) um ihre Pre-IPO-Unternehmen auf renommierten Finanzplattformen wie Bloomberg, Yahoo Finance, Crunchbase, Finanznachrichten.de usw. und gefälschten Websites wie www.asianewswire.com zu bewerben (beispielhafte Links: DigitalPay1; DigitalPay2; Autotech HK, AutoTech HK CB). Weitere Details zu den zahlreichen Fake News finden sich in den **Anlagen A4 und A5.**
    - Über einen Zeitraum von Monaten werden die ahnungslosen europäischen Kleinanleger dazu überredet, ihre Lebensersparnisse auf verschiedene asiatische Bankkonten – hauptsächlich HSBC-Bankkonten – zu überweisen, bevor sich herausstellt, dass alle Versprechungen und hochprofessionell erscheinenden Dokumente nur gefälscht sind und die Anlageberater nicht mehr telefonisch oder per E-Mail erreichbar sind.

21. Die transnationalen kriminellen Organisationen haben in Asien ausgeklügelte Betrugsnetzwerke entwickelt, welche ihre Epi-Center in Hongkong haben. Um den Betrug auszuführen, werden die folgenden Elemente verwendet und synchronisiert:

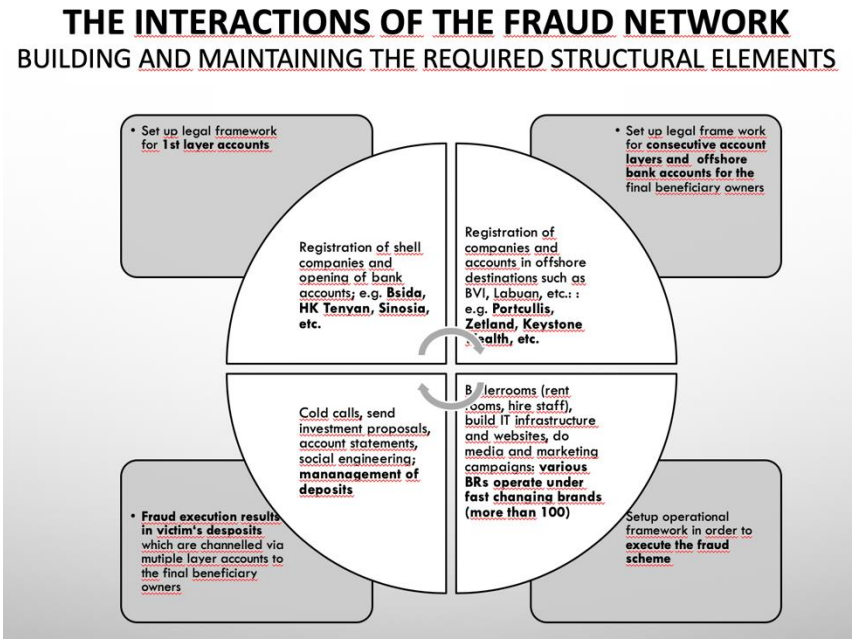
[7] Die erfahrenen Broker entpuppen sich später als mehrsprachige Typen, die betrügerische Marketingmethoden anwenden und mit Hunderten anderer Betrüger neben ihnen in Callcentern in Malaysia und / oder den Philippinen sitzen.

a. Einrichten einer 1. Schicht von Bankkonten, um die Einzahlungen der Opfer entgegenzunehmen.

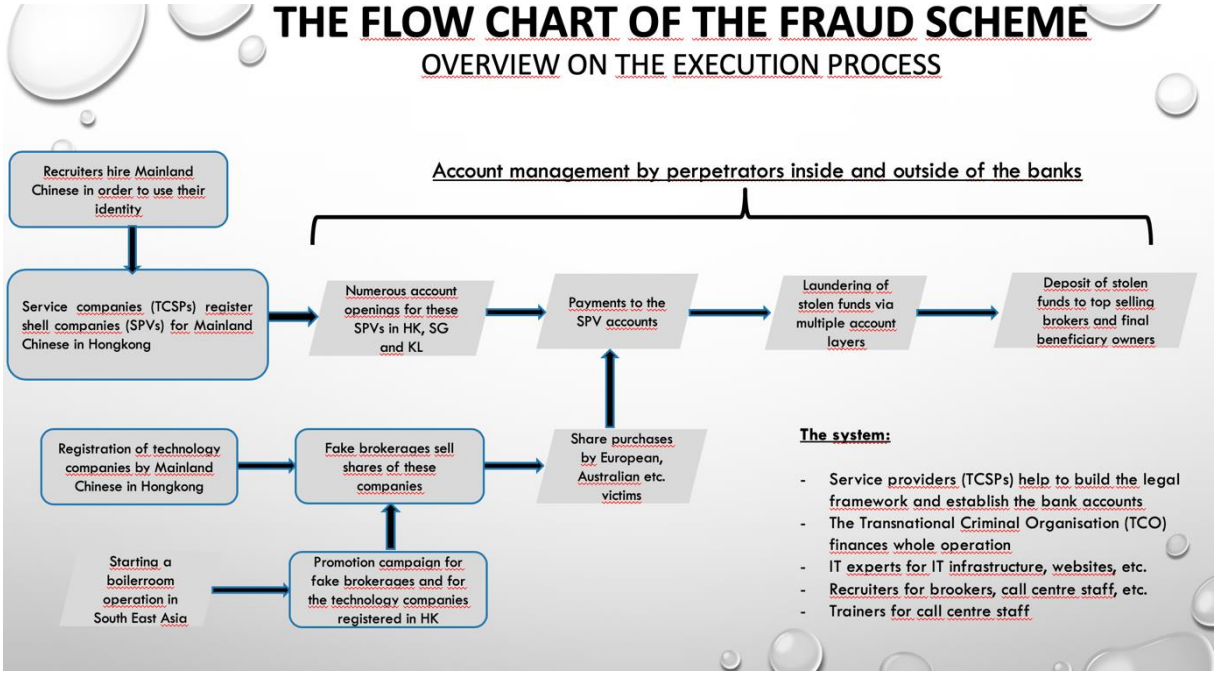
b. Einrichtung von Konten der 2. Schicht und der aufeinanderfolgenden Schichten einschließlich der juristischen Personen, um das gestohlene Geld zu waschen.

c. Einrichten der operativen Ebene, um den Betrug auszuführen. Die operative Ebene erfordert unter anderem Boilerroom - Mitarbeiter, IT-Infrastruktur sowie Medien und Marketing.

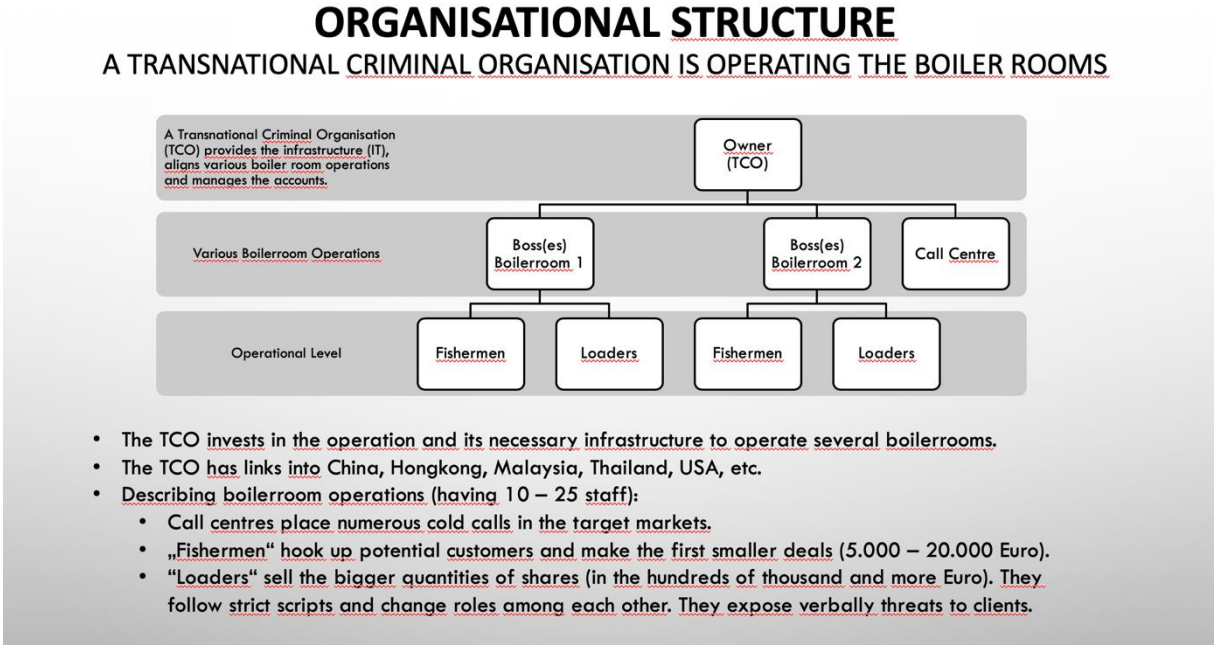
Das folgende Bild zeigt das Zusammenspiel der verschiedenen Elemente und Aktivitäten.



Der Workflow des Betrugs kann wie folgt dargestellt werden:



Das folgende Bild zeigt die Organisationsstruktur des ISA-Investitionsbetrugsschemas.



Weitere Informationen zum Betrugsschema finden Sie in den **Anlagen A6 und A7**.

22. Für den ISA-Betrug gelten folgende[8] Kennziffern:
    a. Mindestens 114 Briefkastenfirmen waren in Hongkong registriert.
    b. Für diese Briefkastenfirmen wurden mindestens 111 aktive Bankkonten eröffnet. Von diesen aktiven Bankkonten wurden 78 aktive Bankkonten in Hongkong und 33 Bankkonten in anderen asiatischen Jurisdiktionen eröffnet.
    c. Mindestens 14 "Technologieunternehmen" alle in Hongkong registriert sind, wurden verwendet.
    d. Mindestens 23 verschiedene Banken wurden genutzt, von denen sich 12 Banken in Hongkong befinden.
    e. Der Gesamtschaden der 82 ISA-Opfer beträgt rund 22 Mio. Euro.
23. Da diese Art von Boilerroom scam seit 2015 oder früher aktiv ist (siehe zum Beispiel Presse- und Medienveröffentlichungen, P1: SCMP_2015 oder P2: Reddit), muss es Tausende von europäischen Opfern geben, die ähnliche außergewöhnliche Verluste erlitten haben, die sich auf mehrere hundert Millionen Euro anhäufen.
24. Alle betrogenen 82 europäischen ISA-Kleinanleger reichten in ihren jeweiligen EU-Ländern Strafanzeigen wegen Anlagebetrugs und anderer Straftaten ein und haben Strafanzeige bei der Hongkonger Polizei (im Zeitraum von Oktober 2020 bis heute) gestellt. Siehe **A8_a, A8_b und A8_c Anlagen.** Das Commercial Crime Bureau (CCB) in Hongkong führt seit Mitte Oktober 2020 eine Untersuchung unter der Referenznummer "CCB RN 20001893" durch.

Die Beteiligung von HSBC an dem Betrug

25. HSBC Holdings PLC ist eine britische multinationale Konzern- und Finanzdienstleistungsholding. Sie ist die zweitgrößte Bank Europas.
26. Laut Informationen, die auf der Website der HSBC veröffentlicht werden (https://www.hsbc.com/who-we-are), verpflichtet sich die HSBC (alle vollständig im Besitz oder unter der Kontrolle der HSBC PLC stehenden HSBC Tochterunternehmen) zur Umsetzung einheitlicher globaler Standards, die von den effektivsten Anti-Geldwäsche-Standards geprägt sind.
27. Dementsprechend hat die HSBC (laut ihrer Veröffentlichungen) ein globales Programm zur Bekämpfung der Geldwäsche ("AML-Programm") eingerichtet. Ziel des AML-Programms ist es, sicherzustellen, dass die von HSBC identifizierten Geldwäscherisiken angemessen adressiert werden. Dies wird durch die Festlegung von vom Vorstand genehmigten Richtlinien, Prinzipien und Standards und die Implementierung geeigneter Kontrollen erreicht, um die HSBC, ihre Mitarbeiter, Aktionäre und Kunden vor Geldwäsche zu schützen. Das AML-Programm bietet allen HSBC-Mitarbeitern eine Anleitung und verpflichtet sie, ihre Geschäfte in Übereinstimmung mit den geltenden AML-Gesetzen, -Regeln und -Vorschriften zu tätigen. (EU MLD6 Richtlinie, UK AML Regime 01/2020 usw.).
28. Gemäß den Veröffentlichungen der HSBC basiert das HSBC AML-Programm auf verschiedenen Gesetzen, Vorschriften und regulatorischen Leitlinien aus dem Vereinigten Königreich, der Europäischen Union, Hongkong, den Vereinigten Staaten von Amerika und gegebenenfalls lokalen

[8] Dies sind nur jene Zahlen, die wir aufgrund der Dokumentation der 82 Opfer kennen; basierend auf der offensichtlich sehr professionellen Art des TCO erwarten wir, dass die tatsächliche Anzahl der Briefkastenfirmen, Bankkonten und Opfer viel höher ist.

Gerichtsbarkeiten, in denen HSBC tätig ist. Laut der Website von HSBC umfasst das AML-Programm unter anderem:

- Die Ernennung eines Global and Country Money Laundering Reporting Officer ("MLRO") oder einer alternativen Position, wie von den lokalen Vorschriften gefordert.
- Ein Customer Due Diligence ("CDD") Programm, das die Grundsätze der Kundenidentifikation und -verifizierung ("ID&V") und der Kenntnis Ihres Kunden ("KYC") umfasst, sowie die Implementierung von Programmen zur angemessenen Korrektur der CDD bestehender Kunden.
- Durchführung einer verstärkten Due Diligence ("EDD") bei Kunden, die als höheres Risiko bewertet werden, wie z. B. politisch exponierte Personen ("PEPs") in leitenden Positionen, deren Angehörige und enger Mitarbeiter.
- Einrichtung von Prozessen und Systemen zur Überwachung von Kundentransaktionen zur Identifizierung verdächtiger Aktivitäten.
- Die Untersuchung und anschließende Meldung verdächtiger Aktivitäten an die zuständigen Aufsichtsbehörden.
- Vorgeschriebene regelmäßige unabhängige Tests und regelmäßige AML-Schulungen der Mitarbeiter und Auftragnehmer.
- Das Verbot der folgenden Produkte, Dienstleistungen und Kundentypen:
    - Anonyme Konten oder nummerierte Konten oder *Kunden, die* ein Konto unter *einem offensichtlich fiktiven Namen führen.*
    - Shell-Banken, d.h. Banken ohne physischen Präsenz oder Personal.
    - Hold Mail, d.h. wenn der Kunde angewiesen hat, dass alle Unterlagen im Zusammenhang mit dem Konto in seinem Namen bis zur Abholung aufbewahrt werden sollen.
    - Payable-Through-Accounts, d.h. HSBC erlaubt in- oder ausländischen Bankkunden nicht, ihren Kunden auf ihren HSBC-Konten Payable-Through Accounts zur Verfügung zu stellen; und
    - Alle relevanten zusätzlichen lokalen Anforderungen.

29. HSBC gibt auch stolz bekannt, Mitglied der Wolfsberg Group zu sein, einem Zusammenschluss von dreizehn globalen Banken, der sich zum Ziel gesetzt hat, Standards für die Finanzdienstleistungsbranche für KYC, AML und Terrorismusfinanzierung zu entwickeln.

30. Ungeachtet des Anspruchs von HSBC, modernste Compliance-Programme implementiert und einzuhalten, haben die Bank und ihre Tochtergesellschaften seit dem Jahr 2000 über 6,5 Milliarden US-Dollar an zivilrechtlichen Strafen gezahlt, insgesamt wurden 59 Verstöße registriert (vergleiche **Anlage A9**).

31. Obwohl das HSBC-Management sich der Verwundbarkeit und Unzulänglichkeit der Compliance der Gruppe aufgrund der zahlreichen Compliance-Probleme bewusst sein muss, die in den früheren Jahren bereits verfolgt und bestraft wurden, täuscht HSBC weiterhin Dritte über die Fähigkeit der Compliance Maßnahmen des Konzerns, Kriminelle daran zu hindern, das Finanzsystem der HSBC zur Geldwäsche zu nutzen.

32. Insbesondere aufgrund der umfassenden Medienberichterstattung über den Missbrauch des Zahlungssystems der HSBC für diese Art von Investmentbetrug (wie unten[9] aufgeführt) in der Vergangenheit – verstärkt dadurch, dass London und Hongkong als internationale Finanzzentren bekannt sind für relativ einfache Unternehmensgründung und dem damit einhergehenden Betrug – muss die HSBC sich des hohen Risikos bewusst gewesen sein, dass ihr Banksystem von Betrügern benutzt werden, um Geld von unschuldigen europäischen Kleinanlegern zu stehlen.

33. Mehr als 110 Briefkastenfirmen (für fiktive Handelsgesellschaften; vgl. 23) in Hongkong, mit mehr als 110 Bankkonten, davon 78 in Hongkong, wurden im Zeitraum zwischen Juni 2013 und Februar 2021 gegründet (vgl. **Anlage A10),** davon **wurden mehr als 33 Bankkonten bei der HSBC HK eröffnet.**

34. Durch die Bereitstellung von Bankkonten für die Briefkastenfirmen der TCO war HSBC die Hauptbank für die beiden oben genannten Betrugsfälle.

35. Wir behaupten, dass die HSBC entweder vorsätzlich oder in Bezug auf die betrügerischen Aktivitäten in ihrem Unternehmen im Zusammenhang mit den beiden Betrugsschemata zumindest fahrlässig gehandelt hat.

36. Wir gehen davon aus, dass die HSBC sich selbst zum Komplizen beim Betrug Tausender ahnungsloser europäischer Kleinanleger gemacht hat.

37. HSBC hat es versäumt, ein Mindestmaß an Vorsicht oder Sorgfalt walten zu lassen, mit dem erschwerenden Faktor, dass das zugrunde liegende Betrugsmuster in Hongkong seit vielen Jahren bekannt ist (z. B. FATF Hong Kong 2019).

Das Muster der kriminellen Aktivitäten

38. HSBC ist seit mehreren Jahren und im Zusammenhang verschiedener Betrugsfälle diverser transnationaler krimineller Organisationen in diese Art von Betrug involviert. Folgende Beitragstathandlungen wurden identifiziert [10]:

    - Bereitstellung von Bankkonten für reine Briefkastenunternehmen (Trading Companies), auffallender Weise in spezifischer HSBC-Filialen in[11] Hongkong.

---

[9] P1: South China Morning Post berichtete 2015 über einen sogenannten "Boiler Room" -Betrug in Kombination mit Geldwäsche. Link: SCMP 2015
P3: South China Morning Post berichtete im August 2018, dass tausende von Betrugskonten in Hongkong existierten, die für Betrug verwendet wurden. Link: Hongkong Bank2
P4: Regulation Asia berichtete im Februar 2021, dass es in Hongkong auch im Jahr 2020 mehr als 10.000 Konten gab, die für Betrug verwendet wurden. Link: Vorschriften Asien
P5: Die South China Morning Post berichtete 2021, dass zum ersten Mal in der Geschichte Hongkongs Bankangestellte verhaftet wurden, weil sie bei der Einrichtung krimineller Konten geholfen hatten.

[10] Die Aktivitäten auf drei beispielhaften HSBC-Konten wurden überprüft. Das Ergebnis ist zusammengefasst in **Anlage A11**.

[11] Von den 550 HSBC-Filialen zeigen 33 Konten bei HSBC Hong Kong, dass:

- 13 Konten wurden unter der Filialnummer "023" ("Hennessy Centre") geführt.
- 8 Konten wurden unter der Filialnummer "741" ("Hong Kong Office Commercial Service Centre") geführt.

- Akzeptanz identischer Firmendokumente zahlreicher Mantelgesellschaften, im Rahmen der Onboarding Due Diligence bei der HSBC HK.
- Akzeptanz der Nutzung derselben Korrespondenzadresse in Shenzhen (Nachbarstadt Hongkong) durch zahlreiche Mantelgesellschaften, ohne dieses Problem im Onboarding-Prozess anzusprechen.
- Akzeptanz eines Wechsels der Geschäftsführung der Mantelgesellschaften unmittelbar nach dem[12]Onboarding. Viele dieser Mantelgesellschaften weisen nach dem erfolgreichen Onboarding Prozess dieselbe französische Person namens Caroline Virgine Valerie Tessier[13] als Geschäftsführerin aus.
- Tägliche stattfindende betragsmäßig sehr hohe Überweisungen aus dem EU-Raum, Auszahlungen die kurz danach, oft mehrmals innerhalb von 24 Stunden nach der Einzahlung, [14] (vergleiche **Anhang A13** Kontobewegungen auf dem Konto von #023 727423 838 (Duplex (HK) Trade Limited für den Zeitraum vom 5. Juni 2019 bis zum 21. Juni 2019) stattfinden, werden ohne Einspruch der Bank akzeptiert. Weder die Höhe der überwiesenen Beträge noch die Häufigkeit der Überweisungen passen zu den Angaben über die während des Onboardings angegebenen und von der HSBC festgestellten Geschäftstätigkeit.
- Annahme hoher internationaler eingehender und ausgehender Fremdwährungsbeträgen (Einzelüberweisungen über 100.000, - EUR), obwohl während des Kunden-Due-Diligence-Prozesses nur chinesische Handelsverträge mit Beträgen unter 10.000 Euro (in chinesischer Währung) vorgelegt wurden.
- Konten mit einem viel höheren als die beim Onboarding Prozess angekündigten Tages-, Wochen- und/oder Monatsumsatz führen offensichtlich nicht zu Warnungen innerhalb der Bank.
- Akzeptieren, dass identische IP-Adressen für die Durchführung von Online-Banking-Überweisungen verschiedener HSBC-Konten verwendet werden, die jeweils unterschiedliche wirtschaftliche Eigentümer aufweisen.

- 6 Konten unter der Filialnummer "582" ("Sun Hung Kai Centre")
- 2 Konten in der Filiale "747" ("Cheung Sha Wan Commercial Service Center")
- 2 Konten in der Filiale "038" ("Shatin Centre")
- Je ein Konto in den Filialen "024", "801" und "817".

[12] Das **Anlage A12** zeigt als Beispiel die Registrierung von Duplex (HK) Trade Limited auf der 27heit vom Dezember 2018 (erste Reihe) im Namen einer chinesischen Person Wang Hong Biao. Auf der 6heit im März 2019 trat dieser Chinese zurück, und eine neue Geschäftsführerin namens Frau Tessier, angeblich eine französische Staatsangehörige, wurde ernannt (zweite Reihe). Der Zweck dieses Wechsels in der Geschäftsführung bestand offensichtlich darin, die volle Kontrolle über das Bankkonto von Duplex (HK) Trade Limited zu haben und jede weitere Anfrage zu verschleiern.

[13] Frau Caroline Virgine Valerie Tessier ist als Geschäftsführerin von 91 registrierten Unternehmen registriert, von denen 5 Unternehmen in die betrügerischen Handelsunternehmen fallen, die an diesem Betrugssystem beteiligt sind (HK Maccard, HK Emay, HK Duplex, HK Yokeda, Yasenda (HK) Co. Ltd., die alle Konten bei HSBC halten.

[14] Basierend auf geprüften Unterlagen für drei HSBC HK-Konten (HK mit #741 147909 838 (Macchard Trade Limited), # 023 727316 838 (HK Emay Trade Limited); # 023 727423 838 (Duplex (HK) Trade Limited)

- Irreführende Auskünfte [15] an europäische Kleinanleger auf Anfrage über verdächtige Transaktionen, sobald der Betrug offensichtlich war.
- Andere fragwürdige Vorfälle vgl. **Anlage A14**

39. Zusammenfassend lässt sich sagen, dass obwohl es genügend Warnsignale gegeben hat, die HSBC nicht angemessen reagiert hat.

Grober Verstoß gegen AML/TF-Gesetz und EBA-Richtlinien

40. Gemäß Artikel 13 Absatz 1 der EU-Richtlinie 2015/849 für Verpflichtete ist CDD (Customer Due Diligence) sowohl für die Risikobewertung als auch für das Risikomanagement von zentraler Bedeutung.

41. Gemäß der EU-Richtlinie 2015/849 umfasst der Customer Due Diligence Prozess folgende Maßnahmen:
    • Identifizierung des Kunden und Überprüfung der Identität des Kunden auf der Grundlage von Dokumenten, Daten oder Informationen, die aus einer zuverlässigen und unabhängigen Quelle stammen;
    • Identifizierung des wirtschaftlichen Eigentümers des Kunden und Ergreifen angemessener Maßnahmen zur Überprüfung seiner Identität, damit der Verpflichtete davon überzeugt ist, dass er weiß, wer der wirtschaftliche Eigentümer ist.
    • Bewertung und gegebenenfalls Einholung von Informationen über den Zweck und die beabsichtigte Art der Geschäftsbeziehung.
    • Laufende Überwachung der Geschäftsbeziehung. Dazu gehört die Transaktionsüberwachung und die Aktualität der zugrunde liegenden Informationen.

42. Die EU-Richtlinie 2015/849 sieht vor, dass Verpflichtete den Umfang dieser Maßnahmen risikosensitiv bestimmen können. Diese Richtlinie sieht auch [16]vor, dass wenn das mit der Geschäftsbeziehung oder gelegentlichen Transaktion verbundene Risiko als gering eingestuft wird, die Mitgliedstaaten den Verpflichteten gestatten können, stattdessen vereinfachte Sorgfaltspflichten gegenüber Kunden (SDD) anzuwenden. Umgekehrt

[15] **Anlage A15** (Dokumente zu drei HSBC-Konten, auf Verlangen zu liefern) und Anlage 14, ab Seite 15: Herr Kroesser, ein deutsches Opfer, überwies am 5. Juni 2019 16.890 Euro auf das Konto 023 727316 838 von HK Emay, die gleiche Überweisung wurde ihm am 21. Juni 2019 mit Abzug der Gebühren zurückerstattet. Bemerkenswerterweise wurde das Konto von HK Emay im April und Mai 2019 ausgiebig genutzt, um zahlreiche Auslandseinlagen zu erhalten, aber es existierte auch im Juni 2019 (siehe Kontoauszüge von HK Emay vom 29. Juni 2019). Während des Klärungsprozesses beschreibt sich HSBC in der offiziellen Antwort an das Opfer vom 5. Februar 2021 als ".... empfangende Bank, die verpflichtet ist, die Zahlungsanweisungen auf der Grundlage der erhaltenen Anweisung zu bearbeiten…". In ihrer weiteren Antwort an den geschädigten Investor vom 20. April 2021 bestreitet die HSBC sogar jegliche Kenntnis dieses konkreten Vorfalls. In Anbetracht der Tatsache, dass das HK Emay-Konto im Juni 2019 und sogar bis Juni 2020 noch existierte, hätte HSBC HK die Überweisung von Herrn Kroesser nach eigener Definition ausführen müssen. Aus unbekannten Gründen wollten die Betrüger seit Anfang Juni 2019 keine Einzahlungen mehr auf das HK Emay-Konto erhalten und beeinflussten offensichtlich HSBC HK, die Überweisung von Herrn Kroesser abzulehnen.

[16] Im Einklang mit den Standards der FATF stellt die Richtlinie (EU) 2015/849 den risikobasierten Ansatz in den Mittelpunkt des AML/CFT-Regimes der Europäischen Union. Er erkennt an, dass wenn das Risiko von ML/TF unterschiedlich sein kann, die Verpflichteten müssen Maßnahmen ergreifen, um dieses Risiko zu identifizieren und zu bewerten, um zu entscheiden, wie es am besten bewältigt werden kann.

müssen die Verpflichteten, wenn das mit der Geschäftsbeziehung oder gelegentlichen Transaktion verbundene Risiko erhöht ist, verstärkte Sorgfaltspflichten gegenüber Kunden (EDD) anwenden.

43. Die Richtlinie legt jedoch nicht im Einzelnen fest, wie die Verpflichteten das mit einer Geschäftsbeziehung oder Transaktion verbundene Risiko bewerten sollten, und legt auch nicht genau fest, was SDD- und EDD-Maßnahmen mit sich bringen.

44. Am 4. Januar 2018 veröffentlichte die ESA gemeinsame Leitlinien gemäß Artikel 17 und Artikel 18 Absatz 4 der EU-Richtlinie 2015/849 [17] über vereinfachte und verbesserte Sorgfaltspflichten gegenüber Kunden und die Faktoren, die Kredit- und Finanzinstitute bei der Bewertung des Geldwäsche- und Terrorismusfinanzierungsrisikos im Zusammenhang mit einzelnen Geschäftsbeziehungen und gelegentlichen Transaktionen berücksichtigen sollten (Leitlinien zu Risikofaktoren).

45. Diese Richtlinien galten ab dem 26. Juni 2018. Gemäß Artikel 16 Absatz 3 der ESA-Verordnungen müssen die zuständigen Behörden und Finanzinstitute alle Anstrengungen unternehmen, um die Leitlinien einzuhalten.

46. HSBC behauptet auf ihren Websites und in der Geschäftsführung, alle diese Regeln einzuhalten (vgl. 28).

47. Offensichtlich ist jedoch der Ansatz der HSBC zur Bewertung und Steuerung des ML/TF-Risikos im Zusammenhang mit Geschäftsbeziehungen und gelegentlichen Transaktionen, wie in den gemeinsamen Leitlinien der ESA und allen anderen anwendbaren regulatorischen Vorschriften gefordert, nicht gelungen:

- Es findet offensichtlich keine angemessene unternehmensweite Risikobewertung statt. Die HSBC müsste nach diesen Bestimmungen der ESA mit ihrem internationalen Engagement und Betrieb an internationalen Finanzzentren (z. B. London und Hongkong), die für die einfache Registrierung von Briefkastenfirmen bekannt sind - eindeutig eine erweiterte Risikobewertung bei Kontoeröffnung durchführen.
- Kein angemessenes CDD-Niveau: die HSBC ist verpflichtet die Ergebnisse ihrer unternehmensweiten Risikobewertung zu nutzen, um eine fundierte Entscheidung über die

[17] Am 26. Juni 2015 trat die Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche oder der Terrorismusfinanzierung in Kraft. Mit dieser Richtlinie sollen unter anderem die Rechtsvorschriften der Europäischen Union mit den internationalen Standards zur Bekämpfung der Geldwäsche und der Finanzierung des Terrorismus und der Verbreitung in Einklang bringen, die die Financial Action Task Force (FATF), ein internationaler Standardsetzer zur Bekämpfung der Geldwäsche, 2012 angenommen hat. Im Einklang mit den Standards der FATF stellt die Richtlinie (EU) 2015/849 den risikobasierten Ansatz in den Mittelpunkt des Regimes der Europäischen Union zur Bekämpfung der Geldwäsche (AML) und der Terrorismusfinanzierung (CFT). Er erkennt an, dass das Risiko von Geldwäsche und Terrorismusfinanzierung (ML/TF) unterschiedlich sein kann und dass die Mitgliedstaaten, die zuständigen Behörden sowie die in ihren Anwendungsbereich fallenden Kredit- und Finanzinstitute (im Folgenden "Unternehmen") Maßnahmen ergreifen müssen, um dieses Risiko zu ermitteln und zu bewerten, um zu entscheiden, wie es am besten bewältigt werden kann. Gemäß Artikel 17 und Artikel 18 Absatz 4 der Richtlinie (EU) 2015/849 müssen die Europäischen Aufsichtsbehörden Leitlinien herausgeben, um Unternehmen bei dieser Aufgabe zu unterstützen und die zuständigen Behörden bei der Bewertung der Angemessenheit der Anwendung vereinfachter und verbesserter Sorgfaltspflichten gegenüber Kunden durch Unternehmen zu unterstützen. Ziel ist es, die Entwicklung eines gemeinsamen Verständnisses zwischen Unternehmen und zuständigen Behörden in der gesamten EU darüber zu fördern, was der risikobasierte Ansatz für AML/CFT beinhaltet und wie er angewendet werden sollte.

geeignete Ebene und Art der CDD zu treffen, die sie auf einzelne Geschäftsbeziehungen und gelegentliche Transaktionen anwenden muss.

- Keine ganzheitliche Sichtweise: HSBC muss genügend Informationen sammeln, um überzeugt zu sein, alle relevanten Risikofaktoren identifiziert zu haben, gegebenenfalls einschließlich der Anwendung zusätzlicher CDD-Maßnahmen, und diese Risikofaktoren zu bewerten, um eine ganzheitliche Sicht auf das mit einer bestimmten Geschäftsbeziehung verbundene Risiko zu erhalten.
- Eine permanente Überwachung und Überprüfung der Geschäftsbeziehungen findet nicht statt. Durch die ständige Überwachung der Transaktionen soll sichergestellt werden, dass sie mit dem Risikoprofil und dem - bekanntgegebenen - Geschäft des Kunden in Einklang stehen. Ebenso muss die Herkunft der Mittel überprüft werden, um mögliche ML/ TF zu erkennen. HSBC muss auch die Dokumente, Daten oder Informationen, die sie besitzt, auf dem neuesten Stand halten, um zu verstehen, ob sich das mit der Geschäftsbeziehung verbundene Risiko geändert hat.

Nichtanwendung von EDD für die Briefkastenfirmen mit ungewöhnlichen Transaktionen:

47. Gemäß Artikel 18 Absatz 2 der EU-Richtlinie 2015/849 muss die HSBC angemessene Richtlinien und Verfahren zur Erkennung ungewöhnlicher Transaktionen oder Transaktionsmuster festlegen.

    Wobei ungewöhnliche Transaktionen wie folgt definiert sind:

    - Betragsmäßig höhere Transaktionen als im Onboarding festgelegt.
    - Transaktionen, die nicht in das beim Onboarding festgelegte Schema über Kundenstruktur und Art der Geschäftsbeziehung passen.
    - Transaktionen mit einem ungewöhnlichen oder unerwarteten Muster im Vergleich zum erwarteten Muster des Kunden und zum Muster bei vergleichbaren Kunden mit entsprechenden Produkten und/oder Dienstleistungen;
    - Komplexere Transaktionen wieder im Vergleich zu ähnlichen Kundentypen, Produkten oder Dienstleistungen, ohne dass es dafür eine entsprechende wirtschaftliche Begründung gibt.

48. Daher wäre die HSBC gemäß den gemeinsamen Leitlinien verpflichtet gewesen, folgende EDD-Maßnahmen anzuwenden:

    - Überprüfung der aus dem Rahmen fallenden Transaktionen eines Kunden durch Verlangen zusätzlicher Dokumentation für die einzelne Transaktion
    - Feststellung des wirtschaftlichen Zwecks der einzelnen Transaktion z.B. durch Ermittlung der Quelle und des Ziels
    - Nachforschung über die tatsächliche Geschäftstätigkeit des Kunden
    - Vermehrte Überwachung der Geschäftsbeziehung und der nachfolgender Transaktionen
    - Verstärktes Monitoring einer Kundenbeziehung und Erhöhung der Risikoeinschätzung.

Nichtbeachtung erhöhter Kundenrisikoanforderungen gemäß den Gemeinsamen Leitlinien.

Kapitel 2: Sektorale Leitlinien für Privatkundenbanken

49. Gemäß Kapitel 2 der gemeinsamen Leitlinien müssen Privatkundenbanken, die Girokonten anbieten, erhöhte Kundenrisikofaktoren berücksichtigen (die wiederum EDD-Maßnahmen erfordern), wenn die folgenden Kriterien erfüllt sind:

- ein ungewöhnlich hohes Umsatzvolumen oder einen ungewöhnlich hohen Wert bei den Transaktionen (98).
- **Der Kunde ist ein neues Unternehmen ohne Historie (100 v).**
- Die Geschäftsführung des Unternehmens ist nicht im Land der Bank ansässig (100 vi).
- Das Verhalten oder das Transaktionsvolumen des Kunden entspricht nicht dem, was von der Kundenkategorie, zu der er gehört, erwartet wird, oder entspricht nicht den Informationen, die der Kunde bei der Kontoeröffnung angegeben hat (100 iii).

ZUSAMMENFASSUNG

50. HSBC unterstützte die transnationalen kriminellen Organisationen dabei, die Kontrolle über die gestohlenen Gelder zu erhalten. Die Verwendung von HSBC-Bankkonten war für die Entgegennahme des Geldes der Opfer, für das Waschen des Geldes und schließlich für die Überweisung der Gelder auf Bankkonten unter der direkten Kontrolle der Betrüger unerlässlich.

51. HSBC ermöglicht es den kriminellen Organisationen, Gelder von unschuldigen europäischen Kleinanlegern einzuwerben.

52. Die Mitglieder der kriminellen Vereinigung übernehmen spezifische Rollen beim Raub der Lebensersparnisse der europäischen Investoren. Die Rolle von HSBC bestand darin, den kriminellen Organisationen Zugang zum etablierten Finanzsystem zu gewähren. Dabei hatte die HSBC entweder Kenntnis über die illegale Inanspruchnahme ihrer Dienste oder hat grob fahrlässig gehandelt.

53. Unabhängig von der spezifischen Entität, die eine Rolle spielte, waren die Rollen klar definiert, etabliert und von den Mitgliedern der kriminellen Organisation akzeptiert. Jeder Beitrag war unerlässlich, um die Lebensersparnisse der europäischen Investoren zu stehlen.

54. Wir sind davon überzeugt, dass die HSBC-Gruppe das AML-Programm der Gruppe vorsätzlich nicht angewandt hat und daher auch die Bedingungen der bedingten Strafverfolgungsvereinbarungen der US-Behörden vom 12. Dezember 2012 nicht erfüllt hat. Die HSBC war gemäß den Bestimmungen der US-Behörden verpflichtet, erweiterte AML- und andere Compliance-Verpflichtungen innerhalb ihrer gesamten globalen Geschäftstätigkeit anzuwenden. Dies, um eine Wiederholung des Verhaltens zu verhindern, das zur strafrechtlichen Verfolgung von HSBC führte, nachdem es die Geldwäsche von Millionen von Drogengeldern aus dem Jahr 2012 ermöglichte.

55. Trotz der Hinweise auf bestehende Geldwäscherisiken im Zusammenhang mit Geschäften in Hongkong und London hat HSBC es versäumt, ernsthafte Maßnahmen zu ergreifen, um zu vermeiden, dass sie für Anlagebetrugsaktivitäten missbraucht werden.

56. **Wie in den gemeinsamen Leitlinien der ESA in[18] Abschnitt 62 dargelegt, darf die HSBC keine Geschäftsbeziehung eingehen, wenn sie nicht in der Lage ist, ihre CDD-Anforderungen zu erfüllen, und damit sich nicht ausreichend davon überzeugen kann, dass der Zweck und die Art einer Kundenbeziehung legitim ist oder wenn sie nicht davon überzeugt sind, dass sie das Risiko, dass ihre Konten für ML/TF-Zwecke verwendet werden, wirksam managen kann.**

Erhobene Vorwürfe

57. Wir werfen der HSBC-Gruppe vor, sich zu Komplizen von Anlagebetrügern gemacht zu haben, die zu größeren kriminellen Organisationen (russisch und asiatisch) gehören, indem sie gegen ihre Anti-Geldwäsche-Richtlinie der Unternehmensgruppe verstoßen hat.

58. Es ist davon auszugehen, dass HSBC durch die Vernachlässigung beruflicher Pflichten einen sittenwidrigen Schaden für europäische Kleinanleger vorsätzlich hingenommen hat.

[18] https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1890686/66ec16d9-0c02-428b-a294ad1e3d659e70/Final%20Richtlinien%20on%20Risk%20Faktoren%20%28JC%202017%2037%29.pdf?retry=1

59. Darüber hinaus sind die zugrunde liegenden Muster, die Betrug in Hongkong ermöglichen, in Fach- und Regulierungskreisen allgemein bekannt (wie unter anderem im FATF Mutual Evaluation Report of Hong Kong, China 2019 erwähnt).

60. Das eklatante Versäumnis von HSBC, angemessene Kontrollen zur Bekämpfung der Geldwäsche einzuführen und ein angemessenes risikobasiertes Compliance-Programm anzuwenden, erleichterte die Geldwäsche von Hunderten von Millionen gestohlener Gelder von ahnungslosen europäischen Kleinanlegern.

61. Die offensichtlichen Mängel des Compliance-Programms von HSBC – einschließlich der Anwendung entsprechender Screening-, Test-, Audit- und Transaktionsprüfungsverfahren – ermöglichten es kriminellen Organisationen, Millionen, wenn nicht Hunderte von Millionen von unschuldigen europäischen Verbrauchern zu stehlen und zu waschen.

62. HSBC wusste oder muss gewusst haben, dass die Organisationsstrukturen der HSBC-Gruppe nicht den erforderlichen gesetzlichen Bestimmungen entsprachen und dass das Risiko eines Missbrauchs des Finanzsystems durch kriminelle Organisationen hoch war. Dies hat in den letzten Jahren den Diebstahl von Hunderten von Millionen lebenslanger Ersparnisse von europäischen Kleinanlegern ermöglicht.

63. Daher ist das Ausmaß der offensichtlichen groben Fahrlässigkeit bei der Durchführung bestehender KYC-Sorgfaltspflichten, Überwachungspflichten und Meldepflichten auf einen vorsätzlichen Verstoß gegen internationale Vorschriften und eine vorsätzliche Schädigung europäischer Kleinanleger zurückzuführen.

64. Es ist daher davon auszugehen, dass das Handeln von HSBC, nämlich die bewusste Vernachlässigung eines gesetzlich vorgeschriebenen adäquaten Aufbaus eines Risikomanagementsystems und anderer Organisationseinheiten zur Verhinderung von Geldwäsche, durch reines wirtschaftliches Eigeninteresse motiviert war, um sich einen Wettbewerbsvorteil zu verschaffen.

Mit freundlichen Grüßen

Elfriede Sixt Nigel Kimberly

Diese Beschwerde wird auch eingereicht bei:

Die Hong Kong Monetary Authority
55th Floor
Two International Finance Centre
8 Finance Street
Central
Hong Kong
Tel.: (+852) 2878 8196
E-Mail: ETR@hkma.gov.hk

Die Hongkong Police Force
Herr FONG Hon-ho, Terry
Detective Inspector of Police Fraud Section 10C
Commercial Crime Bureau
Hong Kong Police
Tel: (+852) 2860 4745
E-Mail: terryhhfong@police.gov.hk; ip-sip-fs-10c-b-div-ccb@police.gov.hk;
sgt-fs-10c-b-div-ccb@police.gov.hk
Reference Number: CCB RN 20001893

Die Financial Conduct Authority (UK)
Herr Hassan Kamara
Supervisor / Supervision Hub
Referenznummer: 207629700 (Herr Jan Hektor)
12 Endeavour Platz
London E20 1JN.
Tel.: +44 (0)800 111 6768
E-Mail: firm.queries@fca.org.uk, consumer.queries@fca.org.uk

Bundesamt für Justiz (Schweiz)
Frau Lara Kübler
Referenznummer: B21 – 1826 -1 (Herr Guido Weber)
Bundesrain 20
3003 Bern
Schweizerisch
Tel.: +41 58 464 0038
E-Mail: lara.kuebler@bj.admin.ch

Diese Beschwerde wird den folgenden Organisationen zur Kenntnis gebracht

Financial Action Task Force (FATF)
2, rue André Pascal
75775 Paris Cedex 16 FRANKREICH
Tel.: + 33 1 45 24 90 90
E-Mail: Contact@fatf-gafi.org

EUROPÄISCHE BANKENAUFSICHTSBEHÖRDE
Tour Europlaza20 avenue André ProthinCS 3015492927 Paris La Défense CEDEXFrance
Tel.: +33 1 86 52 70 00
E-Mail: info@eba.europa.eu

Europol
Eisenhowerlaan 73,
2517 KK Den Haag
Niederlande
Tel.: +31 70 302 5000

Bundesministerium der Justiz und für Verbraucherschutz (Deutschland)
Bundesministerium der Justiz und für Verbraucherschutz
Referat II B 5
Mohrenstr. 37
10117 Berlin
Deutschland
Tel.: +49 (0)30 18 580 0
E-Mail: poststelle@bmjv.bund.de

Auswärtiges Amt (Deutschland)
Auswärtiges Amt
Werderscher Markt 1
10117 Berlin
Tel.: +49 (0)30-18-17-0
E-Mail: poststelle@auswaertiges-amt.de

Europäische Zentralbank
Europäische Zentralbank
Sonnemannstraße 20
60314 Frankfurt am Main
Deutschland
Tel.: +49 69 1344 1300
E-Mail: info@ecb.europa.eu

Bundesanstalt für Finanzdienstleistungsaufsicht BAFIN (Deutschland)
Bundesanstalt für Finanzdienstleistungsaufsicht BAFIN
Graurheindorfer Str. 108
53117 Bonn
E-Mail: poststelle@bafin.de

Büro des Chief Executive (Hongkong)
Sonderverwaltungszone Hongkong
Volksrepublik China
Tamar, Hongkong
Tel. : (+852) 2878 3300
E-Mail : ceo@ceo.gov.hk

Das Wirtschafts- und Handelsbüro Hongkong in Berlin (HKETO Berlin)
Jägerstraße 33
10117 Berlin
Tel.: +49 (0)30 22 66 77 228
E-Mail: general@hketoberlin.gov.hk

Botschaft der Volksrepublik China in der Bundesrepublik Deutschland
Politische Abteilung und Abteilung für Wissenschaft und Technologie
Märkisches Ufer 54
10179 Berlin
Tel.: +49 (0) 30-27588 0
E-Mail: protokoll.botschaftchina@gmail.com
E-Mail: wiss.tech.botschaftchina@gmail.com

ANLAGEN

- **A1: Liste der Überweisungen geschädigter Investoren an HSBC UK**
- **A2: Liste aller Überweisungen geschädigter Investoren an HSBC HK**
- **A3: Prospekt von Zijin Mining**
- **A4: Konsolidierte Liste aller Fake News zu den betrügerischen Brokern**
- **A5: Konsolidierte Liste aller Fake News zu den betrügerischen Technologieunternehmen**
- **A6: Beschreibung des Betrugssystems "Investment Scam Asia"**
- **A7: Erläuterung der Betrugsregelung**
- **A8: A8_a, A8_b und A8_c: alle eingereichten Beschwerden im Zusammenhang mit dem ISA-Betrugssystem**
- **A9: Historische Sanktionen der HSBC**
- **A10: Liste aller eingesetzten Briefkastenfirmen**
- **A11: Analyse von drei HSBC-Konten**
- **A12: DUPLEX (HK) Firmenregistrierung**
- **A13: DUPLEX (HK) Kontobewegungen (Beispiel)**
- **A14: Liste der besonderen Bankvorfälle im Zusammenhang mit HSBC Hongkong**
- **A15: Offizielle Bankkontodokumente (auf Anfrage zu liefern)**
- **A15_1: Bankkontodokumente von Duplex Trade Limited**
- **A15_2: Bankkontodokumente von HK Emay Limited**
- **A15_3: Bankkontodokumente von HK Macchard**

PRESSE- UND MEDIENVERÖFFENTLICHUNGEN

Zitierte Pressemitteilungen:

P1: SCMP_2015
https://www.scmp.com/business/money/article/1681719/hong-kong-banks-caught-boiler-room-money-laundering-schemes

P2: Reddit
https://www.reddit.com/r/stocks/comments/6p8jw8/woori_bridgewater_brokerage_boiler_room_fraud/

P3: Hongkong Bank2
https://www.scmp.com/news/hong-kong/hong-kong-law-and-crime/article/2161055/fraudsters-use-thousands-hong-kong-bank

P4: Regulations Asia
https://www.regulationasia.com/hk-banks-used-to-launder-over-hk8-in-scam-proceeds-in-2020/

P5: SCMP1
https://www.scmp.com/news/hong-kong/law-and-crime/article/3118479/police-arrest-seven-hong-kong-bankers-hk63-billion

Weitere Pressemitteilungen:

P6: SCMP2
https://www.scmp.com/comment/opinion/article/3119676/money-laundering-puts-hong-kongs-reputation-risk

P7:HSBC1
https://www.icij.org/investigations/fincen-files/hsbc-moved-vast-sums-of-dirty-money-after-paying-record-laundering-fine/

P8:HSBC2
https://www.ft.com/content/5c8968bc-72a5-4355-9aeb-139ad1e51ae6

P9: HSCB3
https://www.cityam.com/hsbc-shares-hit-lowest-since-1990s-amid-money-laundering-claims/

P10: HSBC4
https://www.fintechfutures.com/2019/09/hsbc-deploys-industry-first-automated-aml-system/

P11: HSBC6
https://violationtracker.goodjobsfirst.org/parent/hsbc

P12: Hongkong Banks1
https://asianextractor.com/2015/01/18/flashback-hong-kong-banks-caught-up-in-boiler-room-money-laundering-schemes

P13: Hongkong1
https://www.scmp.com/business/banking-finance/article/2106478/hong-kong-under-spotlight-australian-money-laundering-case

P14: Hongkong2
https://www.scmp.com/business/banking-finance/article/2106478/hong-kong-under-spotlight-australian-money-laundering-case

P13: Hongkong1
https://www.scmp.com/business/banking-finance/article/2106478/hong-kong-under-spotlight-australian-money-laundering-case

P14: Hongkong2
https://www.scmp.com/business/banking-finance/article/2106478/hong-kong-under-spotlight-australian-money-laundering-case