

**The Hong Kong Monetary Authority**

55th Floor  
Two International Finance Centre  
8 Finance Street  
Central  
Hong Kong  
Tel.: (+852) 2878 8196  
Email: ETR@hkma.gov.hk

**The Hongkong Police Force**

Attention to Mr. FONG Hon-ho, Terry  
Detective Inspector of Police  
Fraud Section 10C  
Commercial Crime Bureau  
Hong Kong Police  
Tel: (+852) 2860 4745  
Email: [terryhhfong@police.gov.hk](mailto:terryhhfong@police.gov.hk); [ip-sip-fs-10c-b-div-ccb@police.gov.hk](mailto:ip-sip-fs-10c-b-div-ccb@police.gov.hk);  
[sgt-fs-10c-b-div-ccb@police.gov.hk](mailto:sgt-fs-10c-b-div-ccb@police.gov.hk)  
Reference Number: CCB RN 20001893

**The Financial Conduct Authority (UK)**

Attention to Mr. Hassan Kamara  
Supervisor / Supervision Hub  
Reference number: 207629700 (Mr. Jan Hektor)  
12 Endeavour Square  
London E20 1JN.  
Tel: +44 (0)800 111 6768  
Email: [firm.queries@fca.org.uk](mailto:firm.queries@fca.org.uk), [consumer.queries@fca.org.uk](mailto:consumer.queries@fca.org.uk)**To the relevant county specific prosecutor's**

10th of August 2021

**Regarding:**

Criminal activity of the board of management as well as the groups' chief compliance officers of HSBC Holdings PLC<sup>1</sup> and HSBC Hong Kong<sup>2</sup> (in the following "HSBC<sup>3</sup>") for participating in an

---

<sup>1</sup> HSBC Holdings PLC, 8 Canada Square, London E14 5 HQ, Großbritannien

<sup>2</sup> HSBC Hongkong, 1 Queen's Road Central, Hongkong

<sup>3</sup> the HSBC group

**Non-Government Organization to fight Cybercrime  
Verein zur Bekämpfung von Cyberkriminalität gegen Kleinanleger und Verbraucher**

Vienna • Austria • Reg No 1493630560 • [www.efri.io](http://www.efri.io) • email [office@efri.io](mailto:office@efri.io)

association-in-fact enterprise with Transnational Criminal Organizations (TCO) and thereby aiding and abetting financial fraud of thousands of innocent European consumers.

## General

1. The *European Funds Recovery Initiative (EFRI)* is a victim protection organization in line with the Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 ("Victim Protection Directive"). We support victims of cybercrime in coping with the crime committed against them, cooperate with law enforcement authorities all over Europe and act on behalf of victims in claiming damages.
2. EFRI, an association based in Vienna, Austria, founded in spring 2020, now represents more than 1.052 European consumers who were defrauded by cybercriminals as of writing over EUR 59,2 million in the form of investment scams also referred to as boiler room scams.
3. The damage done to thousands of European retail investors - mainly elderly people - by various types of investment fraud and boiler room scams is rampant in recent years and within the EU amounts to at least EUR 1 billion of damages on a monthly basis<sup>4</sup>.
4. Innocent European retail investors are deceived by promises of highly professional acting cybercriminals regarding advantageous investment possibilities, transfer their life savings and, only later realize that they have become victim of unscrupulous transnational criminal organizations (TCO).
5. This type of fraud has been drastically increasing over the past 10 years posing a serious threat to society, due to the resulting manifold consequences, such as old-age poverty, depression, social isolation, psychological and physical consequences.
6. **The use of the incumbent financial system is a critical success factor for the scammers** in addition to sophisticated software tools, aggressive marketing, fraudulent affiliate campaigns and unscrupulous call center employees.
7. The utilization of the incumbent financial system is essential to the intake of the victims' money, to launder it and, ultimately, to transfer the money to bank accounts under the direct control of the scammers.
8. Without the processing of illicit proceeds, used to fund serious criminal activities, the lifeblood of the scammers operations is disrupted.
9. As a gatekeeper to the financial system, banks have an important role in the collective fight against financial and economic crime.
10. By performing proper customer due diligence banks are mandated to detect and prevent the financial system from being misused by criminal activities, including money laundering and terrorist financing, for the safety and security of their customers and society.

---

<sup>4</sup> <https://www.fca.org.uk/publication/research/quant-study-understanding-victims-investment-fraud.pdf>

11. Banks are the first layer of defense against money launderers and other criminal enterprises who choose to utilize the global financial system to further their criminal activity.
12. Banks have the responsibility to apply appropriate due diligence in monitoring the transactions processed on their financial systems and identifying the origin of funds in order not to assist any criminal activity.

### Payments to HSBC

13. EFRI represents 145 (63+82) European retail investors who have lost more than EUR 13.7 (1.9+11.5 + 1.3) Mio of their life savings to TCOs which made use of the HSBC payment system<sup>5</sup> to intake the stolen money, to launder it and to garner the proceeds of crime.
14. Related to UK banking sector activity, 63 victims were tricked by the Russian-led investment scam Blue Trading (also referred to the “Blue Trading Fraud”) to transfer EUR 1.9 Mio. to the account of the company Vilardes Group Ltd, 62-76 Park Street, London SE1 9DZ (GB10HBUK40127882816886, HBUKGB4BXXX) operated by the HSBC PLC UK from February 2018 up to February 2019 (compare **Attachment A1** for details on the victims involved and the money transferred).
15. 82 victims lost their money to a UK-led investment scam TCO, with boiler rooms being in South East Asia (referred to as the “Investment Scam Asia” (ISA) Fraud”). 30 of these victims have transferred EUR 10.5 million from July 2017 to March 2020 to 33 different HSBC Hong Kong bank accounts of special-purpose companies acting as illegal payment services providers (money mules). Additional 1.3 Mio. Euro were transferred by 5 victims to 6 Hang Seng Bank accounts between November 2017 and November 2018.
16. The details of the transfers of the European victims to HSBC Hong Kong and Hang Seng Bank fraudulent bank accounts as well as any other banks involved are shown in **Attachment A2** (A2\_a: wire transfers to HSBC; A2\_b: wire transfers to Hang Seng Bank; A2\_c: wire transfers to all other banks).

### The Blue Trading Fraud

17. The Blue Trading Forex and Crypto investment fraud was set up by Russian scammers. This boiler room fraud was run over a period of 2,5 years from January 2017 up to April 2019 and has defrauded several thousand European consumers by approximately EUR 165 Mio. Through a global network of shell companies with bank accounts with international banks like Deutsche Bank and HSBC UK the stolen money was laundered. The victims have filed criminal complaints in multiple Europe jurisdictions.

---

<sup>5</sup> Hang Seng Bank is a subsidiary of the HSBC group with HSBC management being part of the board of directors of the Hang Seng Bank (source: Hang Seng Bank annual report 2019). HSBC group owns 62.14 % of Hang Seng Bank (source: Yahoo Finance, Wikipedia).

## The ISA Fraud

18. Allegedly highly experienced brokers pretending to call from New York or London<sup>6</sup> conceive unsuspecting high-wealth European retail investors in depositing material amounts with Asian banks for investments in Hong Kong-based technology companies.
19. Hong Kong-based technology companies are promoted as compelling investment opportunities in the promising Asian high-tech economy.
20. So called trading companies – pure shell companies – established and used exclusively for the intake of the money from the European victims - have the following characteristics:
  - Most of these trading companies are newly founded, the formation as well as the registration process is done by Hong Kong Company builders (TCSPs).
  - All Trading as well as “promising” technology companies have their registered offices at the Hong Kong company builder’s offices.
  - The registered managing directors and nominee shareholders are mainland Chinese with no residency in Hong Kong – we learned that mainland Chinese, selling their identity - are continuously recruited by Hong Kong company builders.
  - All these trading companies and promising technology companies have no employees, or substantiated operational history.
  - Their business purpose, as registered in the commercial register of Hong Kong, does not match with the financial activities of these Trading Companies – who act exclusively as illegal payment service providers.
  - The scammers use highly professional marketing materials to attract investors (**Attachment A3**: prospectus of Zijing Mining Corp HKEX:2899 sent by a fake brokerage named Osaka Matsui Management) and promote their pre – IPO companies on renowned financial platforms such as Bloomberg, Yahoo Finance, Crunchbase, Finanznachrichten.de, etc. and fabricated sites such as [www.asianewswire.com](http://www.asianewswire.com) to market their fraudulent activities (exemplary links: [DigitalPay1](#); [DigitalPay2](#); [Autotech HK](#), [AutoTech HK CB](#), [AutoTech Finanzen.at](#)). More details on the numerous fake news can be found in the **Attachments A4** and **A5**.
  - Over a period of months, the unsuspecting European retail investors are conceived and driven to transfer their life savings to different Asian bank accounts – mainly HSBC bank accounts - before it becomes evident that all promises and highly professional appearing documents are just fake, and their money has been stolen and the investment advisers are no longer reachable by phone or email.
21. The TCOs have developed a sophisticated fraud network in Asia, which has its epi - center in Hongkong. In order to execute the fraud, the following elements are used and synchronized:
  - a. Setting up 1<sup>st</sup> layer accounts in order to receive the victims’ deposits.

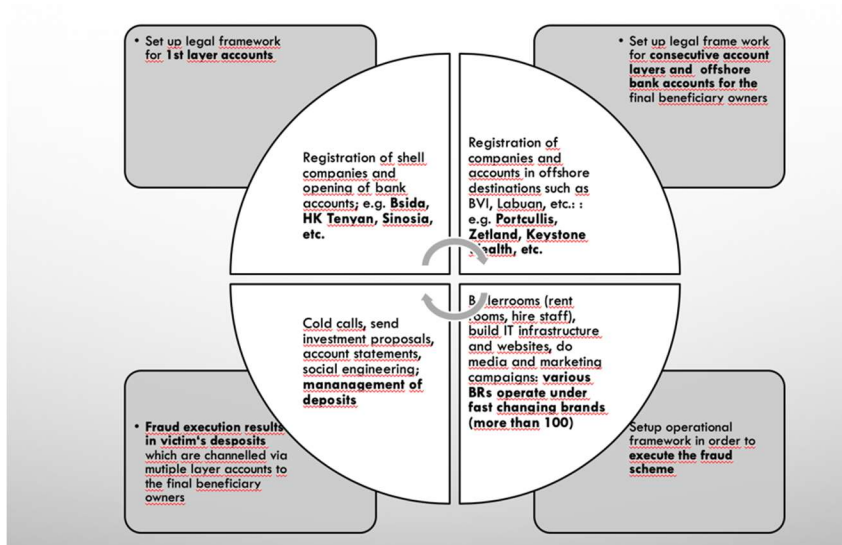
---

<sup>6</sup> The experienced brokers later turn out to be just multilingual guys applying deceiving marketing methods and being sitting with hundreds of other scammers next to them in call centers in Malaysia and/or the Philippines.

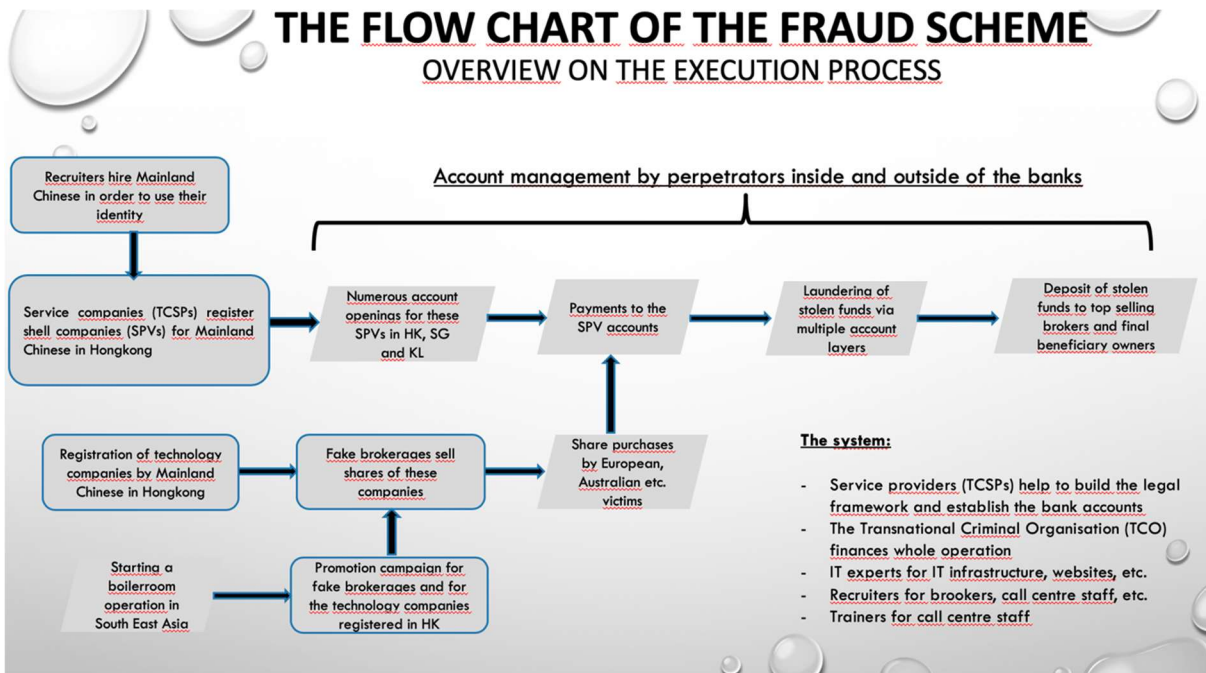
- b. Setting up 2<sup>nd</sup> layer and consecutive layer accounts including the legal entities in order to launder the deposits.
- c. Setting up the operational level in order to execute the fraud. The operational level requires inter alia boiler room staff, IT infrastructure as well as media and marketing.

The following picture shows the interaction of the various elements and activities.

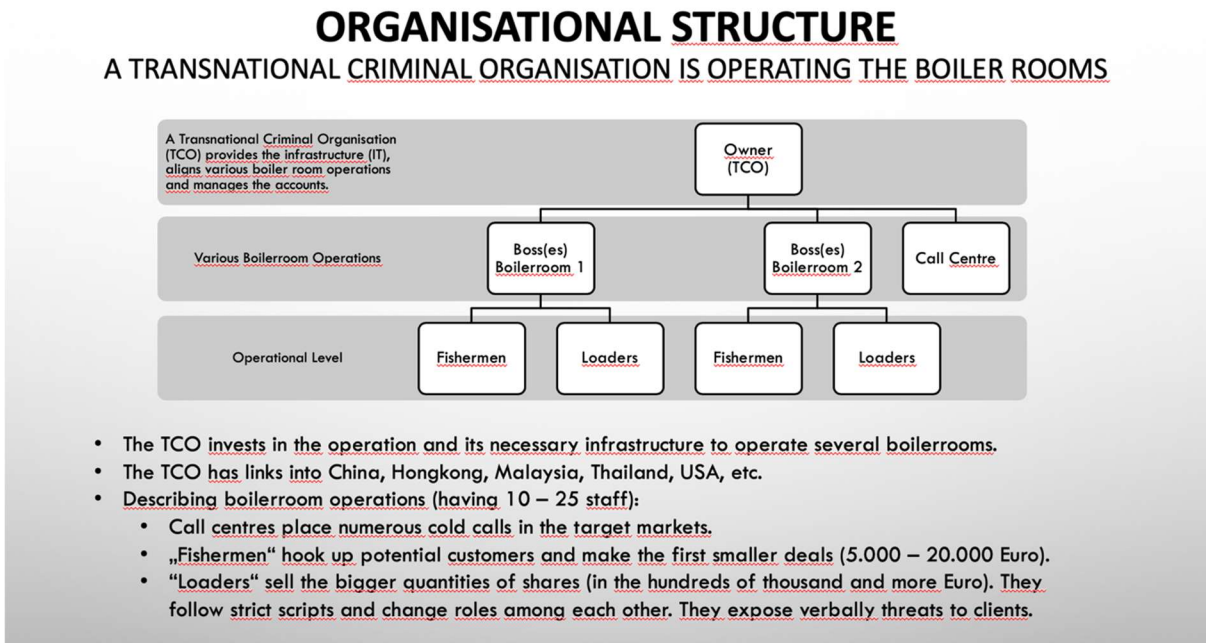
### THE INTERACTIONS OF THE FRAUD NETWORK BUILDING AND MAINTAINING THE REQUIRED STRUCTURAL ELEMENTS



The fraud itself if executed following a specifically designed workflow.



The following picture shows the organizational structure of the ISA investment fraud scheme.



Additional information on the fraud scheme can be found in the **Attachments A6 and A7**.

**Non-Government Organization to fight Cybercrime**  
**Verein zur Bekämpfung von Cyberkriminalität gegen Kleinanleger und Verbraucher**

Vienna • Austria • Reg No 1493630560 • [www.efri.io](http://www.efri.io) • email [office@efri.io](mailto:office@efri.io)

22. For the ISA fraud the following numbers<sup>7</sup> apply:
- a. At least 114 shell companies were registered in Hongkong.
  - b. At least 111 active bank accounts were opened for these shell companies. Of these active bank accounts at least 78 active bank accounts were opened in Hongkong and 33 bank accounts were opened in other Asian jurisdictions.
  - c. At least 14 “technology companies” were used, all registered in Hongkong.
  - d. At least 23 different banks were used of which 12 banks are located in Hongkong.
  - e. The total damage of the 82 ISA victims is 22.05 Mio. Euro.
23. As this kind of Asian investment fraud scheme has been active since 2015 or earlier (see for example of press and media publications, here [SCMP 2015](#); or here [Reddit](#)), there must be thousands of additional European victims, who have suffered similar extraordinary losses, accumulating to several hundreds of million EUR.
24. All defrauded 82 European ISA retail investors filed criminal complaints in their relevant EU jurisdictions on charges of investment fraud and other offences; as well having lodged criminal complaints with the Hong Kong Police beginning in October 2020 until present day. See **Attachments A8\_a, A8\_b and A8\_c**. The Commercial Crime Bureau (CCB) in Hongkong launched a joint investigation by middle of October 2020 under the reference number "CCB RN 20001893".

The participation of HSBC in the fraud

25. HSBC Holdings plc is a British multinational group and financial services holding company. It is the second largest bank in Europe.
26. According to information published on its website <https://www.hsbc.com/who-we-are> HSBC (all wholly owned or controlled HSBC Group of companies) is committed to implementing single global standards shaped by the most effective anti-money laundering standards available in any location where HSBC operates.
27. According to HSBC’s announcements - as advertised on its public website - it has established a global anti-money laundering programme (“AML Programme”). The objective of the AML Programme is to ensure that money laundering risks identified by HSBC are appropriately mitigated. This is achieved by establishing board-approved, minimum governing policies, principles and standards and implementing appropriate controls, to protect HSBC, its employees, shareholders and customers from money laundering. The AML Programme provides guidance to all HSBC employees, requiring them to conduct business in accordance with applicable AML laws, rules, and regulations. (EU MLD6 Directive, UK AML regime 01/2020).
28. According to the HSBC’s announcements the HSBC AML Programme is based upon various laws, regulations and regulatory guidance from the United Kingdom, the European Union, Hong Kong,

---

<sup>7</sup> These are just the numbers we know based on the documentation of the 82 victims - based on the evident very professional manner of the TOC – we expect that the actual numbers of shell companies, bank accounts used, and victims are much higher.

the United States of America, and as applicable, local jurisdictions in which HSBC does business. According to HSBC's website the AML Programme includes, but is not limited to:

- The appointment of a Global and Country Money Laundering Reporting Officer ("MLRO") or alternative position as required by local regulation
- A Customer Due Diligence ("CDD") Programme, which incorporates Customer Identification and Verification ("ID&V") and Know Your Customer ("KYC") principles, and the implementing of programmes designed to appropriately remediate CDD of existing customers
- Conducting enhanced due diligence ("EDD") on customers assessed as higher risk, such as Politically Exposed Persons ("PEPs") in senior positions, their relatives and close associates.
- Establishing processes and systems designed to monitor customer transactions for the purpose of identifying suspicious activity.
- The investigation and subsequent reporting of suspicious activity to the appropriate regulatory bodies.
- Mandated regular independent testing and regular AML training of its employees and contractors.
- The prohibition of the following products, services and customer types:
  - Anonymous accounts or numbered accounts or *customers seeking to maintain an account in an obviously fictitious name.*
  - Shell banks, i.e., banks with no physical presence or staff.
  - Hold Mail, i.e., where the customer has instructed all documentation related to the account are to be held on their behalf until collection.
  - Payable-through-accounts, i.e., HSBC does not allow domestic or foreign bank customers to provide payable-through-accounts to their customers on their HSBC accounts; and
  - Any relevant additional local requirements.

29. HSBC also announces proudly to be member of the Wolfsberg Group, an association of thirteen global banks that aims to develop financial services industry standards for KYC, AML and Counter Terrorist Financing.

30. Notwithstanding HSBC's claim to have implemented and abide by state-of the art compliance programs, the bank and its subsidiaries have paid over USD 6.5 billion in civil penalties since 2000, in total 59 violations have been registered (compare **Attachment A9**).

31. Although the HSBC Management, must be aware of the vulnerability and inadequacy of the group's compliance in general due to the numerous compliance issues already heavily prosecuted and penalized in former years HSBC continues to deceive third parties about their commitment to hinder criminals to use their financial systems to launder money.

**Non-Government Organization to fight Cybercrime**  
**Verein zur Bekämpfung von Cyberkriminalität gegen Kleinanleger und Verbraucher**

Vienna • Austria • Reg No 1493630560 • [www.efri.io](http://www.efri.io) • email [office@efri.io](mailto:office@efri.io)

32. Specifically due to the hefty media coverage about the misuse of their banking system for investment fraud (as listed below<sup>8</sup>) in the past – strengthened by London and Hong Kong being international financial centers with a relative ease of company formation - HSBC must have been aware of the high risk that their financial system is used by scammers to steal money from innocent European retail investors by maintaining accounts in an obviously fictitious name (something actually forbidden under HSBC's developed AML Programme (compare 28)).
33. More than 110 shell companies (for fictitious Trading Companies; compare 23) in Hongkong, with more than 110 bank accounts, 78 of them in Hongkong, were established in the period between June 2013 and February 2021 (compare **Attachment A10**), **thereof more than 33 bank accounts were opened with HSBC.**
34. By providing the TCOs' shell companies with bank accounts, HSBC was the primary bank for these two fraud schemes mentioned.
35. We claim that HSBC either knew about the wrongdoing or at least willfully acted negligent regarding the fraudulent activities within its enterprise related to the two fraud schemes.
36. Therefore, we must assume that HSBC participated in an association-in-fact enterprise with the TCOs and made themselves accomplices in defrauding thousands of unsuspecting European retail investors.
37. HSBC failed to exercise a minimal degree of caution or care, with the aggravating factor that the underlying pattern of fraud in Hong Kong has been known for many years (e.g., FATF Hong Kong evaluation 2019).

The pattern of the criminal activity

38. HSBC engaged in this pattern of criminal activity over several years and in connection with several different raids of transnational criminal organizations. The incidents of criminal activity include, but are not limited to, those set forth below<sup>9</sup>:
  - Providing bank accounts to the shell companies dressed as trading Limited's, notably in quite a restricted number of specific HSBC branches in Hong Kong<sup>10</sup>.

---

<sup>8</sup> P1: South China Morning Post reported in 2015 on a so-called "boiler room" scam combined with money laundering. Link: [SCMP 2015](#)

P13: South China Morning Post reported in August 2018 that thousands of fraud accounts existed in Hong Kong that were used for fraud. Link: [Hongkong Bank2](#)

P4: Regulation Asia reported in Feb 2021 that there were more than 10,000 accounts in Hong Kong used for fraud in 2020 as well. Link: [Regulations Asia](#)

P2: South China Morning Post reported in 2021 that for the first time in Hong Kong's history, bank employees were arrested for helping to set up criminal accounts. a so-called "boiler room" fraud.

<sup>9</sup> The activities on three exemplary HSBC accounts were checked. The result is summarized in **Attachment A11**.

<sup>10</sup> Out of 550 HSBC branches, 33 accounts established at HSBC Hong Kong show that:

- 13 accounts were held at branch number "023" ("Hennessy Centre").

- Accepting identical company registration documents of numerous shell companies, e.g., using identical wording and submitted during the onboarding due diligence to HSBC HK.
- Accepting that several of the trading Limited were registered at the same correspondence address in Shenzhen (neighboring city of Hong Kong) without raising this issue in the onboarding process.
- Accepting a change of directorship of the trading Limited's to non-verified foreign identities, following the onboarding<sup>11</sup>. Many trading Limited's onboarded, had the same French person appointed, named Mrs. Caroline Virgine Valerie Tessier<sup>12</sup>, as company director following the onboarding process.
- Raising no issues although immediately following the onboarding, high wire transfers from EU countries, occur daily, with withdrawals shortly after, often several times within 24 hours of deposit,<sup>13</sup> (compare **Attachment A13** account movements on the account of #023 727423 838 (Duplex (HK) Trade Limited) for the period from 5<sup>th</sup> of June 2019 to 21<sup>st</sup> of June 2019) can be observed.
- Raising no issues although neither the size of the amounts transferred, the nomination, nor the payees, or the frequency of the wire transfers fits with the business activity as presented during the onboarding process.
- Accepting high international inbound and outbound wire transfers (single transfers exceeding 100.000, - EUR with one transfer) although only Chinese trade contracts foreseeing amounts below 10.000 Euros were presented during the customer due diligence process.
- Accepting a significant excess of the account turnover announced during the onboarding process. The total of the actual deposits and withdrawals made, exceeded the expected annual or monthly turnover given during the onboarding process by multiple factors.

- 
- 8 accounts were held at branch number "741" ("Hong Kong Office Commercial Service Centre")
  - 6 accounts at branch number "582" ("Sun Hung Kai Centre")
  - 2 accounts at branch "747" ("Cheung Sha Wan Commercial Service Centre")
  - 2 accounts at branch "038" ("Shatin Centre")
  - One account each at branches "024", "801" and "817".

<sup>11</sup> The **Attachment A12** shows as an example the registration of Duplex (HK) Trade Limited on the 27<sup>th</sup> of December 2018 (first row) in the name of a Chinese person Wang Hong Biao. On the 6<sup>th</sup> of March 2019 this Chinese resigned, and a new company director named Ms. Tessier, allegedly a French national, was appointed (second row). The purpose of this change in directorship was obviously to have full control on the bank account of Duplex (HK) Trade Limited and obfuscate any further enquiry.

<sup>12</sup> Ms. Caroline Virgine Valerie Tessier is registered as general manager of 91 companies registered, of which 5 companies fall into the fraudulent trading companies involved in this fraud scheme (HK Maccard, HK Emay, HK Duplex, HK Yokeda, Yasenda (HK) Co. Ltd., all of them holding accounts at HSBC.

<sup>13</sup> Based on reviewed documentation for three HSBC HK accounts (HK with #741 147909 838 (Macchard Trade Limited), # 023 727316 838 (HK Emay Trade Limited); # 023 727423 838 (Duplex (HK) Trade Limited)

- Accepting that identical IP addresses were used for online banking transfers of various HSBC accounts, each having a different beneficiary owner.
- Giving misleading information<sup>14</sup> to European retail investors on request about suspicious transactions, once the fraud was evident.
- for other questionable banking activities as summarized in **Attachment A14**.

39. Summarizing, red flags must have been always raised - but HSBC did not act on appropriately.

Gross Violation of AML/TF Law and EBA guidelines

40. According to 13 (1) of EU-Directive 2015/849 for obliged entities, CDD (customer due diligence) is central for both risk assessment and risk management purposes.
41. According to the EU-Directive 2015/849 Customer due diligence includes the following measures:
- identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
  - identifying the customer's beneficial owner and taking reasonable measures to verify their identity so that the obliged entity is satisfied that it knows who the beneficial owner is.
  - assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
  - conducting ongoing monitoring of the business relationship. This includes transaction monitoring and keeping the underlying information up to date.
42. EU Directive 2015/849 provides that obliged entities can determine the extent of these measures on a risk-sensitive basis<sup>15</sup>. It also provides that where the risk associated with the business relationship or occasional transaction is low, Member States may allow obliged entities to apply simplified customer due diligence (SDD) measures instead. Conversely, where the risk associated with the business relationship or occasional transaction is increased, obliged entities must apply enhanced customer due diligence (EDD) measures. However, the Directive does not

---

<sup>14</sup> **Attachment A15** (documents on three HSBC accounts, to be delivered on demand) and Attachment 14, page 15 onwards: Mr. Kroesser, a German victim, transferred 16.890 Euro to the account 023 727316 838 of HK Emay on the 5th of June 2019, the same transfer was returned to him with fees deducted on the 21st of June 2019. Notably, the account of HK Emay was used extensively in April and May 2019 to receive numerous overseas deposits, but it was also in existence in June 2019 (compare the account statements of HK Emay dated 29th of June 2019). During the clarification process, in HSBC's official reply to the victim dated 5th of February 2021 HSBC describes itself as "... receiving bank, which is obliged to process the payment instructions based on the instruction received....". In its further answer to the aggrieved investor dated 20th of April 2021 the HSBC even denies any knowledge on this specific incident. Considering the fact, that the HK Emay account was still existing in June 2019 and even until June 2020, HSBC HK should have executed the transfer of Mr. Kroesser according to its own definition. For some unknown reasons, the scammers did not want to receive deposits in the HK Emay account since beginning of June 2019 anymore and were obviously influencing HSBC HK to reject Mr. Kroesser's transfer.

<sup>15</sup> In line with the FATF's standards, Directive (EU) 2015/849 puts the risk-based approach at the center of European Union's AML/CFT regime. It recognizes that the risk of ML/TF can vary obliged entities have to take steps to identify and assess that risk with a view to deciding how best to manage it.

set out in detail how obliged entities should assess the risk associated with a business relationship or transaction, nor does it set out exactly what SDD and EDD measures entail.

43. As of January 4th, 2018 ESA, issued Joint Guidelines under Articles 17 and 18(4) of the EU Directive 2015/849<sup>16</sup> on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (The Risk Factors Guidelines).
44. These guidelines were applicable beginning with 26 June 2018. In accordance with Article 16(3) of the ESAs Regulations, competent authorities and financial institutions must make every effort to comply with the guidelines.
45. HSBC claims on its websites and business reporting to adhere to all these rules (compare 28).
46. But evidently HSBC's approach to assessing and managing the ML/TF risk associated with business relationships and occasional transactions as requested by the Joint Guidelines and all other applicable regulatory rules failed as follows:
  - No appropriate business wide risk assessment. HSBC with having international exposure and operating at international financial centers (e.g., London and Hong Kong) known for their ease of shell company registration must apply sophisticated risk assessment.
  - No appropriate level of CDD: Firms should use the findings from their business-wide risk assessment to make an informed decision on the appropriate level and type of CDD that they will apply to individual business relationships and occasional transactions.
  - Did not obtain a holistic view: HSBC did not gather sufficient information to be satisfied that in having identified all relevant risk factors, including, where necessary, by applying additional CDD measures, and assess those risk factors to obtain a holistic view of the risk associated with a particular business relationship.
  - No permanent monitoring and reviewing of the business relationships took place. HSBC did not monitor transactions to ensure that they are in line with the customer's risk profile and business

---

<sup>16</sup> On 26 June 2015, Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing entered into force. This Directive aims, inter alia, to bring European Union legislation in line with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation that the Financial Action Task Force (FATF), an international anti-money laundering standard setter, adopted in 2012. In line with the FATF's standards, Directive (EU) 2015/849 puts the risk-based approach at the center of the European Union's anti-money laundering (AML) and countering financing of terrorism (CFT) regime. It recognizes that the risk of money laundering and terrorist financing (ML/TF) can vary and that Member States, competent authorities, and credit and financial institutions within its scope ('firms') have to take steps to identify and assess that risk with a view to deciding how best to manage it. Articles 17 and 18(4) of Directive (EU) 2015/849 require the European Supervisory Authorities (ESAs) to issue guidelines to support firms with this task and to assist competent authorities when assessing the adequacy of firms' application of simplified and enhanced customer due diligence measures. The aim is to promote the development of a common understanding, by firms and competent authorities across the EU, of what the risk-based approach to AML/CFT entails and how it should be applied.

and, where necessary, examined the source of funds, to detect possible ML/TF. HSBC must also keep the documents, data or information it holds up to date, with a view to understanding whether the risk associated with the business relationship has changed.

Failure to apply EDD for the shell companies with unusual transactions:

47. According to Article 18 (2) EU-Directive 2015/849 HSBC must put in place adequate policies and procedures to detect unusual transactions or patterns of transactions.

With transactions being unusual because:

- they are larger than what the firm would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs.
- they have an unusual or unexpected pattern compared with the customer's normal activity or the pattern of transactions associated with similar customers, products or services; or
- they are very complex compared with other, similar, transactions associated with similar customer types, products or services, and the firm is not aware of an economic rationale or lawful purpose.

48. Therefore, HSBC would have been required to apply the following EDD measures<sup>17</sup> to help HSBC determine whether these transactions give rise to suspicion and must at least include:

- taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and
- monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. A firm may decide to monitor individual transactions where this is commensurate to the risk it has identified.

---

<sup>17</sup> As set in section 59 of the Joined Guidelines

Failure to apply increased customer risk requirements as required by the Joined Guidelines.  
Chapter 2: Sectoral guidelines for retail banks

49. According to Chapter 2 of the Joined Guidelines retail banks offering current accounts must allow for increased customer risk factors (again requiring EDD measures) if the following criteria are fulfilled:

- an unusual high volume or large value of transactions (98).
- The customer is a new undertaking without an adequate business profile or track record (100 v).
- The customer is a non-resident. (100 vi)
- The customer's behavior or transaction volume is not in line with that expected from the category of customer to which they belong or is unexpected based on the information the customer provided at account opening (100 iii).

## SUMMARY

50. HSBC supported the TCOs in getting control of the stolen funds. The use of HSBC bank accounts has been essential to the intake of the victims' money, to launder it and, finally, to transfer the funds to bank accounts under the direct control of the scammers.
51. HSBC enabled the TCOs to solicit funds from innocent European retail investors, aiding in the misappropriation of funds. Investors were thus prevented from allocating their funds for the intended purpose, to invest in high-promising Asian Technology companies.
52. The members of the criminal enterprise formed, played specific roles in the robbery of the life savings of the European investors. HSBC's role was to provide access to the incumbent financial system with knowledge of the illegal use of those services and/or a blind eye toward way their services were used for the intake, the laundering and to bring the money under control of criminals.
53. Regardless of the specific entity that played any role, the roles were well-defined, established and accepted by the members of the enterprise. Each of these roles was essential to raid the life savings of the European investors.
54. We are convinced that HSBC group failed willingly the group's AML Programme, therefore also failing to meet the conditions set by deferred prosecution agreements dated December 12, 2012 of the US authorities, as HSBC has committed to undertake enhanced AML and other compliance obligations and structural changes within its entire global operations. In order to prevent a repeat of the conduct that led to the criminal prosecution of HSBC after having facilitated the launder of millions of drug money dating back to 2012.
55. Despite evidence of serious money laundering risks associated with doing business in Hong Kong and London, HSBC missed to undertake any serious action to avoid being misused for investment fraud activities.
56. **As set out in EBA's Joined Guidelines in<sup>18</sup> Section 62 HSBC should not enter a business relationship if they are unable to comply with their CDD requirements, if they are not satisfied that the purpose and nature of the business relationship are legitimate or if they are not satisfied that they can effectively manage the risk that they may be used for ML/TF purposes.**

### Accusations raised

57. We accuse the HSBC group of having made itself accomplices to boiler room scammers belonging to larger TCO networks (Russian and Asian), by violating its corporate group anti-money laundering policy.
58. Therefore, it must be assumed that, by neglecting professional duties, immoral damage to European retail investors was intentionally accepted by HSBC.

---

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

59. Furthermore, the underlying patterns that enable fraud in Hong Kong are commonly known in professional and regulatory circles (as mentioned, amongst others, in the FATF Mutual Evaluation Report of Hong Kong, China 2019).
60. HSBC's blatant failure to implement adequate anti-money laundering controls and in applying a proper risk-based compliance programme facilitated the laundering of hundreds of millions of stolen monies from unsuspecting European retail investors.
61. HSBC's evident compliance program deficiencies— including with respect to screening, testing, auditing, and transaction review procedures—enabled TCOs to steal and launder millions if not hundreds of millions from innocent European consumers.
62. HSBC group is to be held accountable for stunning failures of oversight – and worse – that led the bank to permit scammers and others to launder hundreds of millions of dollars through HSBC subsidiaries.
63. HSBC knew or must have known that the organizational structures of HSBC group did not comply with the required legal provisions and that the risk of misuse of the financial system by criminal organizations has been high. This has enabled the theft of hundreds of millions of lifetime savings from European retail investors over the past years.
64. Therefore, the extent of the obvious gross negligence in executing existing KYC due diligence, on monitoring obligations and reporting obligations needs to be attributed with an intentional violation of international regulations and intentional harming of European retail investors.
65. It is therefore reasonable to assume that HSBC's actions, namely the deliberate neglect of a legally required adequate set-up of a risk management system and other organizational units to prevent money laundering, were motivated by pure economic self-interest in order to gain a competitive advantage.

Best Regards

Elfriede Sixt    Nigel Kimberly

**Non-Government Organization to fight Cybercrime**  
**Verein zur Bekämpfung von Cyberkriminalität gegen Kleinanleger und Verbraucher**

Vienna • Austria • Reg No 1493630560 • [www.efri.io](http://www.efri.io) • email [office@efri.io](mailto:office@efri.io)

**This complaint will also be filed with:**

**Office:**

**Germany -**

**Munich Public Prosecutor's Office II**

Staatsanwaltschaft München II

Attention to State Attorney General Mr. Stephan Necknig

Head of Division VI - Economic Criminal Matters

Seidlstraße 21

80097 München

Germany

Phone: +49 (089) 5597-6000

Email: [stephan.necknig@sta-m2.bayern.de](mailto:stephan.necknig@sta-m2.bayern.de)

[poststelle@sta-m2.bayern.de](mailto:poststelle@sta-m2.bayern.de)

**The Bundesamt für Justiz (Swiss)**

Attention to Mrs. Lara Kübler

Reference Number: B21 – 1826 -1 (Mr. Guido Weber)

Bundesrain 20

3003 Bern

Swiss

Tel.: +41 58 464 0038

Email: [lara.kuebler@bj.admin.ch](mailto:lara.kuebler@bj.admin.ch)

**Non-Government Organization to fight Cybercrime  
Verein zur Bekämpfung von Cyberkriminalität gegen Kleinanleger und Verbraucher**

Vienna • Austria • Reg No 1493630560 • [www.efri.io](http://www.efri.io) • email [office@efri.io](mailto:office@efri.io)

**This complaint will be brought to the attention of the following organizations**

**Financial Action Task Force (FATF)**

2, rue André Pascal  
75775 Paris Cedex 16 FRANCE  
Tel: + 33 1 45 24 90 90  
Email: [Contact@fatf-gafi.org](mailto:Contact@fatf-gafi.org)

**EUROPEAN BANKING AUTHORITY**

Tour Europlaza  
20 avenue André Prothin  
CS 30154  
92927 Paris La Défense CEDEX  
France  
Tel.: +33 1 86 52 70 00  
Email: [info@eba.europa.eu](mailto:info@eba.europa.eu)

**Europol**

Eisenhowerlaan 73,  
2517 KK Den Haag  
The Netherlands  
Tel.: [+31 70 302 5000](tel:+31703025000)

**Federal Ministry of Justice and Consumer Protection (Germany)**

Bundesministerium der Justiz und für Verbraucherschutz  
Referat II B 5  
Mohrenstr. 37  
10117 Berlin  
Germany  
Tel.: +49 (0)30 18 580 0  
Email: [poststelle@bmjv.bund.de](mailto:poststelle@bmjv.bund.de)

**Federal Foreign Office (Germany)**

Auswärtiges Amt  
Werderscher Markt 1  
10117 Berlin  
Tel.: +49 (0)30-18-17-0  
Email: [poststelle@auswaertiges-amt.de](mailto:poststelle@auswaertiges-amt.de)

**European Central Bank**

Europäische Zentralbank  
Sonnemannstraße 20  
60314 Frankfurt am Main  
Germany  
Tel.: +49 69 1344 1300  
Email: [info@ecb.europa.eu](mailto:info@ecb.europa.eu)

**Non-Government Organization to fight Cybercrime  
Verein zur Bekämpfung von Cyberkriminalität gegen Kleinanleger und Verbraucher**

Vienna • Austria • Reg No 1493630560 • [www.efri.io](http://www.efri.io) • email [office@efri.io](mailto:office@efri.io)

**Federal Financial Supervisory Authority BAFIN (Germany)**

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

**Office of the Chief Executive (Hongkong)**

Hong Kong Special Administrative Region  
People's Republic of China  
Tamar, Hong Kong  
Tel. : (+852) 2878 3300  
E-mail : [ceo@ceo.gov.hk](mailto:ceo@ceo.gov.hk)

**The Wirtschafts- und Handelsbüro Hongkong in Berlin (HKETO Berlin)**

Jägerstrasse 33  
10117 Berlin  
Tel.: +49 (0)30 22 66 77 228  
Email: [general@hketoberlin.gov.hk](mailto:general@hketoberlin.gov.hk)

**Embassy of the People's Republic of China in the Federal Republic of Germany**

Political Department and Department of Science and Technology  
Märkisches Ufer 54  
10179 Berlin  
Tel: +49 (0) 30-27588 0  
E-Mail: [protokoll.botschaftchina@gmail.com](mailto:protokoll.botschaftchina@gmail.com)  
E-mail: [wiss.tech.botschaftchina@gmail.com](mailto:wiss.tech.botschaftchina@gmail.com)

**Non-Government Organization to fight Cybercrime  
Verein zur Bekämpfung von Cyberkriminalität gegen Kleinanleger und Verbraucher**

Vienna • Austria • Reg No 1493630560 • [www.efri.io](http://www.efri.io) • email [office@efri.io](mailto:office@efri.io)

## ATTACHMENTS

- **A1: List of transfers made by aggrieved investors to HSBC UK**
- **A2: List of all transfers made by aggrieved investors to HSBC HK**
- **A3: Prospectus of Zijin Mining**
- **A4: Consolidated list of all fake news on the fraudulent brokerages**
- **A5: Consolidated list of all fake news on the fraudulent technology companies**
- **A6: Description of the fraud scheme “Investment Scam Asia”**
- **A7: Presentation on the fraud scheme**
- **A8: A8\_a, A8\_b and A8\_c: all filed complaints related to the ISA fraud scheme**
- **A9: Historical sanctions of HSBC**
- **A10: List of all shell companies used**
- **A11: Analysis of three HSBC accounts**
- **A12: DUPLEX (HK) company registration**
- **A13: DUPLEX (HK) account movements (example)**
- **A14: List of special bank incidents related to HSBC Hongkong**
- **A15: Official bank account documents (to be delivered on demand)**
- **A15\_1: Bank account documents of Duplex Trade Limited**
- **A15\_2: Bank account documents of HK Emay Limited**
- **A15\_3: Bank account documents of HK Macchard**