A Case Study on a Multi-Country Money Laundering Scheme and a Proposed Automatic Detection System

Tsz-Fung Tony Tse[1,2], Xiao Tan[1,2], Siu Ming Yiu[2] and Hiu-Man Human Lam[3]
[1]Hong Kong Police Force, China
[2]Dept of Computer Science, University of Hong Kong, China
[3]Department of Justice, Hong Kong, China

tonytse@police.gov.hk
xtan@cs.hku.hk
smyiu@cs.hku.hk
humanlam@doj.gov.hk

Abstract: This paper presents a case study on the Franco-Israeli syndicates orchestrating their cross-continental money laundering schemes. These money laundering schemes have been operating for over two decades, ever since China's entry to the World Trade Organization in 2001. The paper reviews the operation of the money laundering schemes in detail and highlights the difficulties encountered by bankers and investigators in unearthing and investigating criminal activities within the banking systems. The paper then proposes an automatic anti-money laundering system, which is expected to address these difficulties. Preliminary experimental results show that the system successfully identifies the crux of these money laundering syndicates within a few days' time, something which usually takes years of investigation to track down the suspects using traditional methods, as well as its ability to initiate pre-warning procedures to the banks and law enforcement agencies once suspicious transaction clusters are found. The paper concludes with a discussion on the legal implications encompassing the evidence projected by this system.

Keywords: Cross-continental money laundering, Investigation difficulties, Legal challenges, Automatic AML detection

1. Introduction

1.1 Background

Taking advantage of the "One Country, Two Systems" principle, Hong Kong is crowned world's most open economy. The city operates under a sophisticated financial and legal infrastructure and benefits from various economic freedoms, including the free flow of capital, a free trade policy, a simple taxation system and low tax rates, and the advanced transportation and telecommunication systems, attracting global investors from all around the globe. In 2014, around a quarter of Mainland China's trades chose Hong Kong as the intermediary, be it in the form of offshore trade or re-exports (Hong Kong Monetary Authority, 2016).

Unlike Hong Kong, Mainland China has imposed a foreign exchange control which prevented money from moving in and out of the country freely. Despite the capital controls, China's economy and international trade volumes have been growing substantially and is now the world's second largest economy (Worlddata, 2022). There is a growing need for capital flow, be it for legal or illegal purposes. This encourages the use of underground banks and cash smuggling across the Chinese borders, with Hong Kong, a world-renowned free market economy, being the most viable option of all.

1.2 Introduction of Anti-Money Laundering

Anti-money laundering ("AML") is a major research topic in FinTech; money laundering is a main funding source for organized crimes. Today, money laundering has evolved into an algorithmic-based system with millions of offshore/onshore accounts, traversing countries and continents.

One appropriate definition of money laundering was introduced in Masciandaro 1993, which is structured by two key-characteristics (Donato Masciandaro. 1999): illegality including organized crime, drug trafficking and terrorist financing (general feature) and concealment to hide the illegal source of such revenues (specific feature).

There are three steps in money laundering: placement, layering and integration. Placement is placing the illegal funds in another form, which will enable the money launderer to undertake further layering and therefore disguise these amounts. Layering is washing the placed suspicious funds to produce a false source of fund, and thereby disguising the proceeds of crime, such that the original source and the current position of the funds are unclear (i.e. investing the placed funds into something legitimate). The integration is the final stage, which is to integrate the after-layering assets into a legitimate financial system, with the profits or

benefits earned via the layering process, and to transfer the liquidity assets, which can then be converted to cash easily, all done within the legitimate financial systems.

1.3 Our Contributions

In this paper, the tactics of the trade-based money laundering by the Franco-Israeli syndicates are introduced. Using international trades as its façade, it starts off with the purchase of goods or commodities in Eastern Europe, goods of which are then shipped to and sold in Hong Kong and China, the money, from the selling these goods or from the purchase of antiques or art collections, was then sent to Israel. With the infamous mastermind of such organized money laundering groups being a French-Israeli (Timesofisrael, 2016), such trade-based Anti-money laundering cases are hence called "France-Israeli syndicates". In this case study, we will (i) provide insights and observations as to the difficulties in detecting and investigation this type of money laundering cases; (ii) propose a more efficient automatic detection system which can identify similar suspicious money laundering cases efficiently, significantly shortening investigation by a years' time; and (iii) discuss the legal implications on and the admissibility of the evidence generated from the automatic system.

We hope that the results of this article will ultimately benefit the community in terms of the technological developments of AML tools, the criminal investigations carried out by law enforcement agencies, and the billing of legal frameworks or legislatures by the judiciaries.

2. Selected Money Laundering Cases

Before we provide the observations and insights on the Franco-Israeli model of money laundering (ML), three relevant cases will be outlined to illustrate their ML schemes.

2.1 Case A

In February 2009, an Israeli male – Mr. A came to Hong Kong, incorporated four companies and opened business bank accounts for these companies. Mr. A left Hong Kong shortly after the bank accounts were opened. Ten months later, in December 2009, one of the bank accounts was used to receive crime proceeds of HKD 1.9 million, which originated from a fraud case against a bank in France. The case was later reported to the Police by the bank.

Between June 2009 and January 2010, the police investigations revealed that a total of HKD 69.1 million was remitted from France, Germany and Portugal to the bank accounts set up by Mr. A, and was then further transferred to various locations including China, Cyprus, Israel and Hungary. When Mr. A was arrested, he stated that these bank accounts were opened for tax evasion purposes only. In the end, Mr. A was charged with money laundering.

2.2 Case B

In June 2009, an Israeli male – Mr. B came to Hong Kong, incorporated one company called Golden Longon Ltd. and opened a bank account at the "Hong Kong and Shanghai Banking Corporation" ("HSBC"). Mr. B left Hong Kong shortly after the bank account was opened. One month later, in January 2010, a French company was deceived in a telephone deception scam and transferred Euro 982,000 to Mr. B's account.

Bank record of the HSBC account showed that two transfers, totaling Euro 1.48M was made to a local Bank of China ('BOC") account under the name of Bisley Global BVI Co. in June 2009 and November 2009 respectively. Bisley Global BVI Co. was incorporated by another suspect, Mr. C in April 2009. The company had a total of three accounts held at BOC, Standard Chartered Bank ("SCB") and HSBC and Mr. C was the sole account signatory. Bisley Global BVI Co. was reported to be engaged in the trading of computers in Hong Kong and overseas.

Mr. C had also incorporated a local company – Tobo Group Ltd. in March 2009. The company had a total of two bank accounts at BOC and SCB and Mr. C was the sole account signatory. Tobo Group Ltd. was reported to be engaged in general trading in Hong Kong and overseas. Altogether, Mr. C had five business bank accounts, three under the name of Bisley Global BVI Co. and two under the name of Tobo Group Ltd.

Bank records showed that large funds were deposited into bank accounts operated by Mr. C, there were some inter-transactions among these bank accounts. And funds were mainly withdrawn either by way of remittances or were withdrawn in cash. Fund flow showed that most of the fund originated from France, Germany and Cyprus, and was then further transferred to Mainland China, Israel or back to Cyprus. Although funds were drained out eventually, the disposals were not all done immediately. In fact, some funds were held

in the accounts for weeks and months before they were transferred. Between May 2009 and April 2012, at least HKD 120M was laundered via these bank accounts.

Investigation into the bank accounts, under the name of Nice Alpha Ltd (incorporated by Mr. C), found that Euro 1.52M & USD 0.3M were transferred from a local BOC account under the name of a local company - Company Z - between April 2010 and September 2010. The company had another bank account at SCB. A local male – Mr. L (Mr. C's friend) was the account signatory of both accounts. At least HKD 31.05 million was laundered. The fund flow and the operation period of the two bank accounts were similar to the bank accounts operated by Mr. C, i.e., majority of the fund was originated from France, Germany and Cyprus, etc. and was further transferred to Mainland China, Israel or back to Cyprus. Some of the funds were first transferred to local money service operators before they were transferred to Mainland China. Investigation with the recipients in Mainland China of this case revealed that those transfers were supposed to be monies sent from the senders' relatives, who were working in Europe. In the end, Mr. B was included in the Interpol Red Notice.; Mr. C and Mr. L were charged with money laundering.

2.3 Case C

Mr. D is an Australia and Israel national, but regularly resided in Israel. Between January 2010 and April 2012, by instruction of his supervisor in Israel, Mr. D came to Hong Kong on 21 occasions, incorporated 9 companies and opened the business bank accounts for these companies. Mr. D knew that these bank accounts were used to receive crime proceeds (or "black money").

During the two years, Mr. D used the "black money" to purchase 342 gold bars from a gold trader and stored them in two village houses. He also collected three 5-carat diamonds from a jewelry trader on three occasions, for which he was not required to make any payments. On a final note, Mr. D also received HKD 2.68M in his personal bank accounts at HSBC and Citibank.

In May 2012, three other Israeli males – Mr. E, Mr. F and Mr. G were employed by an unknown male (not Mr. D) to assist Mr. D in removing the gold bars and diamonds from the two village houses. Some gold bars were sold back to the gold trader who sold the gold bars to Mr. D in the first place. The sale proceeds, with a total of HKD 73 million, were paid to the company bank accounts controlled by Mr. D.

Mr. D – Mr. G were all charged with money laundering and convicted for the offences charged (South China Morning Post, 2014).

3. Observations and Insights

According to the Hong Kong Money Laundering and Terrorist Financing Risk Assessment Report in 2022, over half of the convicted Money Laundering cases between 2016 and 2020 were identified as third-party Money Laundering ("ML") cases, and bank accounts are still one of the most common tools exploited by money launderers for both domestic and foreign predicate offences via cash deposits, cash withdrawals or wire transfers (Financial Services and the Treasury Bureau, 2023). Prolonged offence period, use of MSO (Money Service Operator), use of multiple layering and structuring, and use of various shell companies and bank accounts all added difficulties in identifying and investigating this money laundering model.

4. A Proposed Automatic AML Detection System

Traditionally, the investigation of such cases is long and resource consuming. Indeed, it took the Hong Kong Police more than one year to deduce the money laundering processes of the above three cases. The traditional way of doing it is to enter all entries in to an excel table including the date of transaction, the amount involved, the parties involved, the beneficiary owner of the bank account, etc. and to identify out the common linkage and money laundering pattern from it. It is not just time consuming, there is also likelihood for the investigation unit to miss out a linage by overlooking the data. However, with the support of Machine Learning and Network Analysis, and the open-source tool (e.g.: Gephy), the process of deduction was shortened substantially. The proposed automatic anti-money laundering detection system can identify suspicious transactions efficiently and accurately and can detect the masterminds, using the self-learn capabilities of artificial intelligence (AI).

4.1 The State-Of-The Art AML using Artificial Intelligence

As early as 2007, the study to automate the Anti-Money Laundering Process is proposed for finance institutions (Han, Jingguang, et al., 2020). Machine learning methodologies, e.g. classification and clustering,

are widely applied to AML systems, in the detection of suspicious transactions. In 2007, Gao and Xu proposed the Herbert A. Simon's Model of Decision-Making, which was used to calculate the likelihood of the transactions being that of high-risk AML (Gao, Shijia, and Dongming Xu., 2009). In 2012, Stefan Axelsson *et. al.* introduced a classification method for money laundering detection in a data set consisting of synthetic financial transactions, thereby targeting anomalies inside a data set of mobile money financial transactions, by using the classification techniques to categorize transactions as either suspicious or non-suspicious (Lopez-Rojas, Edgar Alonso, and Stefan Axelsson, 2016). In the paper published by Nida S. Khan *et. al.* in 2013, a Bayesian network (BN)-based approach is proposed to calculate the account holder's transaction behavior score, based on the transaction history. An alert will be generated if a significant difference is detected in the account holder's transactional patterns and behaviors (Khan, Nida S., et al., 2013). However, for the aforesaid supervised methods, the imbalanced training dataset between normal transactions and anomalous transactions is the key defect, in terms of the performance in detecting suspicious transactions.

Except for the machine learning and deep learning methodologies of transactions identification and classification, network analysis is another type of methodology used in analyzing the money laundering process. Common network analysis systems contain variables, e.g., the degree of centrality, authoritativeness, and closeness centrality. These indices measure the closeness and betweenness of the relationship of the connections and the importance of each node in the networks. In 2015, Drezewski *et. al.* introduced a network analysis of bank statements and the National Court Register data to deduce the analysis of social networks for money laundering cases. In 2017, Colladon and Remondi (2017a, b) built several networks to work collectively, including transactions, the economic sector, geographical area, and tacit link networks to prevent money laundering. They used the 19-months data of a factoring company that mainly operates in Italy. They found that network metrics were extremely useful in fraud-risk assessment (Xiao, Guohui, et al., 2019).

In our Automatic Anti-money Laundering System design, both the anomalous transaction detection technology and the link analysis are adopted and combined to construct the main architecture of the system. Except for the suspects detection and monitoring agents, which is based on the unsupervised algorithms and the link analysis, the knowledge graph technology works as the reference library and event analysis to refresh and supplement the features on accounts and account holders' level. The details would be described in the sections below.

4.2 The Methodology

In this section, we propose an Automatic Anti-Money Laundering Detection System ("AAMLDS") which combines the unsupervised algorithm with the link analysis on the financial institutions' transactions, accounts and account holders' data. The data is kept updated using the knowledge graph to identify the missing information or potential errors, as well as to discover the new suspect personalities and their *modus operandi*. The architecture design of the system is briefed as below.

The original data sources include the transaction, accounts and account holders' data from financial institutions, as well as the reference data from external authorities and the AML-related news reports. The original data are loaded to the AAMLDS with an API agent. Based on the different purposes of the transactions, there are two components in AAMLDS. The first one is the Anomalous Transactions Detection Agent, which adopts the incremental principal component analysis ("IPCA"), or density-based spatial clustering of applications with noise (" DBSCAN") for detecting the anomalous changes with imbalanced distributed and unlabeled transaction data. This helps identify suspicious accounts or account holders to generate the labelled data from the original unlabeled raw data. Then, based on the detected suspicious accounts and account holders, the Network Analysis Agent builds up the link analysis and social network analysis ("SNA") to deduce the complete money laundering fund flow by creating the visual representations of transactions to track the movement of the funds, thereby identifying the source and the destinations of the funds, illustrating the relationships between accounts, and predicting the trends and patterns of money laundering (Dre˙zewski, Rafał, Jan Sepielak, et al., 2015). In this paper, we will take Amazon Web Services ("AWS") as the cloud platform example.

This system adopts both security orchestration, automation, and response (SOAR) and elastic security info and event management (SIEM) to build up the security operations platform (Kinyua, Johnson, and Lawrence Awuah., 2021). SIEM investigates and alerts the security risk by analyzing the logs and events. Such traditional security approach is enhanced by SOAR, an automatic, software-defined security with AI/ML involved incidents responses (Sridharan, Anish, and V. Kanchana., 2022). Such security operation platform is capable to provide enhanced security protection for the internal and external data transmission, storage and analysis in the cloud.

This system combines the Anti-money Laundering databases from financial institutions with the alert reports and analysis to the regulatory and the law enforcement agencies. Those reports are refreshed regularly to provide the complete and updated funds flow-in and flow-out processes between various suspects and suspicious accounts. The pros of the system include:

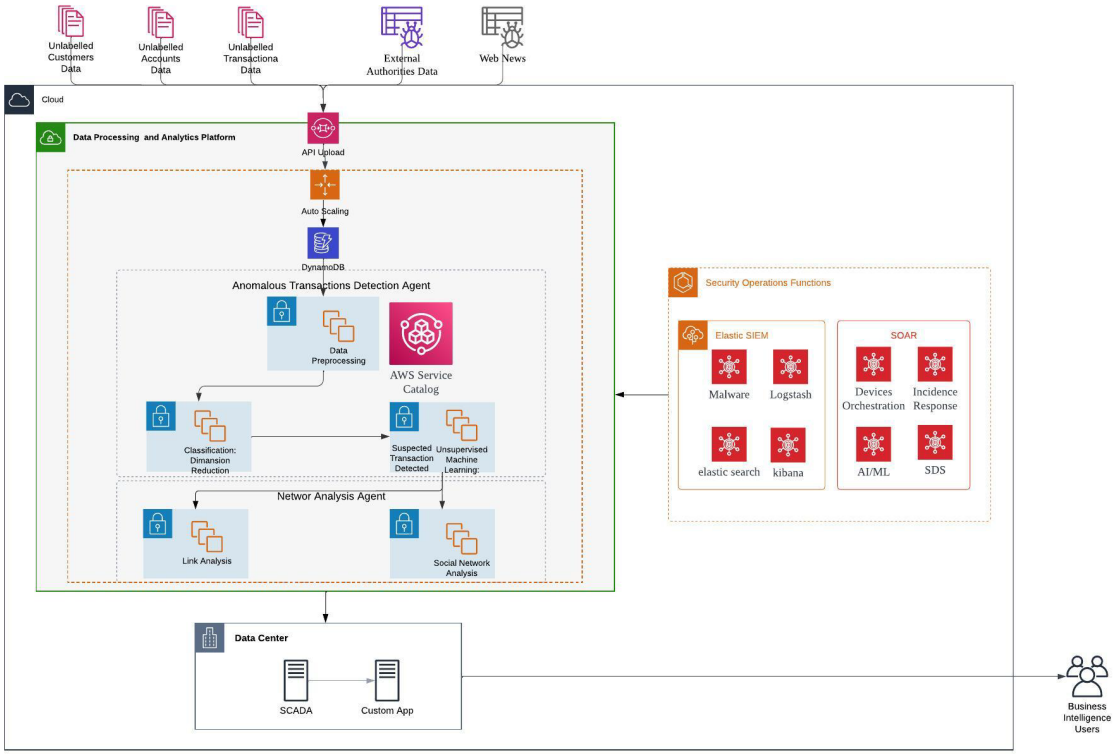

Figure 1: Architecture Design of Automatic Anti-Money Laundering Detection System

4.2.1 Transaction data collection and pre-processing of banking records

The automatic AAMLD system starts from analyzing the suspicious transaction records reported or collected from financial institutions, including banks, insurance companies, trustees, and other investment entities. Generally speaking, 12-36 months of transactions in the accounts are required for training purposes. Basic filtering and pre-processing are deployed to standardize the data formats and to validate the integrity of the data quality from different systems.

4.2.2 Unsupervised algorithms of features extraction

With or without the single label of classifications of the transaction data, unsupervised algorithms are deployed to detect the anomalous transactions from the trained normal transactions. As one type of clustering algorithms, the IPCA based DBSCAN is applied to extract the features of anomalous transactions without the requirement of the predefined labels of the trained dataset.

There are quite a few challenges for solving the Anomalous Transactions Detection problem, and those challenges are mainly related to the limitations of the data collections, which include:

- Imbalanced training dataset.

For most applications, anomaly events with a long time-series data are rare. Generally speaking, data files rarely contain a large volume of normal data and actual anomalous transactions because of the complex scenarios outlined in our case examples. IPCA based DBSCAN, as an unsupervised arbitrary center-based clustering approach, utilizes the density reach ability and the density connection ability to find the optimized center and the radius of each non-overlap clusters when training the unlabeled input data, and detect the anomalous points based on the outliers of any existing clusters of the training.

Because it disregards the normalcy of the dataset input, unbalance will not impact the performance of the algorithm in nature.

- Stability of high performance.

To maintain the high accuracy of detection and prediction, its performance is another issue in real-life application. For example, the Convolutional Generative Adversarial Network and Recurrent Convolutional Autoencoder are capable of achieving high accuracy after sufficient training. However, the stability of the overall predictive performance for each anomality detection is still a concern (Fensel, Dieter, et al. 2020).

Unlike the convolutional neural network etc. deep learning algorithms, IPCA based DBSCAN, as one of the density-based clustering, applies a local cluster criterion. Because of the different methods for regulatory and optimization process, after conducting dimensions reduction using IPCA, DSBCAN adopts the linear optimized calculation of the density and radius and is thus able to achieve the high accuracy once it finds all the clusters after training.

- Hard-coded architecture.

Because different transactions have their own unique signatures, therefore the localized models are required for each different transaction's types or *modus operandi*. DBSCAN in this paper adopts the parameterized architecture instead of hardcoded when defining the radius from the center point to the boundary point ("EPS") and the minimum count of points to define a cluster ("MinPts"). Such self-adapted architecture is able to reduce the dimensionality to the calculated framing for the algorithm to proceed. For different transactions' types, the algorithm will change the temporal of the input data automatically.

Such design, on some level, helps to build auto-localized models to improve the self-adaptability of different money laundering patterns.

4.2.3 Network analysis and data visualization

Based on the results of anomalous transactions detection, such transactions and accounts holders would be filtered out as the entities to set up the network analysis and deduce the money laundering patterns.

The indices of network analysis include: the degree of centrality, which indicates the number of direct connections of one node/vertex in the network; authoritativeness, which is the degree to which one node points to another node via important hubs, and betweenness centrality, which is the measure of the extent to which an actor has control over information flowing between others. During the network analysis procedure, the roles are assigned to nodes in the network, the roles' connections are measured, the entities' mutual proximity are attempted to be determined, and this information to the external role information (e.g., bank statements and the National Court Register) assigned to nodes are compared.

In this article, link analysis and social network analysis are adopted to deduce the process of the money laundering crossing Europe, Hong Kong and China, and identify the roles of the suspicious accounts and account holders in the process. With the auto-construction of the relations between suspicious accounts/account holders, the Network Analysis Agent is able to remove the noise, deduce the money laundering pattern and identify the relationships between suspects. This will be discussed in detail in the results of the experiments.

4.3 The Experiments

4.3.1 The setup

The training data is collected from Kaggle.com (website: https://www.kaggle.com/datasets/ealaxi/paysim1), which only keeps normal transactions. The suspicious transactions are the real data collected from the three cases mentioned in the article, including the eight accounts of Bisley Global, Nice Alpha and Tobo Group in different local banks with different currencies in Hong Kong.

The data classification for anomaly detection is based on the transactions data, including the transaction types, the transaction amount, the balance between the transaction, the balance after the transaction etc. The transaction types include Cash-in, Cash-out, Payment, Debit and Transfer.

In the experiment, the training dataset only includes the normal data downloaded from Kaggle.com, and we randomly pick up 25,000 transactions in the total 65,499 sample normal in 50 times consecutively. The test dataset is from the HK Police, in which we only selected the five attributes to keep consistent with the training dataset. The test dataset includes 200 suspicious transaction records monitored by the banks, which were randomly selected from the total 395 suspicious transaction records and 200 normal transactions data,

totaling at 400. The prediction focuses on the turning point from consecutive 25,000 normal transactions data to 400 mix-up transactions data. Both the train and the test datasets are scaled and normalized.

4.3.2 Performance comparison and analysis

AUC, PAUC, F measure, Accuracy Score, MSE, and Spearman Rank Correlation Coefficient etc. would be set up as the evaluation matrix for performance measures. From the experiment result of 50 random test cases shown in Table 1, it can be observed that when detecting the suspicious transactions of Bisley Global's accounts, the average accuracy is about 0.82, the stability indicators, including Jaccard Score and Spearman Rank Correlation Coefficient are 0.64 and 0.67 respectively. And the detection performance of the suspicious transactions of Bisley Global, which is 26.23% higher than that of Tobo Group. From the result of the experiments, the transactions of Bisley Global are more suspicious for money laundering than those of Tobo Group.

Bisley Global is sentenced for money laundering.

Table 1: Anomaly detection between two suspects

Measurements	Bisley Global	Tobo Group
Number of Test Cases	50	50
AUC	0.82	0.65
PAUC	0.77	0.61
Accuracy	0.82	0.65
MSE	0.18	0.35
Spearman Ranking Correlation Coefficient	0.67	0.37
Jaccard Score	0.64	0.33

4.3.3 Social network analysis

The output generated by the Anomalous Transaction Detection is loaded for the Network Analysis. Based on the classified anomalous transactions and the refreshed data correction and complement from knowledge graph engine, the link analysis and the social network analysis are deployed to set up the relationships between the suspicious accounts and the account holders, and to visualize the money laundering process and pattern.

The social network analysis focuses on the accounts and accounts' holders (customers). And the data classification includes transactions related, accounts related and customer related. Transactions related attributes include Sum-Counts of Transaction, Sumamt and DRCR. Accounts related attributes include target account's ID, target currency, target bank, target region/country, source account's ID, source currency, source bank and source region/country. And Customers related attributes include target name of account holder(s) and source name of account holder(s).

In this case, there are 24 source bank accounts and 86 target bank accounts which are also related to the findings of the Hong Kong Police.

Based on the link analysis of the suspicious accounts shown in Figure 2, several key points could be observed:

- "Bisley Global BVI Co." account of EUR in Bank of China in Hong Kong is the central of the transactions between all accounts.
- "Nice Alpha" is the second centralized entity in the network. The "Nice Alpha" of EUR in Standard Chartered Bank in Hong Kong only receives/sends money with the corporate accounts in Europe and in Hong Kong. The "Nice Alpha" of EUR in Bank of China in Hong Kong transacts with both the individual accounts in China and the corporate accounts in Hong Kong, China and Europe.
- "Tobo Group" of EUR in Standard Chartered Bank in Hong Kong is recognized as another centralized one in the constructed linked network. Similar to the "Nice Alpha" of EUR in Standard Chartered Bank in Hong Kong, this account also transacts only with the corporate accounts in Hong Kong and Europe.

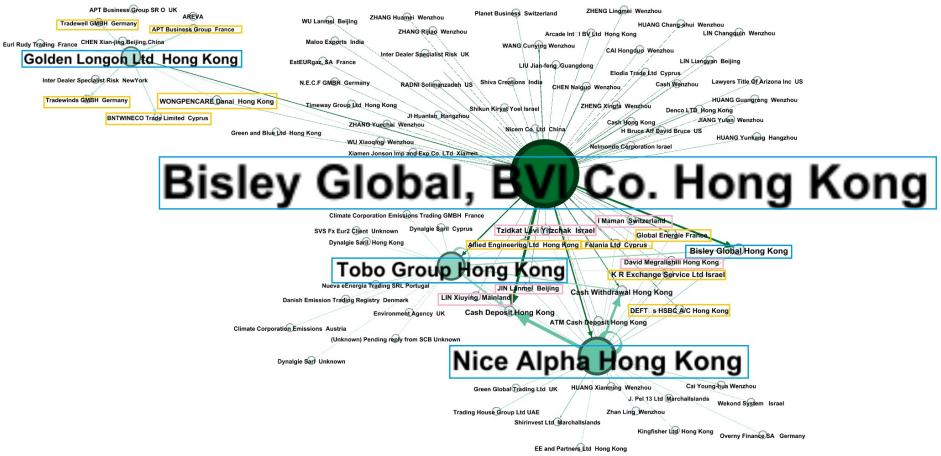

Figure 2: Link Analysis of Suspicious Accounts' Holders

Figure 2 is the link analysis for the suspicious account holders, and the transactions between different accounts are merged if those accounts belong to the same account holder. It shows that there is a cone in the central of the network with the nodes of Bisley Global Hong Kong, Nice Alpha Hong Kong and Tobo Group Hong Kong. In the cone, the direction of the fund is from Bisley Global to Alpha and then to Tobo Group. Except for the transferring out from Nice Alpha to Tobo, there are two other exits: Cash Withdraw and Cash Deposit.

"Golden Longon Limited" of EUR in Bank of China in Hong Kong is observed as another centralized node in the network, but they layered small percentage of the laundered money in the network and only transacted with business accounts in France, Cyprus, or German in Europe.

Bisley and Nice Alpha are charged with money laundering.

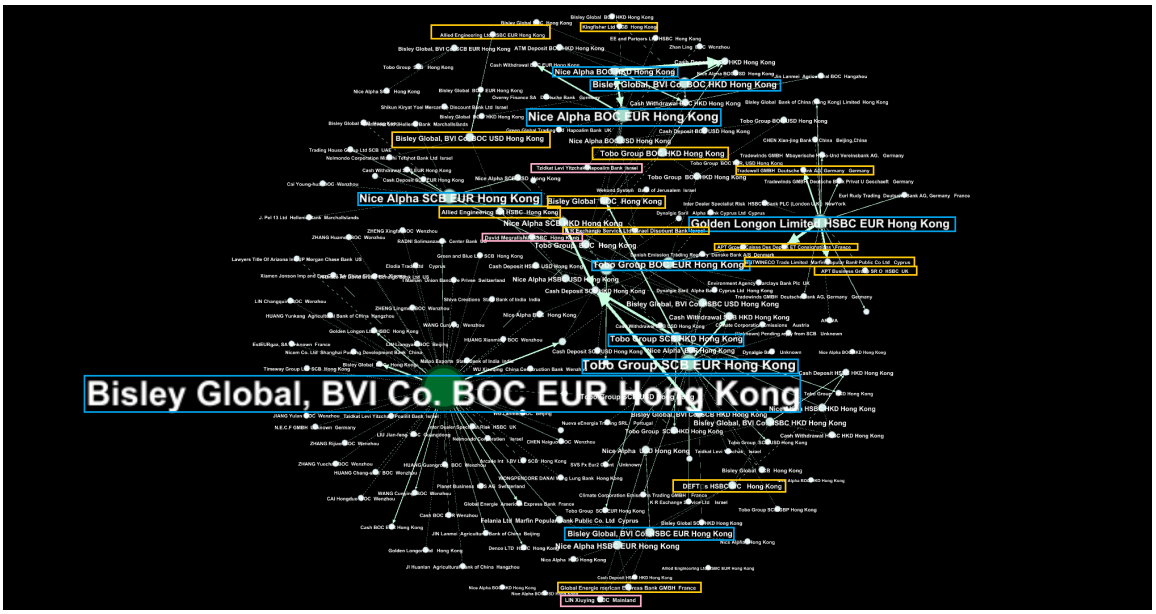

Figure 3: Social Network Analysis of Suspicious Accounts

From the relationship analysis of customers, we extend such analysis to suspicious accounts. Figure 3 shows the hierarchy structure of the accounts, a three tier accounts as follows: -

1. The first-tier accounts are the centralized nodes in the social network. These accounts all belong to the four suspicious account holders: Bisley Global, Nice Alpha, Tobo Group, and Golden Longon. From the narrows of each node of the first tier, it can be observed that these nodes are the main initiators and the main intermediary of the fund flows, because of their high degree centrality and betweenness centrality of other normal nodes. These first-tier accounts are highlighted with the blue frames in Figure 3.

2. Second tier accounts are the accounts which transact with the first-tier accounts more frequently than other accounts. The edges between the first and the second-tier accounts are bolder than those between the first tier and other normal accounts, and most of them are linked to multiple first level accounts. The main observations of second level accounts include:

- Most of the corporation accounts of the second level are from Cyprus, France, Israel, Germany and Hong Kong, e.g.: Felania Ltd Marfin Popular Bank Public Co. Ltd in Cyprus, BNTWINECO Trade Limited Marfin Popular Bank Public Co Ltd in Cyprus, Global Energie American Express Bank GMBH in France, and APT Group Caisse Des Depots ET Consignations in France and UK, etc.
- Three individual accounts work as the connections between Bisley Global and Nice Alpha, and these accounts are from Hong Kong, Israel and Mainland.

3. Finally, the third-tier accounts are the ultimate recipient of the fund, or at least very remote from the first tier account.

5. Conclusion and the Discussion in Future

Automated analysis has yet been widely applied or presented as evidence in criminal proceedings and thus is rarely discussed by the Hong Kong Courts. This section highlights some of the legal implications concerning the admissibility of automated analysis in money laundering criminal cases. In order for the automated analysis to be admissible, one of the criterions must be the genuineness of the underlying raw data such as the inter-account transfers, over-the-counter cash transactions, etc. These raw data should be admissible evidence, supported by a banker's affirmation, under section 20 of the Evidence Ordinance, Cap 8, Laws of Hong Kong (Hong Kong e-Legislation, 2018).

For the purpose of section 20 of Evidence Ordinance, "*any document or record used in the ordinary business of a bank*" includes any report of meeting between the account holder and his banker and credit card sales slip.

Secondly, the software used to generate the automated analysis must be proven to be reliable. The developer should have pre-established models and criteria that are specific and effective, making it possible to identify hallmarks of money laundering in financial activities. The models and criteria should be subject to regular re-examination to ensure that they are reliable and up to date (Westlawasia, 2021).

Since automated analysis should have no or minimal margin of error in processing the raw data, alternatively, the result from the automated analysis should be subject to independent examination by 'non-automated measures' before being tendered for use as evidence in criminal proceedings.

Before employing the software in performing automated analysis, law enforcement agencies may also consider carrying out tests on the software to determine whether it is accurate. Such a test would then provide evidence that the software would then be regarded as reliable in producing automated analysis (Westlawasia, 2012).

In the experiments of anomalous transaction detection, it is observed that the performance of unsupervised anomalous transactions detection achieves 0.82 and is capable to identify the suspicious object from other objects in the real case. However, the volume and complexity of the raw data for the experiments can be improved to mimic the real anti-money laundering environment.

Besides, based on the anomalous transactions' detection engine and the network analysis engine, we expect to set up the knowledge graphs to deduce and enrich the completed money laundering process. Such processes could be mapped to and validated by the admissible evidence, and to be accepted by the court and law enforcement. With knowledge graph engine, the efficiency and accuracy of both anomaly detection and network analysis can be improved continuously. We expect to study on this domain and add more features of Automatic Anti-Money Laundering Detection System in future.

References

Donato Masciandaro. (1999): "Money Laundering: the Economics of Regulation", European Journal of Law and Economics, 7:225–240.

Dre˙zewski, Rafał, Jan Sepielak, et al. (2015): "The application of social network analysis algorithms in a system supporting money laundering detection." Information Sciences 295: 18-32.

Fensel, Dieter, et al. (2020): "Introduction: what is a knowledge graph?" Knowledge Graphs. Springer, Cham, 1-10.

Financial Services and the Treasury Bureau (2023): Hong Kong Money Laundering and Terrorist Financing Risk Assessment Report 2022, Money Laundering Report_2022_EN.pdf (fstb.gov.hk)(accessed 08 Feb 2023).

Gao, Shijia, and Dongming Xu. (2009): “Conceptual modeling and development of an intelligent agent-assisted decision support system for anti-money laundering.” Expert Systems with Applications 36.2: 1493-1504.

Han, Jingguang, et al. (2020): “Artificial intelligence for anti-money laundering: a review and extension.” Digital Finance 2.3: 211-239.

Hong Kong e-Legislation. (2018): Section 20 of the Evidence Ordinance, Hong Kong, Cap. 8 Evidence Ordinance (elegislation.gov.hk)(accessed 09 Feb 2023).

Hong Kong Monetary Authority (2016): Hong Kong, The Global Offshore Renminbi Business Hub, Hong Kong The Global Offshore Renminbi Business Hub (hkma.gov.hk), (accessed 09 Feb 2023).

Khan, Nida S., et al. (2013): “A Bayesian approach for suspicious financial activity reporting.” International Journal of Computers and Applications 35.4: 181-187

Kinyua, Johnson, and Lawrence Awuah. (2021): "AI/ML in Security Orchestration, Automation and Response: Future Research Directions." Intelligent Automation & Soft Computing 28.2.

Lopez-Rojas, Edgar Alonso, and Stefan Axelsson (2016): ”A review of computer simulation for fraud detection research in financial datasets.”2016 Future technologies conference (FTC). IEEE.

South China Morning Post (2014): Israeli soldier convicted for helping money-laundering syndicate, https://www.scmp.com/news/hong-kong/article/1508586/israeli-soldier-convicted-helping-money-laundering-syndicate

Sridharan, Anish, and V. Kanchana. (2022): "SIEM integration with SOAR." 2022 International Conference on Futuristic Technologies (INCOFT). IEEE.

Timesofisrael (2016): How a French-Israeli grifter became a money-laundering pioneer in China, https://www.timesofisrael.com/how-a-french-israeli-grifter-became-a-money-laundering-pioneer-in-china/

Westlawasia (2021): La Quadrature du Net & Ors v Premier Ministre & Ors (2021) 1 WLR 4457. https://launch.westlawasia.com/document/I9C19D40024BD11ECA3D5D6E91F41AA26?srguid=i0ad832f20000018c2b32c34c6e617a61&fromSearch=true&offset=1

Westlawasia (2012): Bevan v Western Australia (2012) WASCA 153. https://launch.westlawasia.com/document/I549a0ff0d7c811e2a455b12f5e340c12?startChunk=1&endChunk=1&fromSearch=true&offset=1

Worlddata (2022): The world's largest economies, https://www.worlddata.info/largest-economies.php.

Xiao, Guohui, et al. (2019): “Virtual knowledge graphs: An overview of systems and use cases.” Data Intelligence 1.3: 201-223.