Egmont Group
of Financial
Intelligence Units

BEST EGMONT CASES

Financial Analysis Cases **2014–2020**

THE EGMONT GROUP SECRETARIAT
Tel: 1 647-349-4116
E-mail: mail@egmontsecretariat.org
Website: www.egmontgroup.org

TABLE OF CONTENTS

Remarks by the Chair of the Egmont Group

This latest edition of the Best Egmont Case Award has been in the making for a long time now — I am certain it is worth the wait.

The BECA is a treasured initiative as it provides FIUs with the opportunity to contribute to the money laundering and terrorist financing case database and share their knowledge, expertise, and experiences within the global AML/CFT community. Although 2020 was a challenging year due to the COVID-19 pandemic, the BECA competition proceeded with great success. I am proud to say that no less than 117 cases were submitted for the period 2014–2020. The Project Team had the difficult task to review all submissions and selected the 26 best Egmont cases across 7 targeted categories of predicate offences and associated ML typologies. The high quality of the submitted cases will make the selection of the winner a very challenging task for the delegates and therefore, I am sure the BECA competition will be one of the high points of the upcoming Egmont Group Plenary again.

With the publication of the 2014–2020 BECA book, readers will observe the evolution of money laundering and terrorist financing typologies and predicate offences through the 26 cases from different jurisdictions around the globe. It brings a lot of learning opportunities to our community: it's a compilation of real cases that FIU's have worked on and where the cooperation amongst ourselves has been crucial to come to results. As such it gives the most perfect description of what the Egmont Group of FIU's is all about.

I extend my sincere thanks to all the FIUs that have contributed to the Best Egmont Case Award (BECA) over the past decade. I also congratulate the Technical Assistance and Training Working Group on the 2014–2020 Best Egmont Case Award book's successful publication.

Mrs. Hennie Verbeek-Kusters
Chair, Egmont Group of FIUs
Head of FIU-the Netherlands

Introduction

The Best Egmont Case Award (BECA) annual competition was developed in 2011 by the Training Working Group — now called the Technical Assistance and Training Working Group (TATWG). The BECA initiative is designed to encourage Egmont members to contribute to the Egmont Group's money laundering and terrorist financing case database to benefit Financial Intelligence Units (FIUs) and stakeholders in anti-money laundering/combatting the financing of terrorism (AML/CFT). The BECAs provide a valuable opportunity for FIUs to share their knowledge, expertise and experiences within the global AML/CFT community.

The competition process starts with a call letter from the BECA Champion to invite all Egmont member FIUs to submit their best cases. To encourage active participation from the FIU members and enrich the BECA database, there is no limit on how many cases an FIU member can submit. In addition, the FIUs may submit cases solely about their own efforts, and they may collaborate to submit cases as a combined effort. Therefore, joint submissions that can best demonstrate the close cooperation between the Egmont Group members are welcomed.

After a given deadline of case submission, a panel of four to six judges scores all cases and determines the two best cases, which would be marked against a set of criteria. The finalist FIUs would then be invited to present their case to the plenary. The Heads of FIU would be asked to vote for the case that they considered as the "best case" and the winner would be awarded the BECA trophy. The BECA has become a tradition and one of the highlights of the Egmont Group Plenary.

Philip Hunkin, a former BECA Champion, envisaged that BECA case submissions could become valuable case studies that could be used as AML/CFT training materials. He proposed highlighting the best of the BECAs in a publication. With the support of the Egmont Group Secretariat, the first BECA Book was published in 2015, which contained 22 of the best case submissions between 2011 and 2013, and has

since become a useful reference for case studies and best practices of FIUs globally.

In 2020, as the HoFIU Ecuador, I stepped in as the BECA Champion to continue this important tradition. The year 2020 marked the 10th Anniversary of the BECAs. However, the COVID-19 pandemic went global just after the launch of the annual BECA Competition and impacted the organization of a face-to-face Egmont Plenary meeting. Despite this, the 2020 BECA competition went ahead and, in fact, it was a great success. There were 24 case submissions from 19 FIUs and the winner was selected through virtual voting. At the same time, with the support of the Egmont Group Secretariat, we decided to prioritize the development of the second BECA publication, which contains the best case submissions between 2014 and 2020.

In this context, in June 2020, a subgroup composed of 12 FIUs was formed and started to review all case submissions. It is a challenging task to scope the selection with regional balance and the diversity of predicate offences associated with money laundering typologies. From among 117 case submissions, the subgroup selected 26 best cases and established the following seven targeted categories of predicate offences and associated money laundering typologies:

1. Bribery and Corruption
2. Cybercrime and Cryptocurrency
3. Drug Trafficking
4. Fraud and Embezzlement
5. Smuggling and Gambling
6. Trade-Based Money Laundering and Third-Party Money Laundering
7. Terrorism Financing, Organized Crime and Human Trafficking

Case Submissions between 2014 and 2020

YEAR	# CASES/# FIUS	THE TWO FINALISTS	WINNER
2014	13 cases from 12 FIUs	AUSTRAC (FIU-Australia)	**FinCEN (United States) and UIF (Mexico)**
		FinCEN (FIU-United States) and UIF (FIU-Mexico)	
2015	12 cases from 10 FIUs	UIAF (FIU-Colombia)	**AMLC (Philippines)**
		AMLC (FIU-Philippines)	
2016	18 cases from 16 FIUs	IMPA (FIU-Israel)	**IMPA (Israel)**
		UIAF (FIU-Colombia)	
2017	12 cases from 10 FIUs	PPATK (FIU-Indonesia)	**Rosfinmonitoring (Russia)**
		Rosfinmonitoring (FIU-Russia)	
2018	19 cases from 16 FIUs	PPATK (FIU-Indonesia)	**SDFM (Ukraine)**
		SDFM (FIU-Ukraine)	
2019	19 cases from 14 FIUs	Rosfinmonitoring (FIU-Russia)	**UIF (Peru)**
		UIF (FIU-Peru)	
2020	24 cases from 19 FIUs	UPK (FIU-Brunei Darussalam)	**UPK (Brunei Darussalam)**
		IVE (FIU-Guatemala)	

ACKNOWLEDGEMENTS

At this stage, I would like to take the opportunity to thank former BECA Champion Philip Hunkin for leading the BECA project from 2011 to 2019, and the judges for their time and efforts in reviewing cases for the BECA competitions.

2014 BECA Panel of Judges

Amar Salihodzic
EFFI (FIU-Liechtenstein)

I. Nyoman Sastrawan
PPATK (FIU-Indonesia)

Nischal Mewalall
FIC (FIU-South Africa)

Sasha Behari
MOT (FIU-Aruba)

Sinclair White
FIA (FIU-Bermuda)

Stefan Lundberg
NFIS (FIU-Sweden)

2015 BECA Panel of Judges

Alejandra Medina
UIF (FIU-Mexico)

Nischal Mewalall
FIC (FIU-South Africa)

Sasha Behari
MOT (FIU-Aruba)

Sinclair White
FIA (FIU-Bermuda)

Stefan Lundberg
NFIS (FIU-Sweden)

2016 BECA Panel of Judges

Abdelsattar Elnajar
EMLCU (FIU-Egypt)

Gustavo Vega Ruvalcab
FIU (Mexico)

Maria Colonnello
UIF (FIU-Italy)

Susan François
FIUTT (FIU-Trinidad and Tobago)

Wilson Alejandro Martinez Sanchez
UIAF (FIU-Colombia)

2017 BECA Panel of Judges

Alejandra Perez
FIU (Mexico)

Amr Rashed
EMLCU (FIU-Egypt)

Maria Colonnello
UIF (FIU-Italy)

Markus Erikson
AUSTRAC (FIU-Australia)

Melanie Gration
AUSTRAC (FIU-Australia)

Michelle Cantwell
AUSTRAC (FIU-Australia)

Sigita Wilson
FIU (New Zealand)

2018 BECA Panel of Judges

Atuweni Agbermodji
FIU (Malawi)

Elżbieta Franków-Jaśkiewicz
GIFI (FIU-Poland)

Gilbert Lee
AMLD (FIU-Taiwan)

Guillaume Ollivr
FIU (Mauritius)

Maria Colonnello
UIF (FIU-Italy)

Sigita Wilson
FIU (New Zealand)

2019 BECA Panel of Judges

Brian Kauzeni
FIC (FIU-Zambia)

Elżbieta Franków-Jaśkiewicz
GIFI (FIU-Poland)

Francisca Brito
UIF (FIU-Angola)

Maria Colonnello
UIF (FIU-Italy)

2020 BECA Panel of Judges

Arnaldo Sanchez Brugal
UAF (FIU-Dominican Republic)

Dominic Offor
FIU (Nigeria)

Elżbieta Franków-Jaśkiewicz
GIFI (FIU-Poland)

Simon Zaugg
MROS (FIU-Switzerland)

Tarun Tapan Tripura
FIU (Bangladesh)

Teale Earner
AUSTRAC (FIU-Australia)

In addition, I would like to take this opportunity to acknowledge the work and effort undertaken in the publishing of the second BECA book by the following FIU officials:

- **Aldo Farfán**, from FIU-Ecuador
- **Andrey Krankov**, from FIU-Russia
- **Elza Robert**, from FIU-Seychelles
- **Maria Paz Ramírez** and **Karina Uribe**, from FIU-Chile
- **Meriton Shoshi**, from FIU-Kosovo
- **Mikko Värri**, from FIU-Finland
- **Nathalie Kläy**, from FIU-Switzerland
- **Sergio Espinoza** and **Paola Gabriela Torres Velez**, from FIU-Peru
- **Soraya Jesus Cardoso**, from FIU-Angola
- **Tafsir Hane**, from FIU-Senegal
- **Javier Alberto Gutiérrez López** and **Alvaro Mauricio Torres Ramirez**, from FIU-Colombia

Also, I would like to recognize **Jérôme Beaumont**, Executive Secretary, and **Michelle Ouyang**, Senior Officer of the Egmont Group Secretariat, for the support we have received from them.

I hope you enjoy reading these excellent case studies and benefit from the successful experiences and impressive cases investigated by the contributing jurisdictions.

Leopoldo Quirós
Head of FIU-Ecuador
BECA Champion
Chair
Technical Assistance and Training Working Group
Egmont Group of Financial Intelligence
2020–2021

The Role of Financial Analysis in the BECAs

Evaluating "Exceptional" in Financial Analysis

The overarching commonality of the selected cases in this book is the exceptional financial analyses undertaken by each of the Financial Intelligence Units (FIUs). The cases presented clearly show how analysts analyzed financial data to form these cases and successfully uncover complex illicit schemes. Often, these cases were generated from piecemeal information provided through a suspicious activity report or suspicious transaction report. FIU analysts took information that may have been overlooked by criminal investigators to piece together schemes that often included multitudes of financial transactions and layered corporate and legal structures. What is remarkable in the chosen cases is how analysts used limited data to trace and unravel multimillion-dollar frauds and other types of financial crimes that spanned numerous countries and even continents.

This publication comprises 26 cases that illustrate the exceptional financial analytical capabilities of the FIUs involved in uncovering various money laundering schemes and predicate offences throughout the world. In determining the best cases, the evaluation undertook a review of the quality and range of analytical tools used and the clarity of how planning was undertaken, data and intelligence collected and collated, and how this was evaluated and presented with the purpose of educating others on successful techniques that solved complex problems.

Leveraging Lessons Learned

No single method of financial analysis is guaranteed to produce results. These cases highlight various approaches taken to analyze financial data from open sources, information provided from other FIUs, financial data from the private sector, and criminal and financial data from criminal justice and regulatory bodies. It is intended that readers can extract from these cases some ideas on the tools that would be best for their investigations and how careful financial analysis planning can lead to excellent results.

In fact, the most important byproduct of this publication is that of an educative tool for FIUs, financial regulators and the entire anti-money laundering structures in the public and private sectors. Publishing these cases is intended to illustrate for anti-money laundering authorities what financial analysis tools were successful in uncovering crimes and how these could be replicated or adapted to local circumstances.

The following cases illustrate how FIUs used investigative and analytical techniques to build successful cases that resulted in confiscation of stolen assets and sanctioning of perpetrators. Crucially, they show how FIUs used intelligence to help gather evidence for building cases through extracting information from a wide array of sources and piecing this together to create a factual narrative of how crimes were committed. It may very well be that some anti-money laundering authorities and FIUs reading these cases have never encountered these types of money laundering. For precisely this reason, it is invaluable that they analyze these cases with an eye toward preparing for the eventual introduction of these types of illicit schemes within their own jurisdictions. Perhaps this forward thinking will help to uncover these types of criminal schemes with greater ease and mitigate potential financial and other damages.

Meriton Shoshi, FIU-Kosovo

This publication comprises 26 cases that illustrate the exceptional financial analytical capabilities of the FIUs involved in uncovering various money laundering schemes and predicate offences throughout the world.

BRIBERY AND CORRUPTION

In the modern world, practically any society or any state is vulnerable to corruption. Moreover, corruption has taken on a pronounced international character, thanks in large part to globalization. While globalization creates economic transparency and the free movement of capital, goods and labour across national borders, it also invites the criminalization of national economies.

Bribery and corruption pursue only personal enrichment and the concentration and retention of power. The principles of corruption include the expression "vicious circle." This means that corrupt officials create a structure of their own kind. Thus, the knowledge that each of these officials is involved in bribery is the basis for this completely vicious structure.

Corruption erodes trust in government and undermines the social contract. The World Bank Group considers corruption a major challenge in ending extreme poverty and boosting shared prosperity for the poorest 40 percent of people in developing countries. Empirical studies have shown that the poor pay the highest percentage of their income in bribes. Some studies have suggested that

the poor may even be targeted since they are seen as powerless to complain. Every stolen or misdirected dollar, euro, peso, yuan, rupee or ruble robs the poor of an equal opportunity in life and prevents governments from investing in their human capital.[1]

In the public sector, it is not just a matter of officials taking bribes to award contracts or favouring friends and family when approving projects. Corrupt officials might also artificially slow down bureaucratic processes to increase their chances for personal enrichment — the longer the queue for a service or the more complicated the paperwork, the higher the incentive for citizens to offer a bribe so they can jump the queue or cut the red tape.

All of these elements underline the need to intensify the global fight against corruption in the interest of ensuring economic recovery, improving services with taxpayers' money and re-establishing public trust around the world.[2]

Efforts to combat money laundering introduced by international organizations and governments of various countries are aimed, in particular, at eliminating the conditions that facilitate the legalization of dirty money. One of these conditions is corruption in the ranks of government officials, representatives of political forces and business.

Making inroads against corruption often requires determined efforts to overcome vested interests. Transparency and open governance are typically part of the story, but rarely the whole story. When popular disaffection with corruption and cronyism reaches a boiling point, the political rewards to addressing corruption can exceed the costs of upsetting interests.

The cases in this section demonstrate how the work and techniques of the Financial Intelligence Units are critical to exposing increasingly sophisticated schemes, such as profiting from the misfortune of bankrupts, using a complex array of offshore accounts to launder bribes, creating a bogus non-governmental organization to disguise a multimillion-dollar pork barrel scam, and leveraging corrupt government officials to win government tenders and then using those contracts to embezzle public funds.

To root out corruption means to create a strong, legal, democratic state that effectively serves society. In fact, the absence of corruption indicates the maturity of civil society, where the majority of the population is free, responsible and creative. Today, the world community is committed to fighting corruption, increasing the requirements for those hired or appointed by state bodies, and implementing various forms of regulation of the relationship of state bodies with the population.

Indicators

- Suspicious cash transactions, including:
  - purchase of high-value items with cash
  - credit card debt paid off in cash
  - large cash deposits made to personal accounts and subsequently transferred to overseas accounts
  - payments made primarily in cash through dummies and intermediaries to obscure the audit trail
- Multiple financial transactions to blur the trail of source of funds
- Use of currency exchanges to remit funds abroad
- Use of multiple offshore companies to blur the audit trail and hide the ultimate beneficial owner
- Use of fake contracts to justify receipt of large sums of money
- Embezzlement of state funds through fake NGOs
- Corrupt government officials receiving kickbacks/commission for facilitating the transfer of state funds

1 World Bank, *Combating Corruption*, Brief, n.d., www.worldbank.org/en/topic/governance/brief/anti-corruption

2 Organisation for Economic Co-operation and Development, *Boosting Integrity, Fighting Corruption*, n.d., www.oecd.org/investment/50350066.pdf

CASE 1

Judges Stealing from Court-Protected Coffers (Brunei Darussalam, AMBD)

Introduction

Two corrupt officers of the court, Ms. RR, and her husband, Mr. NB, abused the power of their positions at the State Judiciary Department to embezzle debtors' funds from Official Receiver accounts.

This case involves 255 Official Receiver accounts related to 234 victims, and more than BND 15.7 million (equivalent to USD 11.1 million) in funds embezzled between 2004 to 2017. These funds were used to obtain premium services and luxuries, including the purchase of at least 19 luxury cars and at least 456 high-value assets such as watches, designer handbags, accessories and shoes, and long-term rental of homes outside of Brunei Darussalam.

The Investigation

The Anti-Corruption Bureau of Brunei Darussalam approached AMBD, the country's Financial Intelligence Unit (FIU), on December 31, 2017, to share information about complaints made against the two judicial officers and to request financial information on them to determine how they were able to afford their lifestyle.

Keywords	official receiver account, magistrate, unexplained wealth, criminal breach of trust, money laundering, international cooperation, domestic cooperation
Countries involved	Brunei Darussalam, United Kingdom, Singapore, Malaysia, Thailand
Sectors involved	banking

Two key types of information became useful in developing the investigation:

1. information on the two suspects' overseas wire transfer activities; and
2. cash transaction reports filed on the suspects.

Between 2011 and 2017, Ms. RR and Mr. NB transferred an equivalent of BND 1,374,212 to their accounts in Country A. Ms. RR and Mr. NB usually travelled to that country after these transactions were made.

Open-source information indicated that Ms. RR and Mr. NB had a significant presence in Country A. Their social media platforms indicated that they were living at their own residence in Country A, and drove their own vehicles. Early feedback from Country A's FIU indicated that the properties thought to be owned by the suspects were all rental properties.

AMBD also sought the cooperation of countries B, C and D to obtain information that would refute the suspects' claims made that their sources of wealth were legitimate, and to help trace the funds.

The information gathered from overseas wire transfers proved that their existing assets within their country of residence (that could only have been purchased overseas) were in fact purchased using embezzled funds and, therefore, were proceeds of crime.

Furthermore, Brunei Darussalam has two types of cash transaction reports (CTRs). The first is a threshold-based report that financial institutions and designated non-financial businesses and professions, as well as motor vehicle dealers, must complete for transactions exceeding a certain amount.

The second type of CTR is a currency notes transaction report: banks are required to file reports on all transactions involving BND 10,000 (equivalent to USD 7,000) or SGD 10,000 currency notes. These reports record the transactor's details and the serial number of the note. This type of reporting was intended to mitigate the risk of money laundering through the use of this large denomination note.

Based on these records, AMBD found several transactions spread over several years involving the withdrawal of large amounts of cash from debtors' accounts at one bank. Further assessment of the CTRs and investigation indicated that Ms. RR was able to withdraw large amounts of cash from the debtors' accounts without arousing suspicion by using her status and position of authority to release funds.

A significant portion of the cash withdrawn from the Official Receiver accounts were subsequently traced to deposits to Ms. RR and Mr. NB's joint personal savings account at another bank. The currency notes CTRs were able to link the serial numbers of cash withdrawn from the Official Receiver accounts to the cash deposited to the judicial officers' personal savings account.

In addition, further tracing revealed that a portion of the serial numbers of currency notes withdrawn from the Official Receiver accounts had the same serial numbers as those reported by motor vehicle dealers for deposit to their corporate accounts. CTRs received from car dealers on the car purchases and CTRs filed on car dealers from banks were successfully linked and the cars owned by the judicial officers were identified as proceeds of crime.

Analysis of the flow of funds using serial number tracing enabled the investigators to secure concrete evidence that the two judicial officers were illicitly obtaining money from debtors' accounts, transferring it to their personal accounts, and using it for personal gain.

The couple was charged for **CRIMINAL BREACH OF TRUST BY A PUBLIC SERVANT**, **MONEY LAUNDERING** and **POSSESSION OF UNEXPLAINED PROPERTY**.

FIU Action

AMBD collaborated with the Anti-Corruption Bureau and banks very closely throughout the intelligence gathering and investigation. This collaboration was facilitated by the early appointment of designated individuals at each agency who were preauthorized to exchange information without delay whenever possible. This close contact between AMBD and Anti-Corruption Bureau officers helped reinforce mutual trust and also enabled the relevant authorities to act as quickly as possible to ensure that embezzled funds were not further dissipated or hidden.

Furthermore, AMBD made use of Egmont Group connections and sent requests for information to four other relevant countries as part of the money trail assessment.

Evolution of the Case

The case took only one week from the start of official investigations until seizure of the suspected proceeds of crime. The entire process of intelligence gathering, investigation and prosecution took almost 24 months, which is astounding for law enforcement.

A key factor in speeding the intelligence gathering and investigation stage was the discovery of critical links based on threshold-based and currency note CTRs.

Outcome/Contribution of the Case

On January 15, 2020, Ms. RR and Mr. NB were convicted. Ms. RR was found guilty on all charges of **CRIMINAL BREACH OF TRUST BY A PUBLIC SERVANT** and **MONEY LAUNDERING** while her husband, who was facing eight charges of **MONEY LAUNDERING**, was convicted of six charges and acquitted of two due to insufficient evidence.

Ms. RR and Mr. NB faced a further charge of **POSSESSION OF UNEXPLAINED PROPERTY**. The proceedings for these charges were initially stayed but the stay was lifted after the initial trial was completed. The prosecutors have not announced their decision on whether to pursue these charges.

Appeals filed by Ms. RR and Mr. NB were scheduled to be heard in December 2020.

Valuable indicators of the case

- Car purchases paid in cash, including BND 10,000 notes
- Credit card debt paid off in cash
- Deposits via automated teller machines conducted at an unusual hours (such as close to midnight) to avoid being noticed by the bank's counters
- Large cash deposits made to personal savings account are subsequently transferred to overseas accounts under the senders' name(s)

CASE 2

Exposing the Politically Exposed (Peru, FIU-Peru)

Introduction

A former senior official in one of Peru's most important state-owned enterprises was a politically exposed person (PEP) at the time of the events.

The PEP allegedly received bribes from a Latin American transnational company through payments to his account through an offshore company that had been set up by the PEP just over a month before receiving these funds. The funds were transferred to different accounts in four countries. These accounts belonged to the PEP's immediate family or to companies linked to them (**CONVERSION AND TRANSFER ACTS**). The funds were used to buy real estate (**ACTS OF CONCEALMENT AND POSSESSION**).

The Investigation

The case was sparked by a news report that the PEP had received a bribe from a Latin American transnational company of approximately USD 1,300,000, through an account in Country A.

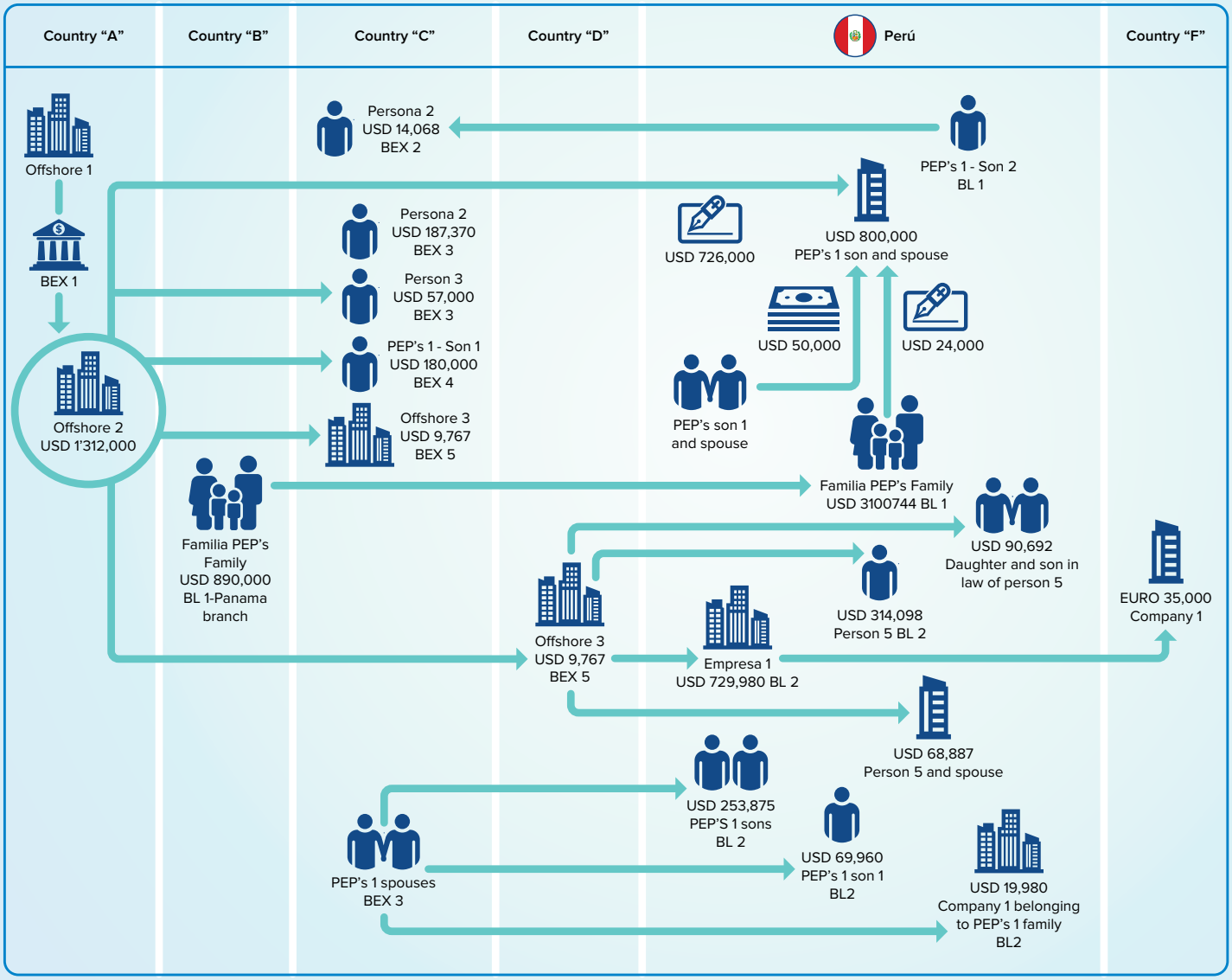
Keywords	politically exposed persons, bribery, corruption, money laundering
Countries involved	Peru
Sectors involved	banking

To corroborate the claim, the Financial Intelligence Unit in Peru (FIU-Peru) requested further information from counterpart Financial Intelligence Units (FIUs) in Country A and Country B. Once received, the information allowed FIU-Peru to identify the first links between those involved in the case and the initial money trail, detecting that the money had allegedly gone to Country B, Country C and Country D, and that it was being mostly transferred to accounts belonging to the PEP's immediate family and to offshore companies owned by them. In addition, it was identified that Offshore 1, which received the bribes, had been established in Country B and that Offshore 3 and Offshore 4 had been established in Country E.

With the information obtained from Country A, FIU-Peru requested further information from its counterparts in Country B, Country C, Country D, Country E and Country F, and from a Peruvian bank (Bank BL 1), seeking to identify the links between those involved and the destination of the funds that allegedly came from the **PAYMENT OF BRIBES**. Similarly, information was requested from the main Peruvian banks; FIU-Peru also researched open data sources and internal databases for the same purpose. This identified the economic activity and assets of the investigated PEP and his affiliates, and allowed the rationality of the funds to be evaluated.

The analysis of this information identified that the money came mostly to Peru and was used to acquire real estate and vehicles. However, one property was located in Country G, which prompted a request to said country for information to identify who uses the property and inquire about other properties that those involved could have had in Country G. Furthermore, it was determined that Offshore 3 belonged to the PEP and his wife, and that Offshore 4 belonged to a Uruguayan citizen and his wife, the former having worked in the same economic sector as the PEP.

CHART 1: MONEY FLOW THAT ALLEGEDLY CAME FROM THE PAYMENT OF BRIBES

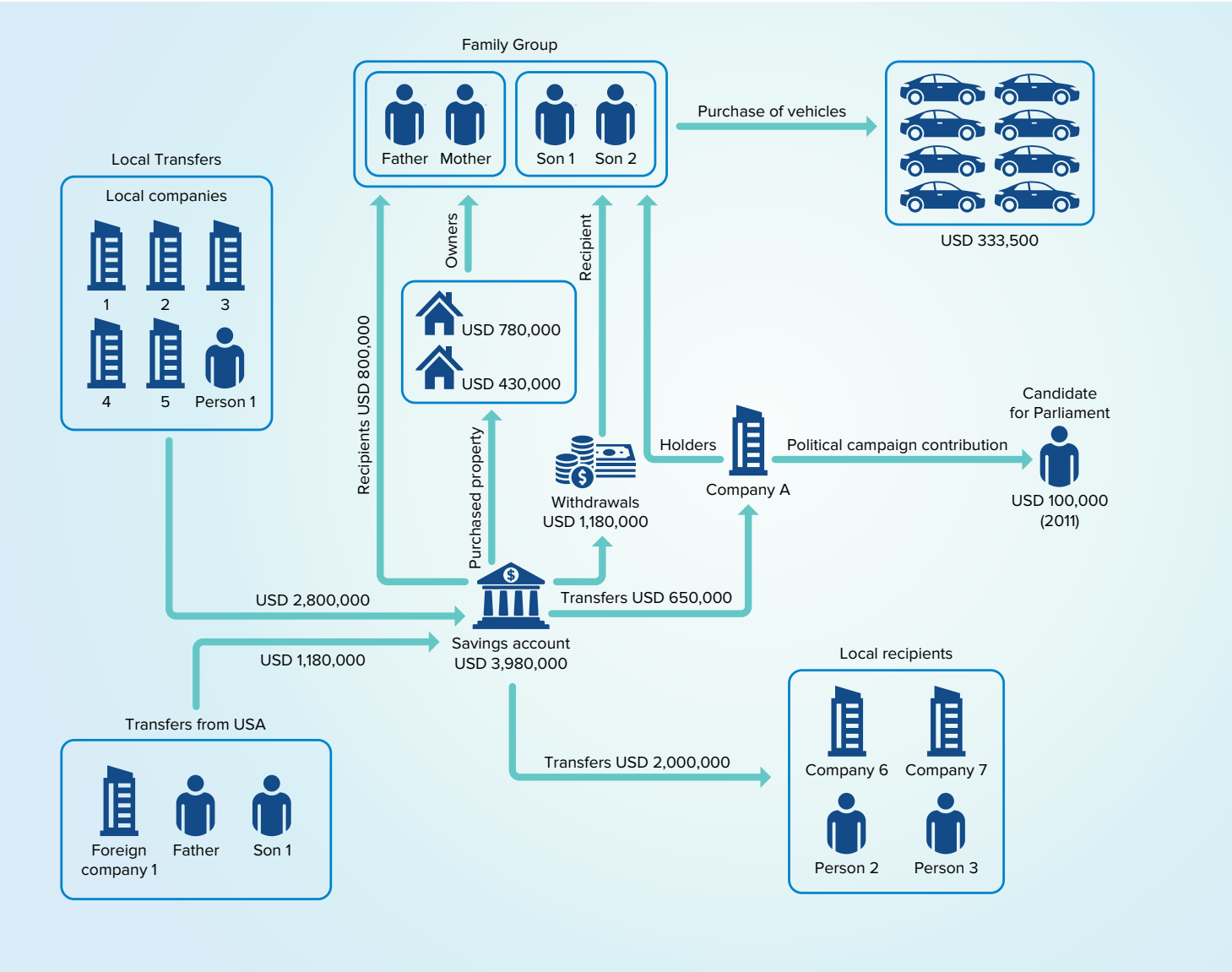


Source: Peru´s supervised entities. Own Elaboration

The money laundering process of funds of illicit origin is shown in Chart 1.

Information obtained from Bank BL 1 identified approximately USD 3,980,000 of unknown origin. These funds were transferred to local accounts owned by the PEP's immediate family and used to acquire real estate and vehicles in the names of the members of that family. These funds were also used to finance a candidate's campaign for the Andean Parliament.

CHART 2: COMPLEMENTARY MONEY FLOW OF FUNDS WITH AN UNKNOWN ORIGIN



The flow of funds with an unknown origin is shown in Chart 2.

The PEP and Son 2 are being investigated for MONEY LAUNDERING for having received USD 1,312,000 in the account located in Country A, which belongs to Offshore Company 1 established in Country B; both the PEP and Son 2 appear to be beneficial owners for this account. This money was transferred to different accounts in Country C, Country B and Country D, and later some of it arrived in Peru and was used to acquire a property in the name of the PEP's Son 1 and his wife, as well as a property in the name of Person 5 and his wife (both Uruguayan citizens).

This case is significant, first, for the sophistication of the money laundering techniques used. More important, however, is that the case is part of more sweeping investigations that have led to a regulatory change in Peru regarding the criminal liability of legal persons (specifically, in public administration crimes) and the obligation of public officials to inform the public of the beneficial owners of their accounts. Both these changes seek to reduce the risks of corruption and money laundering. In addition, FIU-Peru's analysis was vital identifying new linkages, which broadened the government's ongoing investigation and helped to trace the money flow. Furthermore, in coordination with the Public Prosecutor's Office, the investigation was expanded to include more people and new sources that generated illicit funds.

FIU Action

Domestic Cooperation

FIU-Peru requested information from the main Peruvian banks in order to identify transactions carried out by those involved with or those acting on behalf of the PEP. As a result of the requests, three of these banks ultimately submitted information, and subsequently reported suspicious transactions to FIU-Peru. This information allowed FIU-Peru to identify the money flow in Peru and the part of the funds used to acquire real estate both in Peru and Country G, in addition to the purchase of vehicles.

After submitting the financial intelligence report to the Public Prosecutor's Office, FIU-Peru had a meeting with the prosecutor in charge of the investigation of the PEP, in an effort to prompt a complementary evaluation to extend the investigation to four companies linked to the PEP, as well as to the original sources of the money.

International Cooperation

- The information obtained from FIU-Peru's counterparts in Country A and Country D allowed FIU-Peru to identify the money flow that is suspected to come from the payment of bribes as well as the beneficiaries of two bank accounts.
- The information of FIU-Peru's counterparts in Country B and Country E allowed FIU-Peru to identify the shareholders of the offshore companies involved.
- The information provided by Country G allowed FIU-Peru to determine that the PEP and the PEP's family did not have other properties or accounts in that country.
- The information provided by Country F allowed FIU-Peru to locate minor money transfers made by the Uruguayan citizens involved.

Evolution of the Case

FIU-Peru issued two financial intelligence reports by compiling, collating and analyzing the information received.

In the first report, financial operations abroad were identified through offshore companies linked to the PEP. The information provided by the countries involved was crucial for the development of the second financial intelligence report, which allowed FIU-Peru to complete the money trail and know which local banks received these funds, the final beneficiaries in Peru, and the final destination of these funds.

Additionally, the fluid coordination with the Public Ministry (Attorney General) allowed the investigation to be extended to new parties and other sources of money allegedly of illicit origin.

This case demonstrates the contribution of FIU-Peru's work in money laundering investigations carried out by the Public Prosecutor's Office.

Outcome/Contribution of the Case

The information was delivered to the Public Prosecutor's Office and has been included in the prosecutor's money laundering investigation against the PEP and Son 2. In this case, the judge ordered a restrictive measure against the main parties involved, which has prevented the PEP and Son 2 from leaving the country for 12 months.

The case also helped FIU-Peru to identify specific weaknesses regarding the money laundering prevention system of one of the reporting entities. In turn, this prompted FIU-Peru to strengthen its supervision mechanisms of the systems in place for preventing money laundering by reporting entities.

Valuable Indicators of the Case

- Establishment of offshore company to receive alleged bribes
- Simulation of a private real estate sale contract to justify the receipt of the money transferred by the Latin American transnational company
- Diversion of funds of unknown origin to finance a candidate's campaign for the Andean Parliament, transferring funds from the account of the PEP's immediate family in BL 1 to the account of a company owned by the PEP and then paying advertising expenses for the candidate
- Transfer of funds to bank accounts mostly owned by members of the PEP's immediate family and companies under their names

CASE 3

The Pork Barrel Scheme (Philippines, AMLC)

Introduction

As one of the biggest corruption cases in recent Philippine history, this case stemmed from complaints filed with the Office of the Ombudsman by the National Bureau of Investigation (NBI) for plunder, malversation, direct bribery, and graft and corrupt practices related to the use of Philippine legislators' pork barrel allocations. Had this case remained undetected, billions more would have been lost from the country's coffers through corruption.

This case highlights how the Anti-Money Laundering Council (AMLC), which is the Philippines' Financial Intelligence Unit (FIU), plays a vital role in tracing, freezing and seizing proceeds of corruption.

The Investigation

The Priority Development Assistance Fund (PDAF), popularly called "pork barrel," was a lump-sum discretionary fund granted to members of Congress for spending on projects. Members of the House of Representatives received an annual PDAF allocation of PHP 70 million (approximately USD 1.5 million), while every senator received an annual allocation of PHP 200 million (approximately USD 4.4 million)

Keywords	Philippines; AMLC; plunder; bribery; corruption; malversation; PDAF scam; pork barrel scam; NGOs; ultimate beneficial ownership; UBOs; large cash transactions; money changers; MSBs; high-value real estate
Countries involved	Philippines and United States
Sectors involved	Banks, MSBs, Insurance Products, NPOs

The PDAF or pork barrel scam was the alleged misuse by several members of the Philippine Congress of their PDAF allocation by funding agricultural "ghost" projects. These projects were primarily concocted by Ms. N and implemented through her companies, with projects producing no tangible output. Funds would be processed through fake foundations and non-governmental organizations (NGOs) established under the wing of Ns. N's Group of Companies (holding company of Ms. N), with her employees—including a nanny—named as incorporators or directors. Each foundation or NGO had a number of bank accounts where PDAF funds would be deposited, withdrawn by Ms. N's employees and eventually split among Ms. N, the lawmaker (40–60%), the official of the implementing agencies responsible for facilitating the transfer of funds (10–15%), and the local mayor or governor.

Some of Ms. N's employees eventually became whistleblowers, agreeing to expose the scam and testify against Ms. N. They alleged that the legislators who were complicit in the scam were usually paid in cash, through their chiefs-of-staff or other representatives. Consequently, plunder and corruption charges were filed against Ms. N, her employees, officials of the implementing agencies, and lawmakers, including three prominent senators.

The financial analysis and investigation conducted by the **AMLC** based on the predicate offence of **BRIBERY** and **CORRUPTION** confirmed that pork barrel funds were released to Ms. N's bogus NGOs through the implementing government agencies and that the kickbacks to the legislators were paid in cash in an attempt to obscure the money trail.

While Ms. N denied involvement in the scam and/or any connection with the involved NGOs, the bank documents examined by the AMLC belied her claim.

The cheques paid to the NGOs and the withdrawal slips contained handwritten notes made by bank employees that prior confirmation was sought from Ms. N before the transactions were effected. It was also observed that: (1) the transactions in the accounts of Ms. N, her companies and her employees involved transactional amounts not commensurate with their declared business, financial or earning capacity, and sources of income; and (2) the bank accounts of the NGOs were used merely as pass-through accounts since deposits and withdrawals of the same amount were made on the same date or the next banking day.

The financial analysis and investigation also showed that for one senator, cash deposits were made to various bank accounts and investments totalling more than PHP 87.6 million (approximately USD 1.95 million) from 2006 to 2010. The cash deposits were made within 30 days from the dates the senator allegedly received PDAF commissions. During the same period, cash deposits totaling more than PHP 27.7 million (approximately USD 615,000) were also made to NCDR Corporation, a company owned and controlled by the senator's wife, which apparently had no operations as it did not file financial statements with the Philippine Securities and Exchange Commission.

In relation to the funds received by Ms. N from the scam, the investigation revealed that aside from the use of bank deposits, investments in variable insurance, prime real estate and expensive motor vehicles, Ms. N also laundered the funds by using two money service businesses (MSBs) to remit more than USD 5.26 million to the United States to the accounts of two companies owned by her daughter and brother.

FIU Action

The AMLC conducted financial analysis and investigation on the covered transaction reports (for cash or equivalent transactions that exceed PHP 500,000) and suspicious transaction reports involving the bank accounts of Ms. N, her companies and employees, the implementing government agencies, and the lawmakers involved in the scam.

In August and November 2013, the AMLC filed Petitions for the Issuance of Freeze Orders against the bank accounts, investments, real properties and motor vehicles of Ms. N, her companies and her employees, which were granted by Court of Appeals. In February and June 2014, the AMLC filed Petitions for Civil Forfeiture before the Regional Trial Court in Manila against the said properties. These petitions led to the issuance of Asset Preservation Orders to cover the following:

1. Funds and investments totalling more than PHP 155 million (approximately USD 3.4 million);
2. Dollar bank accounts totalling approximately USD 697,000;
3. 47 real properties; and
4. 16 motor vehicles.


Noy, Singapore leader discuss defense cooperation

THE PHILIPPINE STAR

TRUTH SHALL PREVAIL

Be talked about with DEVANT TV

[redacted] assets frozen

Source: https://www.pressreader.com/philippines/the-philippine-star/20140404/page/5

In the course of its investigation, the AMLC coordinated with the NBI and the Office of the Ombudsman, providing them with pertinent bank documents for their investigation of the predicate crimes. For purposes of forfeiture, the AMLC also sought and received information from the Land Transportation Office, Land Registration Authority and numerous Registries of Deeds to determine the ownership and acquisition by Ms. N and her family members of real and other personal properties.

The AMLC also coordinated with the U.S. FinCEN and acted on the Mutual Legal Assistance Treaty request from the U.S. Department of Justice for the production of documents in relation to the seizure and eventual forfeiture of the properties of Ms. N and members of her immediate family in the United States, which were acquired while the pork barrel scam was ongoing.

Evolution of the Case

The scam was exposed in March 2013 when NBI agents rescued Mr. BL, a trusted aide and distant cousin of Ms. N, who later turned out to be the key witness in unlocking the pork barrel scam. Mr. BL had been illegally detained by Ms. N after she learned that the former was planning to establish his own business using a similar scheme to the one Ms. N herself had devised.

On September 16, 2013, NBI filed complaints with the Office of the Ombudsman for **PLUNDER**, **MALVERSATION**, **DIRECT BRIBERY**, and **GRAFT AND CORRUPT PRACTICES** against three incumbent senators and five former congressmen, their chiefs-of-staff or representatives, the heads and other officials of three implementing government agencies, Ms. N, several presidents of the NGOs set up by Ms. N, and private individuals. The complaints filed by the NBI were used by the AMLC as the main basis for financial analysis and investigation.

Outcome/Contribution of the Case

Ms. N was convicted of **PLUNDER** in December 2018. In February 2021, she and one of the representatives were convicted of **GRAFT** and **MALVERSATION**. Her assets are currently frozen and subject of civil forfeiture cases for eventual confiscation in favour of the Philippine government.

As a result of several cases questioning the constitutionality of the PDAF, the Supreme Court of the Philippines ruled that the PDAF was unconstitutional for violating the constitutional prohibition against lump-sum allocations for projects.

Valuable Indicators of the Case

- Use of NGOs for Money Laundering — NGOs are generally viewed as at-risk to terrorism financing. This case shows that NGOs, which were supposedly formed for laudable objectives, have been misused and exploited for the perpetration of other equally heinous crimes, such as large-scale corruption.
- Ultimate Beneficial Ownership — Both Ms. N and the lawmakers (i.e., senators and congressmen involved) used dummies and intermediaries through employees and friends to provide a layer of anonymity. These dummies and intermediaries typically received the funds in cash and transacted with the banks and other financial institutions on behalf of Ms. N and the lawmakers.
- Large cash transactions — The lawmakers preferred to receive their kickbacks in cash through dummies and intermediaries to obscure the audit trail.
- Use of MSBs to remit funds abroad — Ms. N avoided using banks by using her trusted MSBs to transfer funds to the United States to her daughter and brother.
- Purchase of high-value real estate and other property abroad — With the funds transferred to the United States, Ms. N laundered the proceeds through the purchase of high-value real estate (e.g., condominium at the Ritz-Carlton, a 63-room hotel in California, etc.) and personal property (e.g., luxury car, stock shares, etc.).

CASE 4

State Contracts for Construction Objects of Federal Importance Scheme (Russia, Rosfinmonitoring)

Introduction

The Federal Financial Monitoring Service of the Russian Federation (Rosfinmonitoring) worked with Russian authorities to conduct a financial investigation targeting individuals suspected of being part of an organized criminal group and embezzling public funds allocated for state-run construction and installation projects.

By leveraging corrupt contacts in several ministries, members of the criminal group kept winning government tenders and embezzling allocated public funds. The proceeds gained were not only spent on bribes but were also invested in the multisectoral holding structure owned by the criminals.

The Investigation

In its capacity as Russia's Financial Intelligence Unit (FIU), Rosfinmonitoring received several suspicious transaction reports (STRs) from credit institutions detailing suspicious activity in the accounts held by company Alpha. Analysis of the STRs and the statements on the Alpha-owned accounts made Rosfinmonitoring analysts suspect the misuse of public funds.

Keywords	embezzlement, laundering of public funds
Countries involved	Russia, Latvia, Estonia, Cyprus, United Arab Emirates and Switzerland
Sectors involved	construction, banking

As well, a law enforcement agency approached Rosfinmonitoring in connection with the preliminary investigation of the possible **EMBEZZLEMENT OF PUBLIC FUNDS** under a government contract for the construction of a facility for Russian ministry M1. According to the information provided by the law enforcement agency, Alpha had been awarded the contract and senior Alpha employees colluded with officials from ministry M1 to embezzle public funds.

Rosfinmonitoring began by checking all contracts for construction and installation works carried out for ministry M1. The probe revealed that a vast majority of these contracts had been awarded to company Alpha. It also revealed that a significant amount of funds received by Alpha came in the form of advance payments made under government contracts for work carried out for Russian ministry M2. At the same time, Rosfinmonitoring discovered that the contracts with Alpha were not concluded directly by the ministry, but instead were signed by the state-run company Delta, which had been specifically set up by ministry M2 to carry out federal construction projects.

To verify the validity of the suspicions, Rosfinmonitoring analyzed the ways Alpha had spent the funds allocated under the largest government contracts for the work carried out for ministries M1 and M2. The audit exposed a large number of mutual transactions between companies Alpha, Beta and Gamma. A detailed review of bank statements and founders' relationships revealed that companies Beta and Gamma were integrated, albeit unofficially, into the same holding structure, and they were engaged in economic activities that duplicated the activities of company Alpha.

The law enforcement agency also provided Rosfinmonitoring with operational information that showed the beneficial owner of company Alpha was Ivan Ivanov, the owner of a large construction holding company, who was connected to the director of the state company Delta, Petr Petrov. The latter, in turn, had previously run several business entities of the construction holding company. Moreover, Delta's tendering committee was headed by a former employee of the holding company that included shares for companies Alpha, Beta and Gamma.

To support increasing evidence of conspiracy by state officials aimed at embezzlement of public funds, Rosfinmonitoring, working closely with law enforcement, collected and systematized information on the rate of fulfillment of government contracts awarded to companies Alpha, Beta and Gamma. The intelligence gathered exposed the facts of embezzlement of public funds, as well as corrupt intentions of the management of the state-run company Delta, which had deliberately concluded government contracts with its affiliates.

Further analysis of Alpha, Beta and Gamma account statements delivered at the request of Rosfinmonitoring made it possible to identify the first link in the money laundering chain: numerous shell entities that had received more than EUR 200 million of public funds for carrying out fictitious works under government contracts.

According to the audit performed by Rosfinmonitoring, the funds had been transferred to the accounts of numerous entities involved in the activities of professional money laundering centres located across Russia. With the help of Rosfinmonitoring, the Bank of Russia and law enforcement authorities, the identified money laundering centres were subsequently closed and the licences of the credit institutions operating these centres were revoked for violating Russia's anti-money laundering law.

Approximately EUR 75 million of the revealed criminal income was converted into cash by the professional money launderers.

About EUR 50 million of the criminal income was transferred to several credit institutions under contracts for the purchase of promissory notes.

Rosfinmonitoring sent requests to banks for information on transactions with the identified promissory notes. The data provided revealed the final link in the money laundering chain: the promissory notes purchased with criminal income were ultimately redeemed by company Zeta, which was managing the finances of the holding company owned by Ivan Ivanov.

The rest of the money, at least EUR 80 million, was siphoned off overseas through transnational money laundering centres. To uncover the remaining pieces of the money laundering scheme, Rosfinmonitoring requested the assistance of its Latvian colleagues, who, having been informed about the offence committed in Russia, froze about EUR 1 million in the account of the company owned by one of the investigated individuals.

FIU-Latvia provided Rosfinmonitoring account statements for the affiliated Latvian companies Sigma, Epsilon and Tau, which revealed that the criminal group used these Latvian companies as cash accumulators. The funds transferred to the account of company Sigma were subsequently accumulated in the account of company Tau, beneficially owned by the key suspect — Ivan Ivanov.

To complete the laundering of the criminal proceeds, the funds were placed in a security deposit held with a Latvian bank under a trust agreement. Then, within a few days of each deposition of new funds to the security deposit, the bank issued a loan in the amount of the deposited funds to the Russian company Omega that, like Zeta, managed the finances of the holding company owned by Ivan Ivanov. The amount of loaned funds totalled about EUR 65 million, which were subsequently invested in Russia. In the end, EUR 70 million from the security deposit was transferred under assignment contract to settle the loan issued to the company Omega.

FIU Action

During the course of the investigation, Rosfinmonitoring identified:

- the scheme for the embezzlement of funds allocated under the investigated government contracts;
- the scheme for laundering criminal proceeds in Russia through the use of cash and promissory notes;
- the scheme for laundering criminal proceeds siphoned off overseas by means of a loan issued by a Latvian bank;
- the individuals involved in criminal activities along with the affiliated organizations; and
- the assets in possession of the members of the criminal group (i.e., movable and immovable property, including foreign-based, and businesses).

Rosfinmonitoring asked for additional information related to the cash flow of companies affiliated with the perpetrators. This information identified the main financial assets of the individuals involved in the criminal case, as well as an incident of laundering at least EUR 65 million through a Latvian bank. The European Central Bank has already liquidated this bank.

In accordance with the procedure provided by Russian law, the intermediate and final results of the financial investigation, as well as banking secrets, were made available to law enforcement agencies in the form of analytical references and diagrams. The investigation findings were used to charge the suspects with the creation of a criminal community.

Rosfinmonitoring provided its facilities for joint working meetings with the representatives of various Russian law enforcement agencies involved in the investigation and criminal prosecution of the suspects. This ensured effective coordination of the ongoing proceedings, as well as consensus on the mechanism used to commit predicate offences and the subsequent money laundering.

While working on the case, Rosfinmonitoring maintained contact with a total of 15 foreign FIUs from the following countries: Austria, British Virgin Islands, Bulgaria, Cyprus, Estonia, Finland, France, Germany, Israel, Italy, Latvia, Monaco, Switzerland, United Arab Emirates and United Kingdom.

Intelligence received from foreign FIUs made it possible to identify foreign assets belonging to the suspects — including a country house valued at EUR 5 million and numerous motor vehicles — and cash held in the suspects' and their relatives' accounts.

Evolution of the Case

As part of the financial investigation conducted by Rosfinmonitoring, an alleged scheme used for laundering of about EUR 200 million has been identified, including at least EUR 65 million laundered abroad with subsequent transfer of these funds into the territory of the Russian Federation.

The investigative authorities have completed their investigation, and the criminal cases are being tried. Authorities obtained, including with the help of Rosfinmonitoring, irrefutable evidence of the involvement of the perpetrators in this case, forcing them to admit their guilt in a number of incidents and to cooperate with the investigators. Among those already convicted are a high-ranking public official from ministry M1, as well as one of the deputy heads of the state-run company Delta.

The trials of the main suspect, Ivan Ivanov, and the head of the Delta organization, Petr Petrov, as well as other related individuals, are still ongoing.

Outcome/Contribution of the Case

This case represents an excellent example of a comprehensive financial and corruption crimes investigation. Triggered by STRs that dealt with possible embezzlement of public funds allocated for state construction works, the investigation led to the detection and dismantling of an interregional corruption network whose beneficiaries used the illegally obtained funds to further their own business interests.

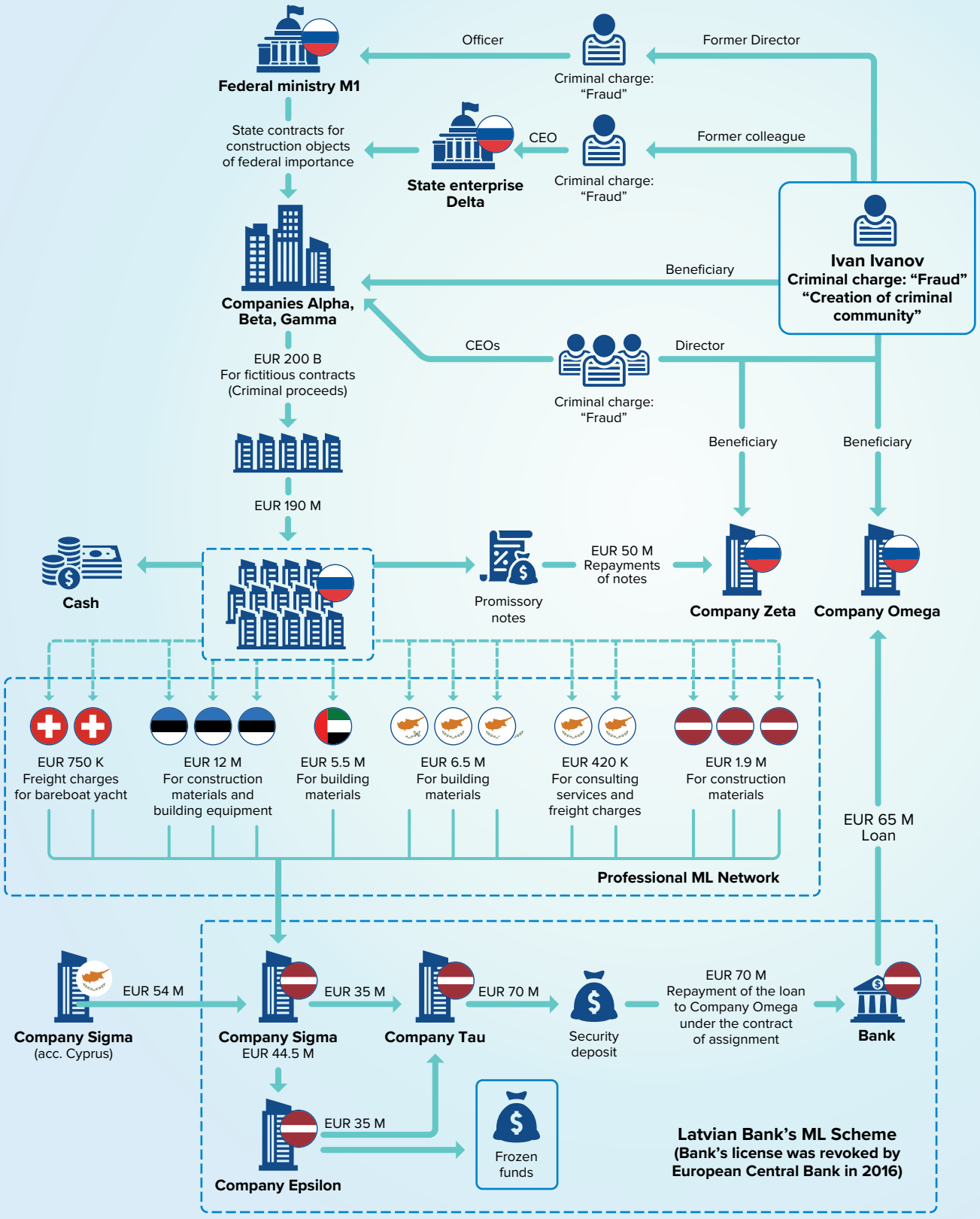
The success of this investigation has largely contributed to safeguarding economic stability in Russia by preventing the holding beneficiaries from using their “dirty” money and corrupt relationships for further subduing competition.

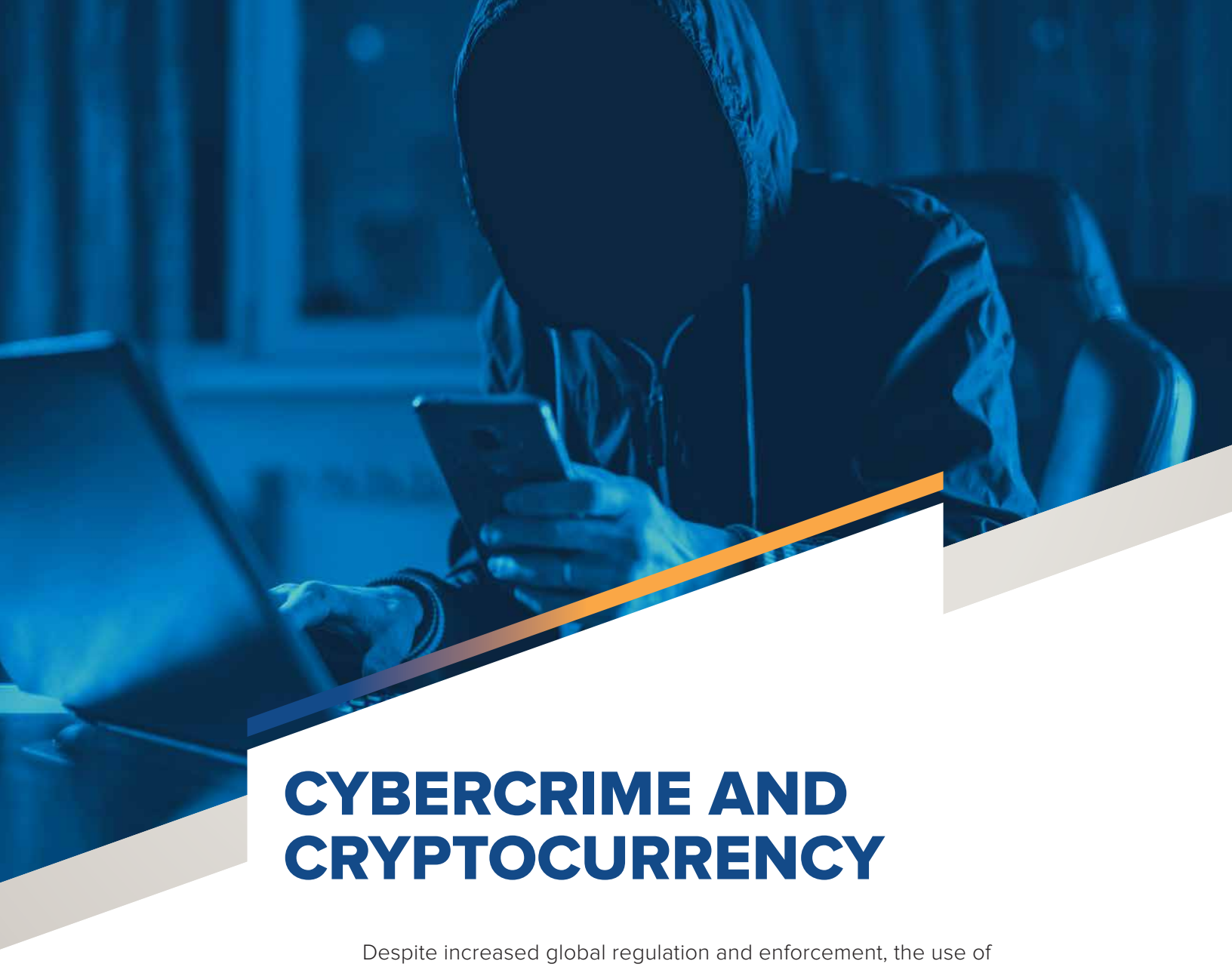
Special attention should be given to the scheme identified by Rosfinmonitoring with the help of FIU-Latvia related to money laundering abroad. The international cooperation undertaken within the framework of the Egmont Group helped to uncover a highly significant money laundering scheme that involved financial institutions from several jurisdictions. Thus, this investigation demonstrates the effectiveness of the global anti-money laundering system. In fact, Rosfinmonitoring continues to work closely with FIU-Latvia. With an interaction system already established, FIU-Latvia has been able to provide information on all Russian organizations that are involved in money laundering through Latvia’s banks.

Valuable Indicators of the Case

- Unusually high number of contracts awarded to the same company or group of companies
- Use of foreign banks
- Use of advance payments for government work
- Relationships among officials of companies and ministries

ANALYSIS OF ML NETWORK





CYBERCRIME AND CRYPTOCURRENCY

Despite increased global regulation and enforcement, the use of cryptocurrencies in illicit trade and money laundering activities grows each year. Preventing cyber criminals from exploiting the global financial system is a fundamental priority for the Egmont Group and its members.

Historically, money laundering has been mostly associated with organized crime and the illicit drug trade. The current rise in the use of new technology and cryptocurrencies, however, has not only simplified illicit online trade but has also boosted cyber-based fraud.

Furthermore, gaps in government regulation and control has driven investors and criminals alike to see these markets as a potential haven to invest, and as a way to commit cybercrimes and avoid asset forfeiture in the event of intervention by law enforcement agencies.

Worldwide, governments are struggling to develop regulatory frameworks to address the rise in popularity in cryptocurrencies while determining how to address digital currency from a tax, asset and monetary policy perspective.[3]

It is important to highlight that the Financial Action Task Force revised its standards in June 2019 to mitigate the risks virtual assets pose for money laundering and terrorism financing. Virtual asset service providers must now implement a full range of preventive measures against these crimes.[4]

Meanwhile, in the following scenarios, FIU efforts uncovered frauds using virtual assets, carrying out SWIFT heists and operating business email compromise schemes, among others. These criminal activities affect financial institutions, expose the financial sector to billions of dollars in losses worldwide, and compromise business or personal email accounts by sending false payment instructions and other information to conduct financial fraud.

Financial institutions can play an important role in identifying, preventing and reporting these criminal fraud schemes by strengthening communication and collaboration with law enforcement agencies.

FIUs are encouraged to work collaboratively with financial institutions and law enforcement to help recover funds for victims by quickly disseminating information related to suspected financial fraud. Quick action on the part of victims, financial institutions and law enforcement agencies, and, critically, the international exchange of information, contribute to the successful recovery of victim funds.

The FIU a plays a vital role within this process as demonstrated in the following cases. Not only in freezing funds, but also in identifying the relevant authorities within their jurisdiction to reach out to. The particular nature of cybercrimes, and the constant development of virtual assets and their use in particular, make the exchange of information between FIUs key to combat this types of crimes.

Indicators

- Crimes that involve multiple jurisdictions
- Use of smaller financial institutions
- Regulatory weaknesses
- Extended statutory holiday which attracts cybercrime
- Fraudster usually registers a domain similar to a legitimate business to fool the target
- Business email compromise schemes usually appear as if they came from the chief operating officer, chief executive officer or senior management to transfer funds into a “changed” bank account
- Funds are transferred to a recipient in the company who the victim has never dealt with in the past
- Transfers are initiated near the end of day or just before weekends or public holidays
- The receiving account does not have a history of receiving large funds transfers in the past
- The receiving account is a personal account

3 Dennis Desmond, *Cryptolaundering: Optimising Cryptocurrency Laundering Interventions* (Doctoral dissertation, University of the Sunshine Coast –USC – Queensland Australia), November 20, 2020, https://research.usc.edu.au/discovery/fulldisplay/alma99489107702621/61USC_INST:ResearchRepository

4 *FATF Report to the G20 Finance Minister and Central Bank Governors on So-called Stablecoins*, June 2020, www.fatf-gafi.org/publications/fatfgeneral/documents/report-g20-so-called-stablecoins-june-2020.html.

CASE 5

Unprecedented Global Multibillion Cryptocurrency Euro Fraud (Kosovo, FIU-Kosovo)

Introduction

The CUMA case is the first successful stand-alone money laundering indictment and prosecution in Kosovo involving a global multibillion-dollar crypto-currency fraud, OneCoin. It resulted in the largest single confiscation of assets ever, totalling nearly EUR 1 million, which was upheld by the appellate court. It was initiated only two months after Kosovo was admitted to Egmont and succeeded due to cooperation with 17 Egmont Group members. The entire case from filing of the suspicious transaction report (STR) to the court verdict was completed in a record time of 18 months.

The Investigation

The case was initiated on the basis of an STR submitted by a bank. The Financial Intelligence Unit (FIU) in Kosovo followed up with qualitative analysis of the individuals and companies listed. After this, tactical cooperation with the reporting entity led to further intelligence that was used to build a case against the company and the owners.

Keywords	money laundering, cryptocurrency, fraud, tax evasion
Countries involved	Kosovo, Denmark, Germany and Poland
Sectors involved	banking, precious metals and precious stones trade

Through the STR, FIU-Kosovo determined that there were three entities: two international websites and one local entity, CUMA, which had four shareholders: two Kosovo nationals and two Danish citizens who opened CUMA, the Kosovo-registered company, offering online tutorial packages for investing in the cryptocurrency OneCoin.

Data from police, taxation and Business Registration Agency databases did not provide information that tied the involved persons to money laundering or other related offences. Through searching open sources, FIU-Kosovo found that the Danish citizen owed debts to the Danish tax and other authorities, as well as a criminal record. FIU-Denmark confirmed this.

Preliminary analysis of financial activity revealed that OneCoin at the time was not considered a pyramid scheme, although there were warnings for customers issued by some authorities (BaFin in Germany, and from Bulgaria, Italy and the United Kingdom). Nonetheless, FIU-Kosovo opened a case and scored it with a prioritized high risk.

FIU-Kosovo continued to use open sources to find more information on the websites that CUMA's owner provided to the bank: onelife.eu and nbh.ea. This information and the STR led FIU-Kosovo to uncover the connection between OneLifeNetwork Ltd. and OneCoin.

FIU-Kosovo then discovered the Facebook profile for one of the local owners and analyzed his fingernails in photos, which indicated that he was a manual labourer and likely a house painter or construction worker. FIU-Kosovo in collaboration with the bank decided to check if this person has any knowledge related

to education packages or to information technology products. When the customer visited the bank, the customer failed to respond convincingly to the bank's due diligence and know-your-customer techniques.

In the meantime, FIU-Kosovo gathered information on the mother company and the main suspect, OneLifeNetwork Ltd., and found it is registered in Belize. The financial monitoring authority in Belize issued a warning that the company is not registered to do trading, and any trading with this entity was considered an offence.

FIU-Kosovo requested information from 17 FIUs through the Egmont Secure Web and determined that customers who were purchasing the products were being defrauded.

From April to mid-July 2017, FIU-Kosovo collected bank information in Kosovo, Kosovo customs information related to the involved entities, 17 international responses through FIU-Kosovo's Egmont Secure Web requests confirming CUMA was part of a global fraud, and taxation and customs authorities information. This information was not enough to convince the Special Prosecution to issue a sequestration order.

To meet the requirements of the prosecutor, FIU-Kosovo developed a strategy based on the account of one of the suspects. On July 21, the balance of this account was EUR 907,406. The suspect had not declared any financial activity in the account. If the suspect failed to declare any financial activity by August 1, then the entity would be committing a **TAX FRAUD** offence. On July 26, FIU-Kosovo was informed that the suspect entity was attempting an outgoing transaction through e-banking. FIU-Kosovo gave permission to the bank for e-banking transactions up to EUR 5,000 and to then pretend that the bank has a cyber security problem. FIU-Kosovo asked the bank to keep in contact with the suspect through email and to try to delay until August 1 so that a **TAX EVASION** charge could come into effect.

On July 28, FIU-Kosovo received information from that bank that the suspect wanted to transfer EUR 858,000 to a jewellery shop in Denmark with the intention to buy precious metals. Through further cooperation, FIU-Kosovo instructed the bank to ask the suspect to provide documents of the jewellery shop and gather as much information as possible. On July 31, the suspect requested to do the transaction while FIU-Kosovo was coordinating in real time with the bank. The bank asked the suspect for an invoice for the transaction to proceed; he provided a copy of an invoice sent by email from the Danish suspect. This invoice was the missing piece of the puzzle — the beneficial owner listed was OneLifeNetwork Ltd. Belize, the entity that was not licensed to do trading and, according to Belize authorities, every trading transaction with that entity was an offence.

Ilustrim

Vëllezërve kosovarë u konfiskohen 1 milion euro

Kastriot Berisha 03.2.2020 - 16:36

Gjykata e Apelit ua ka vërtetuar dënimet dy vëllezërve, FMS, të cilët akuzoheshin për shpëlarje të parave.

https://kallxo.com/lajm/vellezerve-kosovare-u-konfiskohen-1-milion-euro/

With this information, FIU-Kosovo was able to determine that CUMA was being used as a cover company or mule to funnel money via a jewelry shop in Denmark to the beneficial owner of OneCoin. In this money laundering scheme, the fraudsters moved funds from multiple jurisdictions that, they had assumed, had poor bilateral cooperation tools given that Kosovo is not a member of the United Nations or INTERPOL, nor recognized by a number of these jurisdictions. They were mistaken. Just months prior, Kosovo had been admitted to the Egmont Group.

FIU-Kosovo issued a 48-hour freezing order on the account involved in this activity. The total sum frozen by FIU-Kosovo's order was EUR 946,000. The prosecution office issued a sequestration order and indictment, in close cooperation with FIU-Kosovo, that explained the nature of the stand-alone **MONEY LAUNDERING** offence and the use of multiple jurisdictions and corporate vehicles to hide the offence.

FIU Action

After gathering information through FIU-Kosovo's databases, an FIU analyst proceeded to check open sources and conduct background checks and discovered that the two nationals had no experience in information technology and the two foreigners were Danish citizens, one of whom had a previous conviction for tax evasion and illegal weapons possession in Denmark. Through a request sent through the Egmont Secure Web, this information regarding the Danish nationals was verified. FIU-Kosovo requested information from all banks operating in Kosovo about any transactions made by CUMA or the individuals involved, as well as a request to the Tax Administration for information about the financial activity declared by the company.

Further analysis revealed warnings from numerous countries about both OneCoin and OneLifeNetwork. OneCoin was advertised as a cryptocurrency and had billions of euros of investments from throughout the world through education packages on how to invest once the company began publicly selling its OneCoin currency. Climbing on the back of other well-known cryptocurrencies during this global fad, OneCoin advertised itself as an upcoming investment goldmine, and was featured in business magazines and conferences throughout the world. OneLife was directly linked to OneCoin. Its business was specifically selling education packages on how to become an investor in the OneCoin cryptocurrency. CUMA was selling identical education packages developed by OneLife for the purpose of investing in OneCoin. However, this cryptocurrency was one huge global fraud, and Kosovo was one of the puzzle pieces being used precisely because of the perceived lack of bilateral cooperation with non-recognized states and non-membership in INTERPOL, the United Nations and other multilateral bodies.

Evolution of the Case

FIU-Kosovo coordinated extensively with taxation and customs authorities during the information gathering process. Once the case was submitted to the Special Prosecutor and the freezing order was issued, FIU-Kosovo continued to work with the Special Prosecutor. FIU-Kosovo was instrumental in advising the Special Prosecutor in issuing a stand-alone money laundering charge, which, for the first time ever in Kosovo, resulted in convictions by the courts and upheld on appeal.

The CUMA case resulted in EUR 1 million in confiscated assets upheld on appeal for Kosovo's first ever stand-alone money laundering case involving a global multibillion euro cryptocurrency fraud, OneCoin. Analyses involved open source investigation, excellent tactical cooperation with the private sector, the prosecution, and taxation and customs authorities, and invaluable exchange of information involving 17 Egmont Group members just months after Kosovo was admitted into the Egmont Group.

Outcome/Contribution of the Case

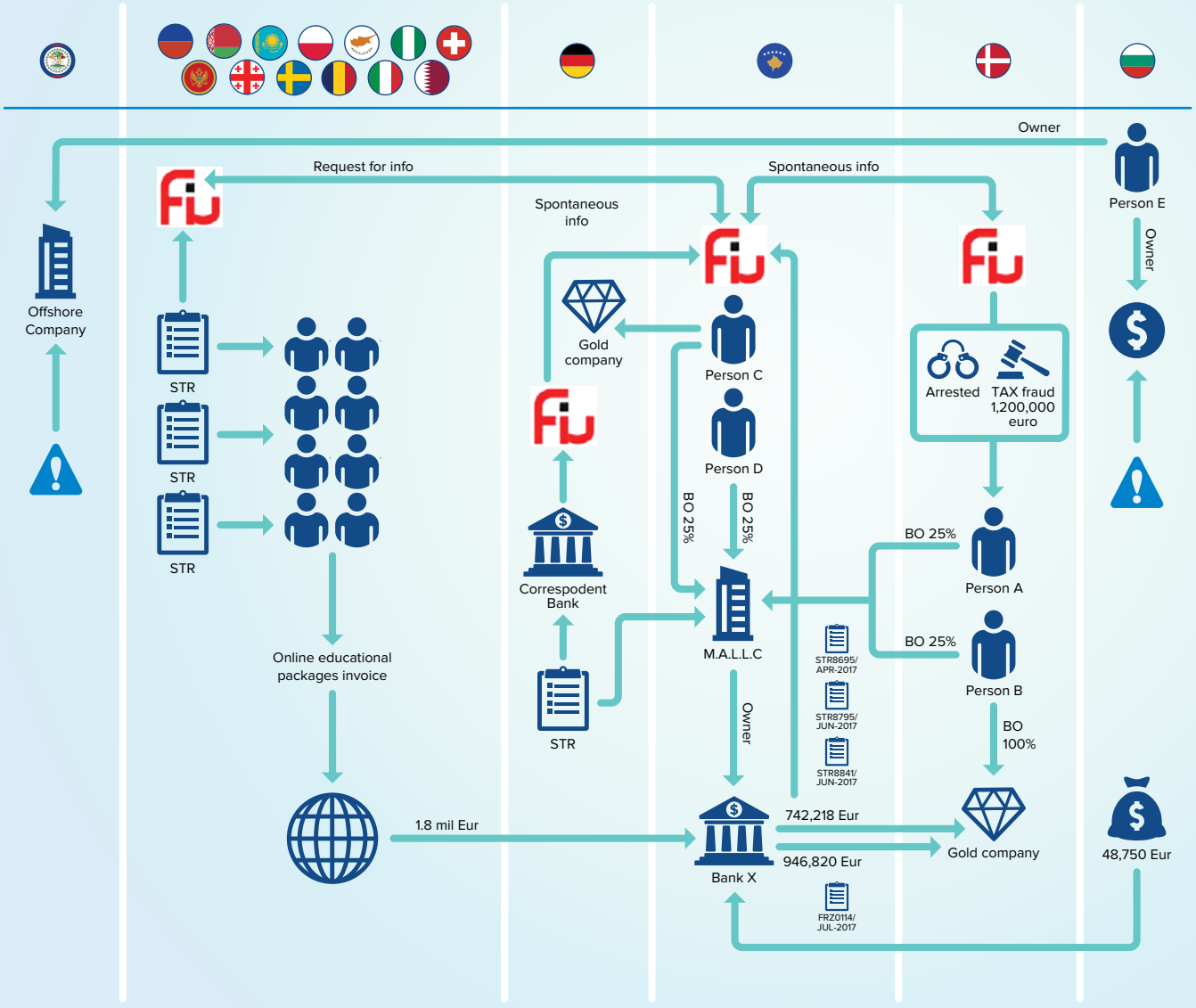
The two Kosovo nationals were sentenced to 2.5 years probational sentence, nearly EUR 1 million was confiscated from them and arrest warrants were issued for the two Danish nationals. Kosovo, through its Ministry of Justice Department for International Legal Cooperation, has been proactive in reaching out to other countries whose citizens are victims of this fraud in order to compensate those victims with the confiscated funds.

To date, Kosovo has been working with Poland and Denmark on compensating their citizens who have fallen victim to this fraud.

Valuable Indicators of the Case

- Movement of funds through multiple jurisdictions
- Suspected pyramid scheme

ANALYSIS OF ML NETWORK



CASE 6

Cyber Attack Through a SWIFT Heist (Nepal, FIU-Nepal)

Introduction

Cyberthieves routed 33 unauthorized transactions using eight different Nostro accounts of XYZ bank, a large commercial bank in Nepal, by hacking the bank's SWIFT interbank messaging service in October 2017.

Funds totalling NPR 465.70 million (about USD 4.5 million) were transferred to 21 different international bank accounts in nine different countries, namely China, Germany, Japan, Hong Kong, Malaysia, Turkey, Singapore, the United States and the United Kingdom.

XYZ bank submitted a suspicious transaction report (STR) to Nepal's Financial Intelligence Unit (FIU) immediately after the heist happened. FIU-Nepal immediately informed the central bank of Nepal and also sought international support via Egmont Group.

The Investigation

Hackers initiated the transactions during a great festival holiday in Nepal, Deepawali/Tihar, which took place October 18–20 in 2017. The information technology team of XYZ bank found that a SWIFT server was not working and suspected that the SWIFT server had crashed. The team attempted to recover the data from the crashed server. Trade Operation staff logged into the SWIFT system and checked the outward SWIFT messages and found 31 SWIFT messages that were not executed by the Trade Operation team. The Compliance team logged in to the SWIFT sanction screening system and found that 10 out of 31 transactions were blocked so they immediately declined the transactions. Central Remittance team logged into the Internet banking service for the Nostro system and found that some transactions had already been debited from Nostro accounts and confirmed that the SWIFT system had been compromised.

Keywords	banking fraud, SWIFT hack
Countries involved	Nepal, Japan, China, Turkey, Hong Kong, Malaysia, Germany, United States, United Kingdom and Singapore
Sectors involved	banking, financial

XYZ bank then asked the banks of the Nostro accounts to stop the payments and refund the money. The bank also filed an STR with FIU-Nepal and informed the head of the FIU (HoFIU) by telephone as well. FIU-Nepal immediately opened a case file and attempted to use the Egmont Secure Web to notify the Egmont Group, but was stopped due to technical issues. A separate email was then sent to the FIUs of the countries involved. At that time, FIU-Nepal contacted foreign counterparts via telephone and other means of communication. The HoFIU received phone calls even at midnight and he discussed all the details and strategies for the return of the funds. FIU-Nepal also informed the central bank of Nepal about the case; as requested by the FIU, the central bank immediately sent the inspection team to the XYZ bank for further investigation. Then the case was referred to the Central Investigation Bureau, a special investigation division of the Nepal police, for joint cooperation to recover the funds from various national agencies, international agencies and central banks.

In addition to this, the XYZ bank itself approached KPMG to investigate the case. KPMG found that the fraudulent SWIFT transactions were made using the bank's user accounts that had been compromised by external attackers as part of a highly complex, multi-layered cyberattack. Forensic analysis of available artefacts suggested that the cyberattack consisted of:

- executing scripts to gain entry to the bank computer systems and network;
- using key loggers to install malware and spread mass infection;
- launching brute force attacks on the email infrastructure; and
- wiping key operating system files from the bank's SWIFT servers after execution of the transactions to make them inaccessible and to avoid early blocking of the SWIFT transactions by the bank.

As part of the **CYBERATTACK**, the hackers compromised the Windows operating system credentials of multiple users, including the network administrator, accounts used for creating requests of SWIFT transactions, accounts used to verify transaction requests, and the USB keys used to carry out anti-money laundering checks and provide approvals. Reverse connections of the malware identified the IP addresses, which belonged to Romania. The KPMG report observed that the cyberattack on XYZ bank was similar to the SWIFT heist of a Taiwanese bank.

FIU Action

After receipt of the information and the STR, FIU-Nepal immediately informed the central bank of Nepal about the case, asked the central bank to send the inspection team in the field and reported the case to domestic law enforcement agencies.

FIU-Nepal then created the case file and notified the Egmont Group via Egmont Secure Web and, through separate emails, the FIUs of the affected countries. All available means of communication were used that day. The HoFIU even received phone calls at midnight and he discussed all the details and strategy for the return of funds.

Within a few hours of being notified, Financial Crimes Enforcement Network (FinCEN) mobilized all U.S. resources. FinCEN provided additional support by calling affected FIUs, countries and law enforcement agencies.

As a result of all these efforts, the bank informed FIU-Nepal immediately that most of the funds were blocked in the respective accounts in respective countries.

FIU-Nepal asked the FIUs in the affected countries for refunds and also coordinated with the Nepal Police Central Investigation Bureau for joint cooperation to return the money.

Evolution of the Case

In October 2017, a highly complex, multilayered cyberattack used XYZ bank's compromised user accounts to make fraudulent SWIFT transactions. The hackers routed 31 unauthorized transactions from eight different Nostro accounts of the bank through unauthorized access to the SWIFT system. Funds were transferred to 21 different international bank accounts in nine different countries.

Outcome/Contribution of the Case

This case is an excellent example of solving banking fraud and SWIFT scams. With the joint efforts of XYZ Bank, FIU-Nepal, Nepal's central bank, law enforcement authorities, foreign FIUs, and other national and international agencies, 85% of the funds were successfully recovered. If FIU-Nepal had not handled the case quickly and carefully, a total of around NPR 466 million might have been available to be used in other criminal activities. Timely detection of the fraudulent transactions and immediate actions taken by the bank and external stakeholders, mainly FIU-Nepal, were the key factors in this level of recovery.

This SWIFT heist case also demonstrated the importance of the FIU's close cooperation with domestic and international counterparts for combatting financial criminal activities. The sizeable recovery would not have been possible without support from FIU-Nepal, foreign counterparts, banks, embassies, foreign officials, etc. Leveraging policy-level international connections for investigations will help lower the impact of financial crime.

Valuable indicators of the case

- Extended statutory holiday, which attracts cybercrime — criminals might take of advantage of targets not being connected to the system due to long holidays or other reasons.
- Crime that involves several different countries — combatting money laundering activities can be more effective if the resources of every country are brought together under a single umbrella

CASE 7

Global Money Laundering Related to Virtual Assets (Poland, FIU-Poland)

Introduction

The Bitfinex case concerns global financial operations related to virtual assets and a shadow banking ecosystem servicing all types of criminal activities. Several companies were established so they could set up accounts in a number of small cooperative banks; they conducted debit operations out of a large international bank, however. Using cryptocurrencies and sophisticated money pooling, the suspects were able to launder funds originating from drug trafficking among other illicit activities. The case involved cooperation among 16 Financial Intelligence Units (FIUs).

The significance of the case for the Polish jurisdiction is related to the volume and value of the operations (USD 380 million in frozen assets) and use of the weaker part of the banking sector for illegal activity (cooperative banks operating outside major financial centres).

The Investigation

FIU-Poland received its first request related to the suspect, Mr. XXX, in February 2015 from a foreign FIU. The main case, however, related to Mr. XXX and two Polish companies, AAA SP. Z O.O. and BBB SP. Z O.O. The companies, represented by Mr. XXX and registered in September 2016, made many transfers for Bitfinex. After two months, the companies started active fund transfers. For incoming funds, they used 70 bank accounts in small cooperative banks outside Warsaw; at the same time, they used a second big international bank in Warsaw for debit operations. Some time between June and November 2016, Mr. XXX created another foreign company, CCC CORP, and acted as its representative. This company performed similar activities as the other two companies.

Keywords	drug trafficking, cybercrime, cryptocurrencies
Countries involved	Brazil, Canada, Denmark, Germany, Gibraltar, Greece, Ireland, Netherlands, Hong Kong, Latvia, Lithuania, Mexico, Panama, Poland, Switzerland and United Kingdom
Sectors involved	Banking

FIU-Poland's investigation of AAA SP. Z O.O. and BBB SP. Z O.O. started with suspicious activity reports (SARs) received from two leading commercial banks in Poland and one local cooperative bank in the July 2016 to January 2017 period. Seven SARs were filed related to the entities.

In January 2017, law enforcement authorities were notified.

In May 2017, FIU-Poland received a request from a foreign FIU outside the European Union related to a few entities, including the key legal entity in FIU-Poland's main case, AAA SP. Z O.O. The main subject of this request was the activities of DDD LLC, a fourth company based outside Poland, which performed the type of activities carried out by AAA SP. Z O.O. in the iFinex/Bitfinex/Tether group.

In September 2017, FIU-Poland received a request from the District Prosecutor's Office related to the key entities in the main case. This request was the result of the previous notification of law enforcement and/or notification by the local cooperative bank to the Local Prosecutor's Office, which passed the case to the District Prosecutor's Office.

In December 2017, FIU-Poland sent a request to the FIU outside the European Union related to three incoming transfers to AAA SP. Z O.O. that totalled USD 14 million.

In January 2018, FIU-Poland froze four incoming transfers to AAA SP. Z O.O. of a total value of USD 20 million and froze the company's bank accounts. There was evidence the origin of the money was diversified: partly sourced from drug trafficking and illegal trade on the dark web. The money laundering technique used cryptocurrencies and very sophisticated money pooling involving a large number of bank accounts.

As the part of freezing procedure, FIUPoland sent a complex notification to the District Prosecutor's Office with a description of the evidence together with related alleged offences (**MONEY LAUNDERING** related to **DRUG TRAFFICKING AND ILLEGAL TRADE WITH ILLICIT GOODS IN DARK WEB**). The same month, FIU-Poland sent requests for information to 13 other FIUs in Brazil, Canada, Denmark, Germany, Gibraltar, Hong Kong, Latvia, Lithuania, Mexico, Panama, Switzerland, Turkey and the United Kingdom.

Since then, information continues to be exchanged with Polish Police, prosecutor's offices, other foreign FIUs, taxation authorities, the banks involved and the Polish Financial Supervision Authority. The exchange of information consists of, among other things, supplementary notifications for the District Prosecutor's Office, incoming SARs from reporting entities, and incoming and outcoming exchange of data with the foreign FIUs.

In February 2018, the case was passed to the Organized Crime and Corruption Unit of the National Prosecutor's Office.

FIU Action

Methods of Gathering Information

The case required complex analyses of the credit and debit transactions from a large number of bank accounts (mass payment and "traditional" customer's accounts). The critical part of the analytical process was prompt data sharing with FIUs in many countries due to extreme international fragmentation of the illegal activity.

Analytical Process

A critical factor for this case was the international exchange of data/analysis results. From the Polish perspective, the initial milestone was the first incoming foreign FIU's request related to Mr. XXX. The next critical component was related to data exchange with the foreign FIU outside the European Union. The aggregated data from a few financial institutions and the exchange of information with law enforcement authorities in Poland also contributed to the analysis. The geographic spread and large number of bank accounts demanded processing capacity and tools.

Later on, the analysis was updated by the data received from foreign FIUs in Germany, Ireland, the Netherlands, Switzerland and the United Kingdom. The data received from the following FIUs also contributed to the effective analytical process: FIU-Brazil, FIU-Canada, FIU-Gibraltar, FIU-Hong Kong, FIU-Lithuania and FIU-Panama. FIU-Poland's significant contribution to the development of the case was active coordination of the financial intelligence data flow related to the Polish legal entities.

Evolution of the Case

The case involved 15 FIUs plus Poland, for a total of 16 FIUs contributing to the analysis. International cooperation was inevitable as the illegal activity was totally fragmented in terms of geolocation, as well as the regular change of legal entities and use of a large number of bank accounts, including mass payment ones.

The Prosecutor's Office investigation is still active at this time. Additional evidence is being gathered related to the origin of the funds involved in the activity of legal and natural persons in the case. One of the main suspects was arrested in Greece near the Bulgarian border under a European arrest warrant that is valid for the whole territory of the European Union irrespective of the issuing member state. The arrested suspect, Mr. XXX, is currently in a Polish jail.

The case has evolved as new sources of the funds have been identified (i.e., VAT carousel). Besides that, separate investigations/lawsuits are being pursued in other countries related to Bitfinex's activity as a cryptocurrency exchange; there is a question about the possibility of misinformation related to the financial services offered and the management practices related to the capital flow within the iFinex/Bitfinex/Tether group. Bitfinex with respect to this particular case claims the frozen funds — when the bank accounts and incoming transfers were frozen, around USD 380 million was blocked — are its capital and the deposits of its customers.

Aktualizacja: 06.09.2019, 17:00 Publikacja: 06.09.2019

Zbigniew Ziobro: Prokuratura zajęła 1,4 mld zł z handlu narkotykami

Fotorzepa / Jerzy Dudek

zew

NAPISZ DO AUTORA

Polska prokuratura zajęła ponad 1,4 mld zł pochodzących z handlu narkotykami i oszustw internetowych - poinformował Prokurator Generalny Zbigniew Ziobro.

Jak oświadczyła Prokuratura Krajowa, pieniądze z kont bankowych przestępców przejmie Skarb Państwa. To największe w historii polskiej prokuratury zabezpieczenie pieniędzy na poczet przepadku.

– Zabezpieczenie pieniędzy było możliwe m.in. dzięki przygotowanej przez Ministerstwo Sprawiedliwości nowelizacji kodeksu karnego, w tym ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu - powiedział Zbigniew Ziobro.

Zbigniew Ziobro: Prokuratura zajęła 1,4 mld zł z handlu narkotykami," Rzeczpospolita, September 6, 2019

Outcome/Contribution of the Case

Collaboration with domestic partners, including the initiative of Prosecutor's Office and the law enforcement agencies, contributed to the successful outcome: frozen funds for the amount of USD 380 million and one suspect arrested.

Best practices identified include early warning based on requests and spontaneous exchange of information; and prompt reply containing data and analytical outcome.

Lessons learned:

- Cryptocurrency cases can require cooperation among several FIUs.
- Virtual business may be borderless, but prosecution is not.
- The prompt exchange of data and analytical hypotheses/conclusions in a standardized format in these kinds of cases is critical.
- A rigorous framework must be adaptable to the digital — and therefore evolving — nature of these types of crimes.

Valuable indicators of the case

- Smaller financial institutions: Special attention is required for smaller financial institutions (some analytical potential exists related to financial institution's balance sheet horizontal change that makes possible to detect sharp increase/change in smaller entities, for example, deposits).
- Regulatory weaknesses: Standards for effective regulations are required with respect to virtual/mass/special accounts and data recovery/processing.
- Cryptocurrency intermediaries: Based on the meta analyses of the broader context of this particular case, special treatment is required against cryptocurrency intermediaries that are "pushed out into the shadows" and looking for banking services including "a central bank."

CASE 8

Effective Collaboration in Business Email Compromise (BEC) Scheme (South Africa, FIC)

Introduction

A transnational syndicate that was operating a Business Email Compromise (BEC) scheme targeted several U.S. residents purchasing a property. This BEC involved the interception of emails where perpetrators carefully selected victims who were in the process of purchasing the property. They communicated with victims and purported to be a known party to the sale, providing alternate banking details for payments that resulted in a loss of funds to their victims.

The Investigation

The BEC Scheme was initially triggered by a request for information via the Egmont Secure Web to South Africa's Financial Intelligence Centre (FIC) from the U.S. Financial Intelligence Unit (FIU), the Financial Crimes Enforcement Network (FinCEN), on January 20, 2016. This was followed by four related subsequent requests from FinCEN.

Keywords	email fraud, email compromise, cybercrime, BEC
Countries involved	South Africa and United States
Sectors involved	Motor vehicles, international real estate

In all mentioned cases, the victims received a legitimate email from their attorneys requesting wire transfers to secure a property that they intended to purchase. Shortly thereafter, the victims received a second email from the perpetrators of the scheme purported to be the same transferring attorney, but stating that the banking details have changed and providing new instructions for the transfers. In each case, the victims failed to notice that the email address differed and effected the transfers as instructed. Thereafter, the victims received emails from the purported attorneys stating that the funds were received and that they should visit the attorney's office to complete the closing of the property transaction. Subsequent to receiving the emails, the victims received a call from their actual attorneys stating that no payments were received.

It became apparent that the perpetrators directed the victims to pay funds to accounts held with the Bank of America and Wells Fargo Bank in the United States under the guise that these were the accounts of the transferring attorneys.

The case involved a **FRAUD** and money laundering investigation into a scheme perpetrated by suspects of Nigerian, Ghanaian, Zimbabwean and South African descent. The criminal activity undertaken was initially difficult to substantiate, but as the investigation developed it became evident that the proceeds from the FRAUD perpetrated were used to purchase numerous high-value vehicles. Cash withdrawals also contributed to the overall disposal of the proceeds of the crime.

The FIC referred the allegation of fraud and theft to domestic law enforcement authorities after receiving statements from the U.S. complainants. A case was duly registered for investigation under a Johannesburg Commercial Crime Enquiry.

FIU Action

On January 20, 2016, the FIC was informed that USD 202,217.25 was misappropriated from Mr. A (a U.S. citizen) and received into an account held at the Bank of America. The funds were transferred on January 13, 2016, to three bank accounts held by individuals and registered businesses in the Republic of South Africa, aggregating ZAR 3,529,693.76.

Upon receipt of the request from FinCEN, the FIC contacted the local banks mentioned in the request to verify the transactions and to determine any positive balances. Once the FIC received confirmation, the FIC issued an instruction on January 20, 2016, to block the funds in the accounts for five days.

During this period, the FIC requested the relevant bank statements and conducted further analysis. The FIC also inquired whether the identified account holders held facilities at other accountable institutions, requested the relevant bank statements and conducted further analysis.

Cash withdrawals and payments to high-value second-hand vehicle dealerships were identified. The dealerships were contacted to determine the details of the vehicles and the identification of the respective buyers. This information was corroborated with data extracted from the Electronic National Transport Information System (eNatis) and confirmed the offers to purchase a Porsche, a BMW and a Mercedes-Benz.

During inquiries with the dealerships, it was confirmed that although the subject had made cash payments aggregating ZAR 700,000.00 to purchase a Mercedes-Benz. This created an opportunity for the FIC to apply its existing legislation in a unique manner. By linking this deposit to the proceeds of crime (transferred from the United States), the FIC supported the application for a preservation order to seize the Mercedes-Benz and to block funds equalling ZAR 652,000.00 held in the accounts of two dealerships for the purchase of two other vehicles.

The FIC's initiatives enabled it to identify the subjects involved in the transnational scheme, the interlinked accounts, the balance of the funds in these accounts and the assets purchased with the funds.

The FIC contacted local law enforcement authorities to secure the remainder of the funds in the accounts that had been blocked (ZAR 1,701,111.92) and seized the assets identified (valued at ZAR 1.6 million). The FIC also drafted and issued a sworn statement in support of the asset forfeiture application for a court-directed order.

Since then and for the next two years, four similar schemes using the same modus operandi took place in August 2017, November 2017, and twice in January 2018. In these cases, the FIC was successful in obtaining preservations and forfeiture orders on several assets.

Evolution of the Case

As the financial investigation progressed, active collaboration between the FIC, FinCEN and several domestic law enforcement authorities developed. The FIC facilitated information exchange and collaboration between the domestic law enforcement agencies and FinCEN through constant communication throughout the investigation. The FIC provided FinCEN with detailed profile information on linked subjects and registered business entities along with an analysis of how the funds were utilized.

Law enforcement agencies were provided with information concerning criminal activities of the persons involved, copies of documents obtained, references and financials.

The FIC facilitated the exchange of information between FinCEN and South African law enforcement to meet the statutory requirements for forfeiture.

In support of court-directed forfeiture applications, the FIC provided sworn statements to attest to the predicate offence, the source of the funds, their flow into South Africa and the transfer of funds domestically. Law enforcement was able to secure preservation orders so that the funds could be repatriated to the victims (in certain instances). Collaboration with the United States Federal Bureau of Investigation resulted in the quick provision of sworn statements from the victims in these matters. The statements provided the confirmation of the commission of the crimes in the foreign jurisdiction, with the funds obtained deemed proceeds of crime in South Africa.

Law enforcement agencies were provided with statements from the FIC and victims of the crimes for the purpose of asset forfeiture proceedings and/or money laundering charges against the subjects identified. These statements resulted in the registration of criminal cases and the issuance of warrants of arrest for the identified perpetrators in the South African jurisdiction.

The FIC initiated meetings with domestic law enforcement agencies and the U.S. Secret Service to prioritize investigations with regard to the subjects identified. A Mutual Legal Assistance Treaty is being drafted for a joint investigation with all law enforcement agencies in the aforementioned matters.

The U.S. Secret Service has embarked on investigations in its American jurisdiction and has already arrested subjects operating within the Bank of America who are suspecting of having assisted the syndicate. The matters are currently being investigated and the subjects are being traced for the purpose of arrest and conviction.

Outcome/Contribution of the Case

The immediate actions taken by the FIC resulted in the blocking of funds to the total value of ZAR 6,871,449.56 (about USD 453,600). The FIC secured the necessary evidence, which resulted in preservation orders being granted against the funds secured. Forfeiture orders have been obtained against the various amounts secured, after which all the funds that have been secured together with accumulated interest will be refunded to the victims of the crimes.

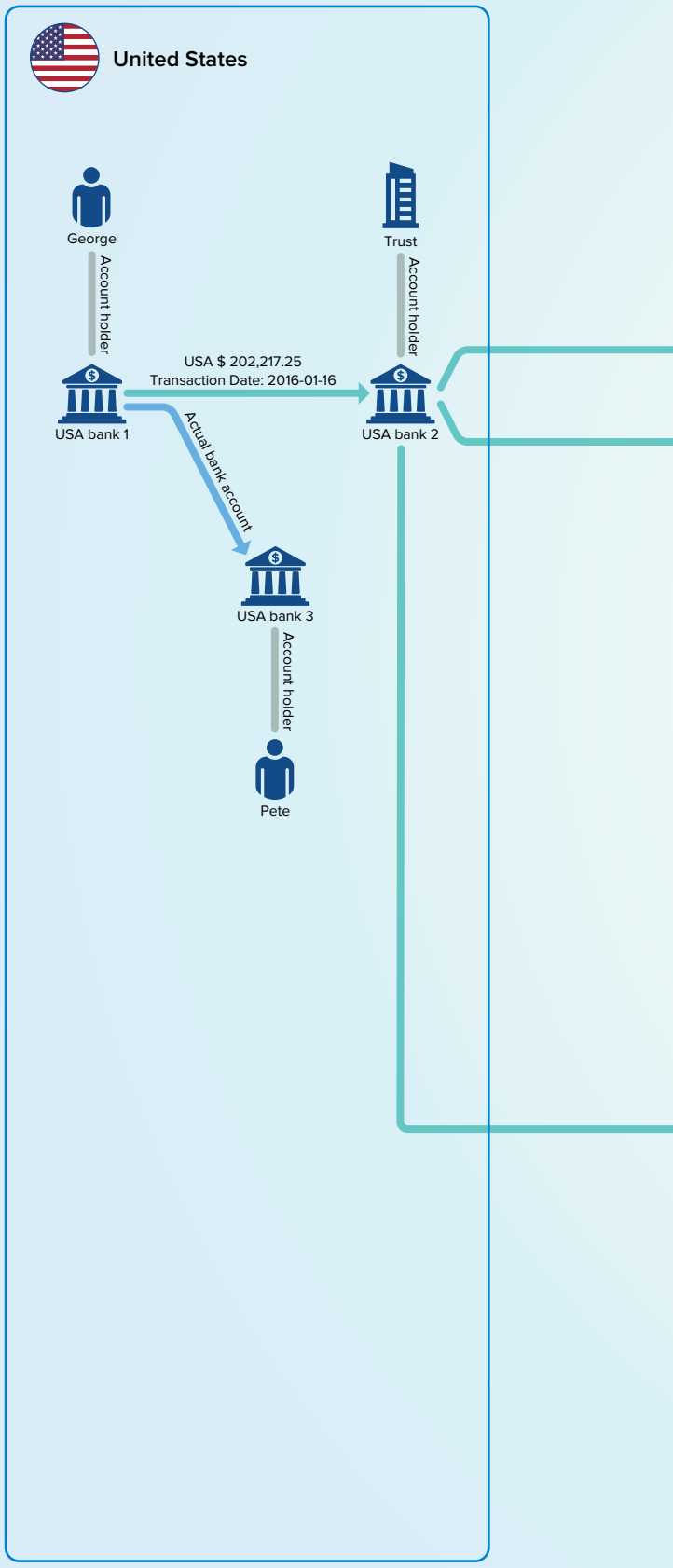
The FIC was also instrumental in identifying vehicles that together were valued at ZAR 1,600,000.00 (about USD 105,600) that were purchased with the proceeds of the international fraud transactions, against which preservation orders were obtained. One vehicle has already been seized and two others have been circulated as being sought. The seized Mercedes-Benz has been forfeited and the proceeds thereof paid to the victim of the fraud in the United States.

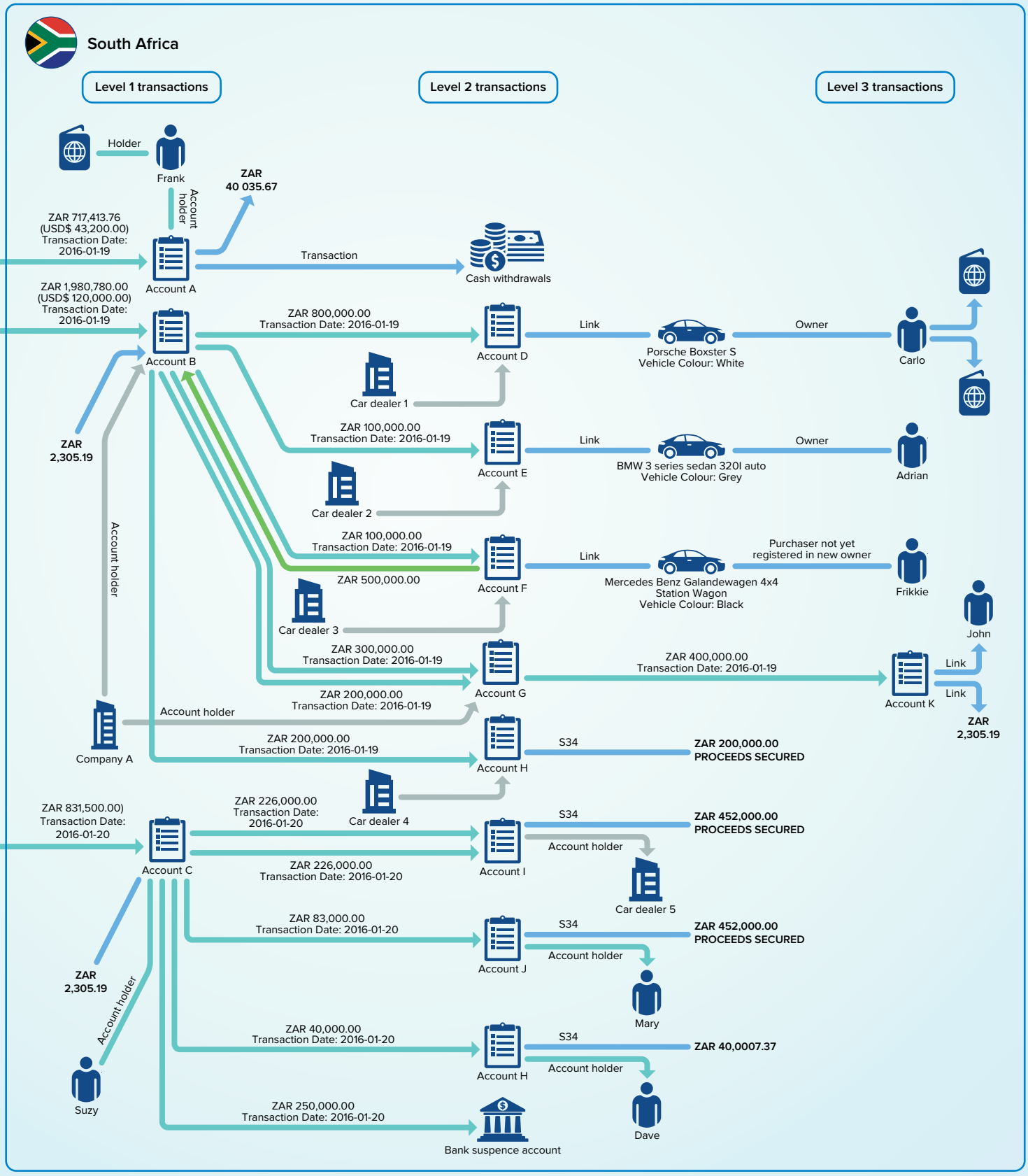
The identified perpetrators of the listed cases are now being investigated in a joint investigation between the United States and domestic law enforcement agencies, which will shortly result in the subjects facing various charges related to the frauds.

Valuable Indicators of the Case

- Fraudsters usually register a domain similar to its target. If the target email is somename@company.co.za, a scammer may use a variation such as somename@company.biz or slightly change the spelling into somename@cmpny.com.
- Cybercriminals employing CEO fraud typically pose as someone influential in an organization. BEC usually appear as if they came from the COO, CEO or Chief Executive to transfer funds into a “changed” bank account.
- Funds are transferred to a recipient in the company who the victim has never dealt with in the past.
- Transfers initiated near the end of day or just before weekends or public holidays.
- The receiving account does not have a history of receiving large funds transfers in the past.
- The receiving account is a personal account.

E-08 SOUTH AFRICA




South Africa
Level 1 transactions
Level 2 transactions
Level 3 transactions
Holder
Frank
Account holder
ZAR 40 035.67
ZAR 717,413.76 (USD$ 43,200.00) Transaction Date: 2016-01-19
Account A
Transaction
Cash withdrawals
ZAR 1,980,780.00 (USD$ 120,000.00) Transaction Date: 2016-01-19
Account B
ZAR 800,000.00 Transaction Date: 2016-01-19
Account D
Link
Porsche Boxster S Vehicle Colour: White
Owner
Carlo
Car dealer 1
ZAR 2,305.19
ZAR 100,000.00 Transaction Date: 2016-01-19
Account E
Link
BMW 3 series sedan 320I auto Vehicle Colour: Grey
Owner
Adrian
Car dealer 2
Account holder
ZAR 100,000.00 Transaction Date: 2016-01-19
ZAR 500,000.00
Account F
Link
Mercedes Benz Galandewagen 4x4 Station Wagon Vehicle Colour: Black
Purchaser not yet registered in new owner
Frikkie
Car dealer 3
John
ZAR 300,000.00 Transaction Date: 2016-01-19
Account G
ZAR 400,000.00 Transaction Date: 2016-01-19
Account K
Link
Link
ZAR 2,305.19
ZAR 200,000.00 Transaction Date: 2016-01-19
Account holder
Company A
ZAR 200,000.00 Transaction Date: 2016-01-19
Account H
S34
ZAR 200,000.00 PROCEEDS SECURED
Car dealer 4
ZAR 831,500.00) Transaction Date: 2016-01-20
ZAR 226,000.00 Transaction Date: 2016-01-20
Account C
Account I
S34
ZAR 452,000.00 PROCEEDS SECURED
Account holder
Car dealer 5
ZAR 226,000.00 Transaction Date: 2016-01-20
ZAR 83,000.00 Transaction Date: 2016-01-20
Account J
S34
ZAR 452,000.00 PROCEEDS SECURED
Account holder
Mary
ZAR 2,305.19
Account holder
ZAR 40,000.00 Transaction Date: 2016-01-20
Account H
S34
ZAR 40,0007.37
Account holder
Suzy
Dave
ZAR 250,000.00 Transaction Date: 2016-01-20
Bank suspence account

DRUG TRAFFICKING

Drug trafficking generates multibillion-dollar revenues annually, making it the main source of revenue for criminal organizations, such as drug cartels.[5] Drug trafficking was identified as the single largest crime category tied to money laundering (accounting for about a third), followed by smuggling (about a fifth).[6] According to the United Nations Office on Drugs and Crime (UNDOC),[7] drug use around the world has been on the rise. In 2009, an estimated 210 million drug users represented 4.8 percent of global population aged 15–64, compared with the estimated 269 million users in 2018, or 5.3 percent of the population.

5 United Nations Office on Drugs and Crime (UNDOC), *World Drug Report 2010*, 2010, p. 5 www.unodc.org/unodc/en/data-and-analysis/WDR-2010.html

6 UNDOC, *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes*, October 2011, pp. 32–33, www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

7 UNDOC, "Executive Summary," *World Drug Report 2020*, 2020 https://wdr.unodc.org/wdr2020/en/exsum.html

According to the Financial Action Task Force,[8] drug trafficking can generate huge amounts of proceeds and "the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention."

The actual payment for drugs is nearly always done with large sums of cash that must be moved and/or eventually integrated into the financial system so that they appear to be legitimate funds that can be used to support a lavish lifestyle or finance other business activities.

Criminal groups are becoming more and more creative with their distribution and payment methods. One of the cases in this section involves a family using fuel transport contracts with the state to not only transport drugs but also to hide the money received for those drugs. Another relates to a crime group whose global drug trafficking ring implicated lawyers, financial experts, a bank manager and dozens of individuals, with the criminal money laundered through various company takeovers.

The sale of synthetic drugs over the Internet is also a growing industry. The 2020 report from UNDOC points to the changes in the drug market, "drug markets are becoming increasingly complex. Plant-based substances such as cannabis, cocaine and heroin have been joined by hundreds of synthetic drugs, many not under international control. There has also been a rapid rise in the non-medical use of pharmaceutical drugs."[9] One case involved a sophisticated network of businesses to hide the international trafficking of drugs on the web and through parcel post. Another organized crime group was headed by a prison inmate who orchestrated the importation and distribution of methamphetamine from inside his cell.

Indicators

- Use of companies to provide a cover of legality
- Public contracts with a state company
- Use of family ties to hide money and confuse investigative services
- Bribery of public officials
- Use of legal companies that receive profits from organized crime
- Use of multiple accounts to collect funds that are then transferred to the same foreign beneficiaries, among others

8 Financial Action Task Force, *What is Money Laundering?*, n.d., https://www.fatf-gafi.org/faq/moneylaundering

9 UNDOC, "Executive Summary," 2020.

CASE 9

Cloaking Drug Trafficking and Money Laundering in State Contracts in Fuel Transportation (Bolivia, FIU-Bolivia)

Introduction

Financial intelligence was able to identify links within a criminal organization that used contracts with a state organization to facilitate international trafficking of controlled substances (marijuana, cocaine) using fuel trucks. These illegal activities generated a large amount of illegal money that was laundered through legally constituted companies and by front companies also related to fuel transport that were run by different family members.

The Investigation

In 2015, the Public Ministry sent Bolivia's Financial Intelligence Unit (FIU) a request for financial analysis of the financial operations of members of the same family who were being investigated for drug trafficking offences. Six obliged subjects also presented seven suspicious transaction reports to FIU-Bolivia that same year, corresponding to spouses X and Y, and their family connections, mainly their eldest son, A.

Keywords	trafficking, controlled substances
Countries involved	Argentina, Bolivia
Sectors involved	transport, fuel tankers

The investigation into the cross-border transportation of drugs led to the identification of vast amounts of money, as well as many assets used for this crime (e.g., fuel tanker trucks). Several companies had been founded whose main purpose was identified as for the transport or sale of fuel through service stations that also belonged to the family.

All these operations were used to clear illicit funds, as spelled out in the typologies and warning signs identified by the Financial Action Task Force.

The financial analysis started with Company C, which was acquired in December 2007 by spouses X and Y. This company's main activity was the "transportation of national and international cargo." Before being purchased by X and Y, this activity generated an annual profit of approximately USD 4,500 in the last four years. After the purchase, it generated an average profit of approximately USD 33,300.

Once in the hands of the family, Company C multiplied both its assets and its earnings in a short time. With family members carrying out operations under the banner of Company C and other front companies set up for this purpose, a lot of money could be moved.

X and Y used Company C to facilitate the free transport of controlled substances through contracts awarded by state companies for fuel transportation. The fuel delivery was used as a cover for the illegal activities. The success of this methodology encouraged the family group to create other companies in the same category and recruit other family members to support the necessary logistics.

The analysis verified that X and Y were owners of Company C, and that they opened and managed bank accounts in local and foreign currency in different financial entities. According to the financial intelligence report, these companies had managed amounts in the X and Y accounts that exceeded deposits of USD 120 million. Approximately 45% of the total money managed could be accounted for through state contracts for the transportation of fuel and derivatives; an additional 10% corresponded to transactions with companies requesting their services that would be legal. The balance of 45% of the money had an unknown source and destination. The analysis identified X and Y's children — A, B, C and D — and companies C1, C2, C3, C4 and C5, which had been created by both X and Y, as well as their children, as being involved in transactions with Company C and with each other.

The analysis carried out by FIU-Bolivia, in close coordination with the Public Ministry, identified **ILLICIT TRAFFIC IN CONTROLLED SUBSTANCES** as a previous crime and established the **LEGITIMATION OF ILLICIT PROFITS** as the main crime.

FIU Action

FIU-Bolivia collected, collated and analyzed information from INTERPOL, the Directorate General of Traffic, Customs, the Minister of Industry and Commerce, the Central Bank of Bahrain, and governmental and international organizations such as the Egmont Group.

FIU-Bolivia sought information such as:

- registration of real estate and vehicles;
- additional economic activities registered in the Registry of Commerce (FUNDAEMPRESA) or autonomous departmental governments;
- taxes; and
- migration.

All financial and equity information was classified and analyzed to detect possible changes in transactional patterns and concentration of resources among the beneficiaries.

The analysis focused on the origin and use of money, in comparison with the socioeconomic and financial profile of the people involved, including the relationships among the depositors or beneficiaries of the transactions carried out.

Because a total of 14 people were involved, FIU-Bolivia applied a new analysis technique to account for this large number. The analysis focused on three people, X, Y and A, with the analysis of the rest of those involved based on relevant links and transactions that led back to the three lead individuals. This technique was able to identify that the funds moved among members of A's family and their personal bank accounts. Links were also identified between A's corporate accounts without a correlation between A's personal bank accounts and X – Y corporate earnings.

Once the indications of **LEGITIMATION OF ILLICIT PROFITS** had been identified and the financial and equity analysis completed, FIU-Bolivia, in compliance with the regulatory powers and attributions, followed regulatory requirements and sent the intelligence report to the Public Ministry or Prosecutor's Office, the body in charge of the prosecution and investigation of crimes related to this charge.

Evolution of the Case

The case involved a year of investigation before any suspects were arrested.

Throughout the investigation, the Public Ministry coordinated effectively with FIU-Bolivia, resulting in the development of objective strategies, thus achieving vital and timely results. Similarly, international inter-institutional cooperation was of vital importance for the investigation, since the information provided by FIU-Argentina helped to precisely identify the links between the members of the family.

The case was in the oral trial stage of the Bolivian criminal process. FIU-Bolivia's coordination with the Prosecutor's Office is important since the information in the Financial and Asset Intelligence Report will be useful in preparing for the oral trial. Now, FIU-Bolivia is waiting for the closing of the trial.

Outcome/Contribution of the Case

The case identified a new legal interpretation of money laundering, originating from illicit activities such as drug trafficking, through a company dedicated to fuel transportation. Through this scheme, the family transported a sizable amount of drugs across the borders of Bolivia and Argentina specifically.

At the same time, coordination with the Public Ministry made it possible to identify the illegal activity in a timely manner, leading to the arrest of the members involved and the subsequent extradition of the main defendant to submit to criminal proceedings for drug trafficking in Argentina.

Valuable Indicators of the Case

- Transfer of significant funds to third-party bank accounts
- Obtaining credits that were paid in advance
- Clients or relatives have a history of being investigated for illicit drug trafficking
- Low-earning company begins to generate a significant income in a short time

CASE 10

Internet Pharmacies Distributing Illegal Drugs Worldwide (India, FIUIND)

Introduction

Psychotropic substances were trafficked by misdeclaration using illegal Internet pharmacies and receipt of remittances from abroad for the psychotropic substances smuggled out, in an attempt to launder the proceeds of crime. The individuals involved managed a software business for maintaining websites to support the illegal activities and used post parcel / courier routes for transporting psychotropic substances. Foreign remittances were received via fake bank accounts and money transfer service scheme (MTSS) franchises were used. Apart from the website management company, five companies were linked to the trafficker and 19 bank accounts and property worth more than INR 220 million were identified in the case. A suspicious transaction report (STR) disseminated by India's Financial Intelligence Unit (FIU-IND) to the concerned law enforcement agencies (LEAs) initiated the case.

The Investigation

FIU-IND analyzed an STR from a bank and disclosed it to LEA-A (the Indian agency dealing with money laundering, related offences and foreign exchange violations), which in turn transmitted the STR to LEA-B (the Indian agency responsible for fighting drug trafficking and the abuse of narcotic drugs and psychotropic substances). The STR indicated that over a three-year period, starting January 2015, XYZ branch of an MTSS had made 11 pay-outs to Mr. A amounting to INR 130,000. These amounts were received from various persons from Costa Rica, the United States, Denmark, Australia and France. Mr. A had informed the bank that the remittances were sent by his friends for his personal use. Details of the remitters did not show any apparent relationship with the receiver.

Keywords	psychotropic substances
Countries involved	Australia, Costa Rica, Denmark, France and United States
Sectors involved	pharmaceuticals, money transfer industry

Enquiries revealed that Mr. A had submitted a forged driver's licence to the MTSS franchisee. When questioned, Mr. A submitted that the foreign remittances actually pertained to his brother, Mr. B.

Further inquiries revealed that Mr. B had worked for nearly three years in customer support and as a data entry operator in what was purportedly a software company, M/s ABC Softech; Mr. B also looked after the company's MTSS-related work. The stated work of M/s ABC Softech was creation of websites but surveillance of company activities indicated that it was involved in sending drugs and medicines outside the country. The investigation also revealed that the company was being used to receive MTSS payments in the name of fake persons based on forged identification documents. The payments were used for the supply of medicines, including some psychotropic drugs. The medicines were distributed in post parcels through India Post.

Preliminary inquiries also indicated the company had created many websites that had names indicating that the company dealt with medicines. The company created customer support to follow up on the orders. The company also collected payments through e-cheques and through certain online e-payment portals.

The inquiries also revealed that the company received payments from abroad using two MTSS franchises, which were owned by Mr. X and his wife Ms. X, who were also directors of M/s ABC Softech. These MTSS franchises were operated from the office of M/s ABC Softech, but the records were maintained at a drug store, M/s Pharma ABC, which was also owned by Mr. X. M/s ABC Softech procured drugs from Delhi and Mumbai, as well as from M/s Pharma ABC.

In a nutshell, M/s ABC Softech was smuggling pharmaceutical formulations containing narcotic drugs/psychotropic substances to overseas buyers using international post. The business appeared to be huge considering that a full-fledged call centre, a drug store and MTSS franchises, all interconnected, had been established to facilitate transactions.

In early August 2018, intelligence indicated that M/s Pharma ABC was about to send 44 parcels containing drugs, some of which were formulations containing psychotropic substances, to the United States, the United Kingdom and Hungary through the Foreign Post Office in New Delhi. The 44 parcels were intercepted and searched. Simultaneous searches were also conducted at four company locations, including the residence of Mr. X. These searches recovered over 22,000 tablets that were formulations of psychotropic substances like Tramadol, Diazepam, Zolpidem, Clonazepam, Alprazolam and Nitrazepam. All of these substances are controlled under the *Narcotic Drugs and Psychotropic Substances Act, 1985* (NDPS Act) and dealing with these substances requires appropriate licences. Their import and export requires a No Objection Certificate of the Narcotics Commissioner. The predicate offence is violation of NDPS Act, section 8, **PROHIBITION OF CERTAIN OPERATIONS**, and NDPS Act, section 21, **CONTRAVENTION IN RELATION TO MANUFACTURED DRUGS AND PREPARATIONS**. All these substances were seized and two people, including the head of the operation, were arrested.

FIU Action

The entire case started with an STR involving an amount of only INR 130,000. Averaging that amount over 11 payouts during a three-year period would translate into an average individual payout of just under INR 12,000, which by itself is not very significant. The STR was generated, however, because these related to remittances from abroad, to a person who would have no obvious reasons to receive the money, ultimately leading to the discovery of an organized drug trafficking racket.

After the suspects' premises were searched and the investigation had led to details of bank accounts being used by the suspects, the information was shared with FIU-IND, which in turn was able to link six additional bank accounts and share that information with LEA-B.

Further, since the psychotropic substances were illegally exported to the United States (as well as other countries) and since a large amount of remittances were sourced from a U.S. company, Uncle Sam LLC, cooperation was sought from the U.S. Drug Enforcement Administration (DEA) through its foreign office located in New Delhi. The inquiries conducted by the DEA revealed that the overseas address of Uncle Sam LLC was not correct, and the company did not exist at that address. This further confirmed the suspicions of money laundering.

Evolution of the Case

The case can be traced from an STR for a small amount that had the earmarks of money laundering. For that reason, FIU-IND involved LEA-A, which in turn involved LEA-B because there were indications of drug trafficking as well. Throughout the preliminary inquiries and the investigations and searches, FIU-IND worked closely with LEA-A and LEA-B in analyzing financial activities, such as tracing bank accounts, the chain of drug trafficking and the financial flows, including those from the United States.

Outcome/Contribution of the Case

The matter is under active investigation. Properties amounting to approximately INR 220 million have been frozen. The investigation identified 19 bank accounts related to Mr. X or the companies owned by him, having balance of over INR 30 million accrued through foreign remittances. The investigation also revealed the use of fake rubber stamps by Mr. X to prepare forged documents, leading to other criminal charges.

Action for forfeiture of the properties identified is being taken following due process. Two individuals have already been arrested. Prosecution against all concerned offenders will be launched after completion of the investigation.

Valuable Indicators of the Case

- Multiple foreign incoming remittances of small amounts from multiple countries
- Reasons for receipt of the money not satisfactory
- Several entities owned by same person

CASE 11

Organized Crime Group Operating from Jail: The Methamphetamine Business Transactions (New Zealand, NZPFIU)

Introduction

Operation GANDOLF was a multi-agency investigation into the importation of methamphetamine. The investigation was led by the Organised and Financial Crime Agency New Zealand (OFCANZ), now called the National Organised Crime Group, and supported by the New Zealand Customs Service (NZCS), the Department of Corrections (Corrections), and the New Zealand Police Financial Intelligence Unit (NZPFIU).

The primary target of Operation GANDOLF was Egyptian national Mohamed Soliman Hussain Atta, who was at the centre of an organized crime group that orchestrated the importation and distribution of methamphetamine throughout New Zealand. At the time, Atta was serving a 10.5-year prison term, at Rimutaka Prison.

The Investigation

In April 2013, a New Zealand-based group was identified as importing crystal methamphetamine from a group based in Thailand. The New Zealand group sent money to the Thailand group, which then posted parcels containing methamphetamine to an agreed address in New Zealand.

Keywords	methamphetamines, drug trafficking, organized crime, Rimutaka
Countries involved	New Zealand and Thailand
Sectors involved	banking, pharmaceuticals, import/export, money transfer industry

In April 2014, the NZPFIU began analyzing a number of suspicious transactions between Thailand and New Zealand and commenced an operation to understand the underlying purpose. The NZPFIU informed OFCANZ, which launched a criminal investigation that the NZPFIU supported through to its conclusion.

Between February and October 2014, Atta was imprisoned at Rimutaka Prison in Upper Hutt for importation of cocaine and aggravated robbery. Between January and July 2014, approximately NZD 1,000,000 was sent to Thailand from New Zealand via international money transfer. This amount of money would purchase approximately 5 kilograms of methamphetamine, worth NZD 5,000,000 when resold in New Zealand.

Atta was identified as having access to and using several mobile phones while in custody, which enabled him to facilitate these activities.

Police also intercepted phone calls involving Atta and other prisoners in which they often used the term back door. This is a term within the prison environment that refers to a corrections officer who smuggles contraband into the prison in return for payment.

Atta was assisted by his wife Linda Olive Aldworth. She provided him with mobile phone top-up vouchers and completed bank transactions at his request. She was jointly charged with Atta for **CONSPIRACY TO IMPORT METHAMPHETAMINE**.

From intercepted communications and interviews, the investigation team was able to piece together an outline of Atta's modus operandi:

1. A customer who wanted to purchase methamphetamine would contact Atta on cell phones that he possessed unlawfully.
2. Atta would obtain a name from his supplier in Thailand.
3. Atta's customer would remit money using an international money remittance service provider to the name (person) provided by Atta's supplier in Thailand.
4. Atta's customer would provide him with the money transfer control number (MTCN) when the customer made the money remittance, along with a name and address for delivery of the methamphetamine.
5. Atta would then forward the MTCN, name and address to his supplier in Thailand who would collect the money in Thailand.
6. When Atta's supplier in Thailand had collected his money, the supplier would post the methamphetamine to the name and address provided in New Zealand.
7. When the customer received the methamphetamine, the customer would pay Atta a commission, which was deposited in Aldworth's bank account.

During the intelligence collection phase of Operation GANDOLF, Corrections voiced its concerns over the corrupt practices of various corrections officers employed at Rimutaka Prison.

Call and text messaging data were collected from various mobile service providers pertaining to Atta's activities. An analysis identified references to the introduction of contraband items into Rimutaka prison by Corrections Officer Alofainui'u Tuisamoa. Various text messages outlined what Atta wanted and how much Tuisamoa expected to be paid for providing it.

A production order revealed texts from Atta to Aldworth in which he requested she pay money to a bank account linked to Tuisamoa. In February 2015, police executed a search warrant at Tuisamoa's home address, where they located a number of handwritten notes, diary entries and related items, such as mobile phones, SIM cards and phone chargers.

Items purchased and supplied by Tuisamoa, including a mobile phone, were located during a search of Atta's cell. Atta had used the phone to facilitate the importation of methamphetamine into New Zealand.

FIU Action

Initial NZPFIU analysis established that between February and April 2014, eight New Zealand-based persons residing in four different regions had facilitated 29 separate transactions to five Thai-based persons, amounting to a total value of NZD 178,451.

NZPFIU also found links to active New Zealand Police and Customs operations and identified associations with New Zealand gangs and to individuals incarcerated in New Zealand prisons. It also identified individuals with criminal convictions, including for drug-related offences.

Over the next few months, the NZPFIU received and analyzed further suspicious transaction reports (STRs). Operation GANDOLF involved a total of 69 STRs containing 486 individual transactions.

During the analysis stage, the NZPFIU used following techniques:

- collection of relevant information from police databases;
- open source information;
- analysis of transactions; and
- charting of transactions and associations.

NZPFIU initially worked on the case for the first two to three months to write up an intelligence product to present to investigative agencies. It then made a presentation in May 2014 to several New Zealand law enforcement agencies. OFCANZ became the lead agency in the joint force investigation, now named GANDOLF.

NZPFIU was responsible for identifying payments rapidly, after which Customs worked with Corrections to immediately arrange intercepts.

Operation GANDOLF proved to have strong ties to Thailand. With the help of a New Zealand Police Liaison Officer who is based in Bangkok, OFCANZ and NZPFIU established efficient communication channels with Thai government agencies, namely the Royal Thai Police and the Thai Anti-Money Laundering Office. NZPFIU received an immediate response and assistance from both Thai agencies.

During the analysis stage, the NZPFIU produced 23 intelligence products, including subject profiles, STR content reports, financial asset profiles and an intelligence report.

All these intelligence products were used by investigators from OFCANZ, Customs, Corrections and an Asset Recovery Unit.

The NZPFIU was involved throughout Operation GANDOLF to detect and identify the movement of money, and continued to work closely with OFCANZ, Customs and Corrections to help detect payments and identify expected dates of shipments to New Zealand.

Evolution of the Case

In April 2014, a New Zealand bank submitted an STR to the NZPFIU, with the following noted:

- Nervous behaviour whilst conducting a transaction
- Gang tattoos noticed
- Multiple large movements of money in less than a month
- Unusual transaction behaviour

Two weeks later, another STR was submitted to the NZPFIU, this time from an international money remittance service provider, with the following noted:

Rimutaka prisoner ran drug importing ring from cell

20:04, Oct 18 2016

Drug ringleader Mohamed Atta is jailed in the High Court at Wellington for 13 years and two months for running a methamphetamine importing ring from prison.

An Egyptian national, already in jail for importing cocaine, ran a methamphetamine importing ring from Rimutaka Prison.

Mohamed Atta, 40, was sentenced to 10 years and six months in jail for importing cocaine in 2010, but began another importing ring in 2014, bringing in 1758 grams of methamphetamine using contacts in Thailand during a three-month period.

Source: https://www.stuff.co.nz/national/crime/85464303/rimutaka-prisoner-ran-drug-importing-ring-from-cell

- Multiple customer transactions from different branches to the same receiver in Thailand
- Unusual pattern of transaction activity as there are few reasons as to why multiple individuals would send to the same individual
- This is a higher than normal frequency and volume of money transmission for [name redacted]
- The transaction pattern shows that the consumers may be splitting a large amount into a number of smaller amounts to avoid transaction limit controls or large principal payment process
- Transactions to high-risk jurisdiction, using multiple agent locations on the same day

In response to these two STRs, the NZPFIU initiated further enquiries.

Outcome/Contribution of the Case

Operation GANDOLF resulted in 15 defendants being charged with variety of offences: 13 have been sentenced to 48 years' imprisonment combined.

Atta pleaded guilty to seven representative charges of **IMPORTING METHAMPHETAMINE** and one representative charge of **CONSPIRACY TO SUPPLY METHAMPHETAMINE**. He was sentenced on October 18, 2016, to 13 years and two months' imprisonment.

Tuisamoa pleaded guilty to one representative charge of **CORRUPTLY ACCEPTING A BRIBE TO DELIVER AN UNAUTHORIZED ITEM TO A PRISONER**, and one charge of **TAKING A PROHIBITED ITEM TO A PRISONER**. He was sentenced on March 18, 2016, to two years and two months' imprisonment.

Aldworth pleaded guilty to the charge of money laundering before trial. Aldworth was sentenced on October 18, 2016, to 10.5 months' home detention.

Total value of assets restrained in New Zealand was approximately NZD $558,000, with over NZD 400,000 forfeited.

Valuable Indicators of the Case

- Large cash transactions with funds moved rapidly
- Unusual transactional behaviour: Out of character with historic account transactional activity
- Smurfing: Multiple persons making payments to a receiver rather than one larger transaction
- Structuring: Splitting transactions into separate amounts under NZD 10,000 to avoid the transaction reporting requirements of New Zealand's *Financial Transactions Reporting Act* and *Anti-Money Laundering and Countering Financing of Terrorism Act*. Many money launderers rely on this technique because numerous deposits can be made without triggering the cash reporting requirements.

CASE 12

Serbian Drug Trafficking Ring Tries to Harvest Legitimacy

(Serbia, FIUSerbia)

Introduction

A Serbian crime group operated a global drug trafficking ring. It established two companies that formed a consortium to participate in a takeover bid of a hotel management company in Serbia. The criminal group hired lawyers and financial experts to take part in the scheme, and involved a complicit bank manager and 42 individuals making structured deposits were as well. The acquisition of the hotel management company was followed by reconstruction works, which enabled the introduction of criminal money into legal financial flows. The hotel business gave way to acquiring two agricultural holdings, with large areas of farmland and good financial standing, which paved the way for an agricultural production business.

The Investigation

The complexity and gravity of the case demanded the involvement of several authorities for parallel investigations of money laundering, drug trafficking (specifically cocaine) as well as the financial investigation. The Prosecutor's Office for Organized Crime led the investigation, the Ministry of Interior led operational activities, and the Serbian Financial Intelligence Unit (FIU) traced money flows between individuals and companies in order to detect the sources and origin of money, channels of criminal money and the methods used for integrating it into legal flows.

Keywords	drug trafficking, organized crime, structured transactions
Countries involved	Serbia, Montenegro, Bosnia and Herzegovina, Croatia, Slovenia, Czech Republic, the United States, Austria and Greece
Sectors involved	banking, hospitality industry, agriculture (takeover of agricultural companies), trade in real estate

The criminal investigation used several investigative means, such as:

- interception of communication between suspects (telephone calls, Internet communication, emails and conversations on business premises);
- search of homes, safe-deposit boxes and offices;
- use of cooperating witnesses and mutual legal assistance.

Tracing money flows, FIU-Serbia identified a large number of accounts in banks in Serbia. The accounts were held by members of organized crime groups, their family members, friends and lawyers, as well as by companies whose owners were members of the group or their associates. Significant amounts of illegal funds were detected in the accounts, which resulted in seizure at the request of the relevant prosecutor.

During the investigation, relevant authorities clearly observed that illegal funds were generated abroad through drug trafficking, and that large amounts were introduced into Serbia from several countries. Through information exchange with other FIUs, FIU-Serbia obtained data to support the fact that members of the crime group owned many companies and extensive real estate abroad, which they financed with criminal money. Criminal flows had also been directed to several investment funds located abroad.

In addition, analysis of money flows showed sizable long-term loans granted by the companies abroad to companies in Serbia. The loaned funds were used for various business activities in Serbia.

All the collected data gathered through FIU-to-FIU cooperation was disseminated to the relevant prosecutor as intelligence. For the purpose of gathering evidence, the relevant prosecutors used the intelligence to send requests for mutual legal assistance in criminal matters to certain countries.

Gathering evidence to build a money laundering case was less time-consuming than gathering evidence for a drug trafficking case. According to an official statement, the trial involved the interrogation of around 100 witnesses and the analysis of tens of thousands of documents and of lengthy audio recordings.

FIU Action

FIU-Serbia identified a large number of accounts in different banks in Serbia. The accounts were held by members of the organized crime groups and their family members, friends and lawyers, as well as by companies whose owners were members of the group or their associates. All these accounts were thoroughly analyzed.

Darko Saric sentenced to 15 years in prison

The Court of Appeals in Belgrade confirmed the verdict by which Darko Saric was sentenced to 15 years in prison in the Special Court.

SOURCE: B92, TANJUG | MONDAY, NOVEMBER 9, 2020 | 19:29

He was convicted of drug trafficking.

Saric was convicted as the organizer of a group charged with smuggling a total of 5.7 tons of cocaine from South America to Western Europe during 2008 and 2009.

Goran Soković, who is on the run and was tried in absentia, was sentenced to the same prison sentence, according to the decision of the Court of Appeals published on its website.

The Court of Appeals upheld the sentences from the first-instance verdict, although it changed the qualification of the criminal offense, while the sentences of the other

Source: https://www.b92.net/eng/news/crimes.php?yyyy=2020&mm=11&dd=09&nav_id=109635

FIU-Serbia contacted the FIUs of Bosnia-Herzegovina, Slovenia, Austria, Greece, Czech Republic, Germany, the Netherlands and the United States, and obtained data that showed that the members of the crime group owned companies and real estate abroad.

The process involved intensive and close cooperation with the Prosecutor's Office for Organized Crime.

Evolution of the Case

After the crime group established itself in the hospitality business, its lawyer approached the owner of a profitable company A and arranged its takeover for EUR 350,000. The company's business had already been relocated to another company, B, so, in practical terms, the organized crime group was actually buying a sound financial report, indicating the good standing of company A, which had everything the group wanted to buy — an agricultural holding in possession of land. The amount of EUR 350,000 was paid in cash.

After the takeover of company A, the organized crime group purchased the stocks of another agricultural holding for EUR 18 million. This amount was paid to the seller, a foreign national, who was eventually charged with being a member of the organized crime group. This person was later on tried in a neighbouring country.

After the purchase of this company, the organized crime group invested dirty money in agricultural production. They invested (layered) criminal money in the total amount of EUR 303,000.

Outcome/Contribution of the Case

As of 2016, 58 members of the organized crime group were indicted for **DRUG TRAFFICKING**, **MONEY LAUNDERING** or both. Nine of them, charged with drug trafficking, entered a plea bargaining agreement, and are now serving 4 to 11 years.

Members of the crime group were active in some neighbouring countries and other countries in the region; two such persons were tried in two former Yugoslav republics.

In 2020, the leader of the crime group, Darko Šarić, was sentenced to 15years for **DRUG PRODUCTION AND TRAFFICKING** of 5.7 tonnes of cocaine. He was also received 9years for **MONEY LAUNDERING** around EUR 22 million, a sentence that is currently being appealed.

Valuable Indicators of the Case

- Large amounts of cash generated by the drug crimes that is then imported in different ways
- Privatization, which is very alluring for money launderers — it often involves the purchase of agricultural land and coercion of innocent individuals to cooperate
- Collusion with highly skilled professionals (financial and legal),which may include bank officials
- Formation and operation of companies conducive to a money laundering enterprise
- Intensive use of cash — this may involve structuring/straw men
- Extravagant lifestyle and purchase of luxury goods (real estate, cars, objets d'art, etc.), which may be an indicator of illicit assets

FRAUD AND EMBEZZLEMENT

Countless people and organizations fall victim to fraud each year, losing their life savings, jobs and investments, and subjecting them to other financial and personal hardships. Equally destructive and often intertwined with fraud is the crime of embezzlement of public and private assets for personal gain. Embezzlement results in the ineffective distribution of goods and services including misdirected or obstructed life-saving medical procurements, shoddy public works, misappropriation of funds meant to help people in need and environmental degradation.

Fraud is always intentional — it aims to trick or deceive a person or company to obtain their wealth. Although fraud does not include the use of physical force like robberies, it is a theft that causes untold misery. Fraud and embezzlement have caused bridges and buildings to collapse, polluted drinking water and air, and the unwitting consumption of poisonous food and medicine. Every person on the planet is potentially a victim of these crimes.

Fraud comes in various forms, such as Internet sales, website misdirection, charities fraud, payroll and employment scams, pyramid schemes, identity theft, credit card fraud, debt elimination, and contract and procurement fraud — all of which produce large profits at the expense of innocent people, organizations and companies.

In 2020, the COVID-19 pandemic created an environment that spawned perhaps the biggest increase in fraudulent activity ever known. As governments throughout the world addressed the pandemic through the urgent procurement of personal protective equipment, virus tests, vaccines and unprecedented financial relief for individuals and businesses, criminals sought to take advantage of this suffering. These fraudsters and corrupt officials in the private and public sectors teamed up through fraud and embezzlement to siphon off for their own personal gain the resources meant to tackle the pandemic. Much of this money has entered the financial system and Financial Intelligence Units (FIUs) throughout the world are actively tracing these funds and analyzing a slew of new types of fraud and embezzlement typologies used in these crimes.

The following selection offers the best examples of a wide variety of fraud and embezzlement cases detected through the work of FIUs over the last six years. They involve various types of fraud including financial statement fraud, asset misappropriation, skimming of cash and cash larceny, misuse of company assets, theft of intellectual property and trade secrets, consumer fraud, insurance fraud, and procurement fraud. Embezzlement crimes in these cases include abuses of office and function for private gain or the gain of a third person, misappropriation and diversion of property by a public official, and trading in influence. These cases demonstrate how internationalized corruption and fraud have become and how quickly criminals move from one illicit moneymaking scheme to another, hiding their ill-gotten gains in multiple jurisdictions along the way. Successful cooperation among law enforcement agencies, financial regulators and public-private partnerships is crucial to identifying these types of crimes. By working together, the public and private sectors can analyze risks so as to better detect illicit activities and return stolen assets, whether they are hidden abroad or at home.

Indicators

- Quick, successive money transfers to another account soon after deposit
- Transfer of funds to countries known for opaque financial sector regulation or high levels of perceptions of corruption without justifiable reason
- Difficulty in verifying customer identification information
- Unnecessarily complicated corporate ownership structuring and hidden beneficial ownership
- Schemes that offer unusually large returns on investment
- Multiple customers sending international fund transfers to the same overseas beneficiary
- Multiple international fund transfers sent to the same beneficiary in one day
- High-value international fund transfers
- U-turn transactions, involving funds being transferred out of the country and then part of those funds being transferred back into the same country
- Series of low-value international fund transfers
- Transfer of funds to recipients in countries where the recipient does not have a valid economic or financial reason for holding a bank account
- Transfer of funds to companies owned by relatives or associates of politically exposed persons

CASE 13

Fraud by Abusing Foreign Trade Operations (Columbia, UIAF)

Introduction

Colombia's Financial Intelligence Unit (FIU), the Financial Information and Analysis Unit (UIAF in Spanish), in cooperation with two foreign intelligence agencies and the Attorney General's Office of Colombia, successfully identified a money laundering network of drug trafficking and terrorism financing that has been in operation for the last 10 years.

This network simulated several foreign trade operations, mainly in the textile and construction sectors. The UIAF shared financial intelligence that led to companies located in three countries in North, Central and South America, as well as bank accounts in the Americas, the Middle East, Asia and Europe.

Keywords	foreign trade transactions, textiles and construction, money laundering
Countries involved	Colombia and three more countries located in North, Central and South America
Sectors involved	money exchange, textile and construction, financial

The Investigation

The trade-based money laundering case was developed in three phases:

Phase I

UIAF analyzed the financial transactions of a specific family that traditionally did business in the textile sector.

After carrying out multiple searches in the databases accessible to the UIAF, priority was given to requesting information from relevant authorities. At this stage, information from the reporting entities was collected, analyzed and processed, and UIAF identified links among people and companies through different types of transactions: imports and exports, foreign trade incomes and expenses, cash transactions, and companies' ownership, among others.

In the analysis stage, differences were established among incomes and expenses of foreign exchanges, through the declared imports statement, where the entrance and exit of foreign trade did not match reported data, such as the registered imports and exports for each analyzed company. The analysis showed that the registered imports and exports were significantly lower than the actual movements of foreign exchange evidenced in those operations. This indicated that the companies and people linked in the case used their extensive experience in the economic sector to mobilize high sums of unjustified money through their commercial operations.

There was also evidence of a link between "narcotrafficking" and one of the company's directors, Andres Covelli Cadavid, as he was extradited to the United States (Law 390 of 2/11/2011, authorized by Colombia's Supreme Court of Justice) for DRUG TRAFFICKING.

The analysis of foreign exchange transactions (income and expenses of foreign exchange) determined that two of the companies involved in the case sent money to two companies located in a Central American country between 2012 and 2013. That money, according to intelligence, belonged to the designated terrorist organization, Hezbollah. It was also established through other background information that the three countries shared the same fiscal auditor.

Likewise, intelligence from one of the agencies that participated in the case development helped to detect links between two of the companies' directors with members of the *Oficina de Envigado*, a Colombian criminal organization.

Phase II

UIAF identified people who operated mainly in the construction sector and who had financial links to people in phase I. Corporate and financial links were established between the companies and people involved in phase I. In addition to the foreign trade activities identified in phase I, a migration of the money to the construction sector (specifically shopping malls) using a "trust fund administrator" was identified.

In the analysis process, the links between family members and trust fund administrators were presented graphically, allowing financial transactions to be mapped out, which focused the case objectives and established traceability of financial information.

Phase III

With the information gathered and analyzed, accompanied with documentation that supported the case and explanations to the Colombian Attorney General's Office and relevant institutions in North America, a simultaneous prosecution process was developed.

FIU Action

The UIAF's role in the case development was achieved through four components of the intelligence cycle:

1. **Planning methods and sources of information.** UIAF used data obtained from suspicious transaction reports, intelligence from foreign intelligence agencies, feedback between the Colombian Attorney General's Office and UIAF, and open source information. More evidence was required in order to confirm links between the different subjects involved.
2. **Specific methods of information processing and analysis.** Several working groups were developed with different foreign intelligence agencies, in Colombia and abroad, for case information exchange. In addition, UIAF analysts explored the databases (imports and exports, foreign trade incomes and expenses, cash transactions, company constitution information and shareholders, among others). With solid bases, UIAF developed a hypothesis about the financial operations that were suspicious and irregular, establishing links through financial transactions and comparing the financial intelligence profile of those reported by financial entities.
3. **Documentation and storage.** The recollection, storage, production and dissemination of the collected intelligence was well documented and stored in magnetic archives in a repository known as the Center for Data Protection (CPD, in Spanish).
4. **Dissemination.** With a solid case and all information gathered and analyzed, UIAF set up a meeting to disseminate the intelligence to the Attorney General's Office, specifically the Assets Forfeiture and Money Laundering Unit (UNEDLA, in Spanish).

UIAF presented the case with links between people and companies, properties, vehicles and financial information that proved that imports and exports of textiles were being simulated in order to justify the foreign exchange incomes and expenses, resulting in money laundering from the proceeds of drug trafficking. The information and explanations provided served as guiding criteria for the relevant authorities to initiate the investigation and prosecution process.

Evolution of the Case

UIAF identified five stages in the case evolution:

1. Information gathering and analysis: The data collected regarded transactions, financial information and links among the actors and companies involved in the case.
2. Warning signs generation: With the collaboration of foreign intelligence agencies and the Colombian Attorney General's Office, UIAF was able to identify typical behaviour in the operability of the Colombian textile sector.
3. Links with criminal organizations: UIAF identified and focalized the network that lent its services to launder resources.
4. Case impact analysis: UIAF quantified the negative economic impact caused by the case, which was three times higher than the volume of money that flowed into Colombia's licit economy.
5. Case closure: Based on the financial intelligence submitted to prosecution authorities, it was possible to initiate the judicial process simultaneously in Colombia and a North American country.

Outcome/Contribution of the Case

The total amount of the case is estimated, based on foreign exchange transactions carried out with Colombia in the 2004–2013 period, to have reached USD 906 million (COP 1.7 billion), involving 32 companies and 34 people. If this amount had not been a product of illicit activities, it could have contributed to the creation of 210,000 jobs in the country, among other positive economic impacts in Colombia.

Through working groups that were carried out during the application of the whole intelligence cycle — in which Colombia's Attorney General's Office, foreign intelligence agencies and the UIAF participated — it was possible to produce feedback among participants, thus benefiting the overall case comprehension and data corroboration. The intelligence that was gathered essentially fulfilled its purpose of serving as a lead for prosecutors to perform their judicial investigation both in Colombia and in a North American country. In the latter case, the prosecution has already begun.

The intelligence practices applied in this case for the dismantlement of a money laundering and terrorism financing network could serve as a reference to other FIUs in terms of cooperation and exchange of information mechanisms. As this case demonstrates, these mechanisms yield results. Most importantly, they exemplify the impact of financial intelligence, as well as economic intelligence overall, on the investigative and judicial tasks that ultimately must be carried out by the competent authorities.

Valuable Indicators of the Case

- Mismatch of entrance and exit of foreign trade against the reported data
- Misuse of commercial operations (import and export of textiles) for unjustified money flows
- Links of company executives to drug offences
- Intelligence links to organized criminal organizations
- Traceability of financial information

CASE 14

Amesta — Embezzlement of Public Funds (Italy, UIF)

Introduction

Complex financial analysis by the Italian Financial Intelligence Unit (FIU-Italy) was the impetus for starting a criminal case, leading to the arrest of individuals that were the subject of the investigation. The investigation was launched on the initiative of the FIU within the liquidation sector of companies and public bodies, in the absence of suspicious transaction reports and according to a proactive approach.

The financial analysis focused on the public company Amesta, which is indirectly controlled by the Ministry of the Economy. Amesta was set up to manage insolvency procedures for public entities.

The Investigation

The in-depth analysis began by checking all the bank movements carried out by Amesta, seeking, in particular, outcoming transactions that could indicate the intention of diverting funds, and ended with a solid suspicion of **EMBEZZLEMENT**. The analysis, on the other hand, highlighted the presence of various wire transfers ordered by private companies to Amesta, with reasons for payment linked to the sale of assets managed by Amesta (credits and share capital of public entities in liquidation). In one case, a company that had purchased a credit paid it to Amesta with the funds obtained from the payment of the credit itself; this circumstance, which resulted in being an undeniable advantage for the acquiring private company (which had operated in a substantial absence of risk in the purchase of credit by Amesta), led FIU-Italy to analyze all transactions in the accounts of Amesta that were attributable to the sale of claims or assets. Therefore, the banking system and the Revenue Agency provided various transfer contracts that related to the purchase and sale of assets that were tied to the identified banking transactions. Various anomalies became apparent.

Keywords	fraud, embezzlement, corruption, public funds
Countries involved	Italy
Sectors involved	Public sector

Among the private transferee companies, one in particular emerged as the counterpart of numerous trades: the holding company called Gesta.

Amesta sold to Gesta, among other things, the majority share capital of an entity in liquidation at a price much lower than the nominal value of the shares. Through an in-depth analysis of the financial statements of the transferred entity, FIU-Italy found that, at the time of sale, an unquantified item was present that contained a pending litigation. The litigation was defined with a sentence issued about a year later, which established that Gesta was creditor for some tens of millions of Euros, an amount not included in the balance sheet of the entity at the time of the transfer to Gesta.

In addition, the financial statements of the company sold to Gesta included securities with a value of EUR 3.5 million that were close to maturity. The intermediary that should have repaid Gesta (the new owner of the entity) the amount equivalent to the securities, who was previously contacted by FIU-Italy for further information, advised FIU-Italy of the upcoming transaction. In December 2016, FIU-Italy postponed the repayment operation, under the powers established for the FIU by legislation. FIU-Italy had been cooperating with the competent Public Prosecutor's Office, which seized the entire transferred entity, taking it away from Gesta and appointing a judicial administrator.

Based on the hypothesis that a series of prearranged acts were aimed at providing an advantage to the private parties in the sales transactions, with consequent damage to Amesta's assets, FIU-Italy analyzed the bank reports of Amesta's directors. The analysis was looking to verify the presence of operations that could constitute an economic advantage perceived by the aforesaid public employees. The following significant aspects emerged: a Gesta transfer of a significant amount was credited to a current account of an Amesta administrator with the reason for payment linked to the purchase of luxury goods. Another Amesta administrator repatriated a few million Euros from Southeast Asia. Based on exchanges with foreign FIUs and investigative evidence, these funds proved to be a donation by Gesta for operations carried out to the detriment of public assets.

FIU Action

The anomalies that emerged in the course of the analysis were of such amplitude and relevance that FIU-Italy carried out an inspection at the bank that managed most of Amesta's current accounts. The on-site inspection enabled not only the analysis of the operations carried out but also a verification of the paperwork acquired by the bank.

Evolution of the Case

FIU-Italy forwarded to the Public Prosecutor's Office a report containing all the anomalous elements revealed. The Public Prosecutor's Office considered the evidence well founded and opened a criminal proceeding for alleged fraudulent conversion of public funds. At the same time, it requested the collaboration of FIU-Italy in the continuation of the investigations. Those efforts lasted for several months, during which a synergic and fruitful in-depth study was carried out. In June 2018, three directors of Amesta and one Gesta director were arrested; nine other individuals were investigated for embezzlement. The estimated damage amounts to more than EUR 60 million.

Outcome/Contribution of the Case

A complex system of diversion of public resources emerged, quantified in tens of millions of Euros, for the benefit of private parties, that had been set up with the complicity of Amesta's directors. The success and timeliness of the investigations conducted by FIU-Italy, which also intervened in one case by postponing a suspicious but not yet performed operation, safeguarded a large share of public assets and prevented misappropriation by private entities.

Valuable Indicators of the Case

Contracts related to the selling of public assets to private parties, characterized by:

- Sales proceeds significantly lower than the value attributable to the claim, also considering the amount actually collected by the assignee or the presumable solvency of the debtor (e.g., tax credits)
- Sales proceeds liquidated by the assignee to Amesta after the assignee cashed the claim.
- Clauses in the sales contract that expressly excluded the need to document the existence of the credit or that provided for the obligation of confidentiality regarding the existence of the assignment or that unjustifiably postponed the liquidation of the amount
- Private purchasers linked to individuals under investigation, for whom FIU-Italy had previously received suspicious transaction reports

CASE 15

Keeping Fraud in the Family (Monaco, SICCFIN)

Introduction

A huge fiscal fraud and money laundering scheme involved an estimated USD 1.6 billion. This fraud concerns mainly three family members, Brazilian and Polish nationals and a resident of Paraguay. The son is Mr. X, the father Mr. Y and the grandfather Mr. Z. This family owned a Brazilian based company, specializing in the installation of vehicle equipment and armour, that was reportedly sold in 2003.

The Investigation

The case started with a suspicious transaction report (STR) sent to the Financial Intelligence Unit (FIU) in Monaco, SICCFIN, by a local bank (Bank A) regarding unusual activity by its customer.

Keywords	international money laundering
Countries involved	Monaco, Brazil, Poland, Paraguay, British Virgin Islands, Liechtenstein, Luxembourg
Sectors involved	financial

Bank A opened an account for a British Virgin Islands (BVI)–based company, Company 1. It was owned by a trust incorporated in Liechtenstein, whose trustee is also incorporated in Liechtenstein. Mr. X and a foreign-based foundation were declared the beneficial owners. These beneficiaries were designated in 2014 and replaced Mr. Y and Mrs. Z (Mr. Z's widow).

The funds in Bank A were sent by Company 2, another BVI-based company, whose account was opened with another local bank, Bank B, which ultimately terminated the customer relationship.

According to the elements communicated by Bank A in the STR, the funds originated from business activities of Mr. Z and Mr. X. The total amount of assets declared by the bank was approximately USD 11 million.

Following the information given by a foreign FIU, Company 2 received USD 20 million in late 2014 from Company 3, another BVI-based company. The ultimate beneficial owner of Company 3 is Mr. Y. The incoming transfer was justified by Mr. X, however, by the fact that he is the ultimate beneficial owner of the Company 3.

Another foreign FIU confirmed that Company 3 owns an account in its jurisdiction at Bank C. The beneficial owner is Mr. Y and his daughter, Mrs. L (Brazilian citizenship), who has power of attorney on the account.

The same foreign FIU informed SICCFIN that the Federal Prosecutor in Brazil approached the Ombudsman and asked for an arrest of a gang of foreign exchange brokers and entrepreneurs that committed **CRIMES AGAINST THE FINANCIAL SYSTEM** in Brazil. The Brazilian authorities obtained 12 arrest warrants and 28 search and seizure warrants, carried out by the Federal Police. According to the same source, the total amount of concealed and **LAUNDERED ILLICIT ASSETS** had reached tens of millions of dollars and may be the proceeds of several highly profitable crimes, mostly from fraud. The financial engineering to hide the assets from the authorities was designed and implemented by the offices of foreign exchange brokers, two of which were owned by Mr. X and Mr. Y. It appears that Mr. Y maintained and managed several accounts belonging to a Brazilian foreign exchange. It was also confirmed that Bank C received an order to transfer USD 150,000 from the Company 3 account to Mr. Y's account in Bank D in Paraguay. Bank C also received an order to transfer USD 20 million from the Company 3 account to the Company 2 account in Monaco.

Mr. Y, Mr. X's father, is under a warrant of arrest issued by a Criminal Court in Brazil for alleged involvement in an international scheme of **MONEY LAUNDERING** and exchange controls fraud. He is wanted by **INTERPOL** and by the Federal Police of Brazil. The Supreme Court of Justice of Paraguay also reportedly issued a court order of arrest and extradition.

Brazilian authorities suspended all procedures against Mr. Y.

Moreover, a confidential database reported that Mr. X, since 2018, has been in the process of being prosecuted on charges of **MONEY LAUNDERING** and he is the object of an international arrest warrant issued by a judge in Paraguay.

At a national level, SICCFIN made requests to local police services. The information received confirmed that Mr. X and Mr. Y are cited in the INTERPOL database on the basis of an arrest warrant for extradition by Paraguayan judicial authorities for money laundering, violation of foreign exchange regulations, fraud and criminal conspiracy. To complete the financial analysis, SICCFIN sent requests to Bank A and Bank B. SICCFIN also cooperated with a third foreign FIU regarding Company 3 and Mr. X, based on an STR involving possible money laundering. On July 4, 2018, Bank A informed SICCFIN that Company 1 wanted to transfer all of its funds to an account in the United States (approximately USD 11 million). Based on SICCFIN's findings, the financial analysis was sent to Monaco's judicial authorities through the General Prosecutor.

Evolution of the Case

To prevent the transfer of the funds from Monaco to the United States, SICCFIN opposed the July 2018 transaction. In that respect, Monaco judicial authorities impounded all the assets held by Company 1 at Bank A. This decision was based on the fact that the business activities of the beneficial owners of Company 1 were closely linked to the activities of Mr. Z and that Mr. Y, who seem, according to Brazilian justice, to be part of the "brains" of a vast financial fraud and an international money laundering scheme.

Outcome/Contribution of the Case

As a result of extensive analysis by SICCFIN, funds and securities suspected of being the proceeds of massive fraud were seized and judicial authorities launched a new criminal case.

Valuable Indicators of the Case

- STR identifying unusual financial activities involving members of the same family
- Suspect subject to judicial proceedings abroad
- Insufficient explanation regarding origin of funds
- Unexplained transfers between company accounts
- Poorly informed transfer schemes with foreign territories of offshore financial centres

CASE 16

Playing a Shell Game with Cross-Border Electronic Transactions (Namibia, FIC)

Introduction

The Financial Intelligence Unit (FIU) for Namibia, the Financial Intelligence Centre (FIC) received a suspicious transaction report (STR) from a local bank on multiple large electronic fund transfers (EFTs) made from a foreign-based bank account of entity A into two Namibian-based bank accounts of entities B and C. On request, funds were converted into U.S. currency and almost immediately transferred electronically to about 18 foreign jurisdictions, with the majority transferred back to the originating account and one other company in a foreign country.

Swift action between the FIC, the Namibian bank, Namibian Police Force and Office of the Prosecutor-General resulted in the restriction of the funds, a preservation application and eventual forfeiture of the money.

The Investigation

In mid-2014, the FIC received an STR from a bank. The STR prompted the analysis of the bank account statements of two newly registered Namibian-based entities, which received more than NAD 70 million during March 2014 and June 2014. The funds were converted into U.S. dollars and transferred to 18 foreign jurisdictions. Most of the money was returned to the originating account and the account of another entity in a foreign jurisdiction. A well-orchestrated pattern of EFT payments was observed: funds were first transferred in smaller portions to the Namibian-based accounts (entities B and C) and then transferred to foreign jurisdictions before the next batch was transferred (to ensure that no bulk amount remains in the account at any given time). The amounts transferred grew into thousands and then millions.

Keywords	electronic funds transfer payments, EFTs; shell companies, financial analysis
Countries involved	Republic of Namibia, South Africa and 18 others
Sectors involved	law enforcement, financial

Analysis and scrutiny of account-opening documents further revealed that entities B and C were registered with legitimate passports issued on false documentation. For example, the identity number of the entity director did not exist nor could his picture or names be linked to any particular person.

The accounts for entities B and C were restricted and the intelligence shared with the Namibian Police Force and Office of the Prosecutor-General. Investigations further revealed more discrepancies, i.e., the entity addresses provided did not exist and individuals listed could not be found. Five more individuals were identified as recipients of legitimate passports with false information, as was an immigration officer who received a significant EFT payment, a day after the issuance of those fraudulently issued passports.

The Prosecutor-General applied to the courts for a preservation order and was able to confiscate more than NAD 700,000 (about USD 47,000) during January 2015.

Charges of **MONEY LAUNDERING**, **CORRUPTION**, **FRAUD** and **EMBEZZLEMENT** were laid and investigated by the Namibian Police Force. The immigration official was also charged.

FIU Action

On receipt of the STR from the bank, the FIC identified the foreign-based source account of the funds transferred into the two Namibian-based accounts of entities B and C. In January 2015, the FIC restricted more than NAD 700,000 (about USD 47,000) in the accounts, and shared the intelligence with the Namibian Police Force and the Office of the Prosecutor-General.

The FIC also involved the foreign FIU to source intelligence on the involved accounts.

The FIC continuously and closely assisted law enforcement agencies (LEAs), as well as financial institutions and the foreign FIU. Further scrutiny confirmed:

- entities B and C were fraudulently registered with fake particulars;
- an immigration official received a sizable EFT payment from a recipient of a fraudulently issued passport that was used to set up the entities B and C — the official was arrested and charged; and
- five additional passports were fraudulently issued.

As a result, the funds were restricted.

Evolution of the Case

The FIC's financial analysis and investigation on the matter was completed within weeks. With the intelligence provided, LEAs, particularly the Namibian Police Force, were able to conduct further investigations before arresting a suspect, the immigration official. The Office of the Prosecutor-General was also able to successfully bring a preservation application before the High Court of Namibia.

Investigative methods included gathering, collating and analyzing information received from the local bank, the Ministry of Trade and Industry, the Ministry of Home Affairs and Immigration, the Deeds Office, and internationally through the FIC's foreign counterparts.

Investigations confirmed that the locally involved entities were fraudulently registered with falsified passports. This confirmed that the suspects wanted to deliberately conceal their involvement in the transfer of funds into and out of the local entity accounts.

Outcome/Contribution

of the Case

The Namibian Police Force finalized the investigations and the matter is with the Office of the Prosecutor-General for prosecution and trial. Arrest warrants were issued for the directors of the fraudulently registered local entities A and B. Investigations and collaboration resulted in the forfeiture of more than NAD 700,000 (about USD 47,000) from the local accounts of entities B and C in January 2015.

Valuable Indicators of the Case

- Large EFT payments received into newly opened accounts of entities B and C over a short period (more than NAD 70 million during the March–June 2014 period
- Structured payments made by the subjects into the entity B and C accounts, starting with smaller amounts gradually increased to millions
- Accumulation of funds in the accounts of entities B and C to less than a million that were transferred out of the account on the same day to ensure that no huge amounts are in the accounts at any given time
- The creation/registration of untraceable (shell) entities (entities B and C) using them to move funds electronically
- Use of passports issued based on fraudulent credentials to open the accounts of entities B and C

SMUGGLING AND GAMBLING

Money launderers have devised an infinite number of schemes to hide the large sums that are generated by illicit businesses. This section analyzes how smuggling and gambling are related to money laundering.

On the one hand, the large sums of money from smuggling need to be laundered. One of these cases relates to tobacco and cigarette smuggling. In this sector, there is a financial incentive to source a product in a lower-priced market and transport, distribute and sell it in a higher-priced market. This can include international movements or movements within countries that allow for intra-community price differentials. Illicit trade in tobacco is made up of various activities. Smuggling is conducted for one or both of the following reasons: to avoid excise taxes, and to evade rules prohibiting the sale of such goods.[10]

10 Financial Action Task Force (FATF), *Illicit Tobacco Trade*, June 2012, https://www.fatf-gafi.org/media/fatf/documents/reports/Illicit%20Tobacco%20Trade.pdf

On the other hand, gambling is another avenue for money laundering, in particular in casinos. By definition, casinos are non-financial institutions. But as one of these cases shows, however, the variety, frequency and volume of casino transactions makes this sector particularly vulnerable to money laundering. Casinos are by nature cash-intensive and the majority of transactions are cash based. As part of their operations, casinos offer gambling for entertainment, but also undertake various financial activities that are similar to financial institutions, thus providing a means of money laundering.[11]

Knowledge of money laundering methods in this sector provides government decision-makers and operational experts a foundation for policies and strategies to combat financial crime. Measures that can help prevent money laundering in this sector include identifying red flags, using a risk-based approach, and reinforcing the duty of employees to report to their officer any knowledge or suspicion of money laundering whether by customers, guests or other employees, among others.[12]

Indicators

Tobacco Smuggling

- Relative maturity of the individuals or groups involved in smuggling
- Mitigation of the risk of detection at source, in transit or at point of sale, as this affects criminal profit margins[13]

Gambling — Casino Sector

- Client produces seemingly false information or identification that appears to be counterfeited, altered or inaccurate
- Pattern of name variations from one transaction to another or use of aliases or counterfeit bank payment cards

11 Asia/Pacific Group on Money Laundering and FATF, *Vulnerabilities of Casinos and the Gaming Sector*, March 2009, https://www.fatf-gafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf

12 United Kingdom, Gambling Commission, "Casinos: Prevention of money laundering," undated, https://www.gamblingcommission.gov.uk/for-gambling-businesses/Compliance/General-compliance/AML/How-to-comply/Casinos-Prevention-of-money-laundering.aspx

13 FATF, *Illicit Tobacco Trade*, June 2012, p. 8, https://www.fatf-gafi.org/media/fatf/documents/reports/Illicit%20Tobacco%20Trade.pdf

CASE 17

Disrupting Tobacco Smuggling in Australia (Australia, AUSTRAC)

Introduction

The Financial Intelligence Unit (FIU) in Australia, AUSTRAC, contributed to a joint Australian law enforcement investigation into a syndicate that imported illegal tobacco and cigarettes from the United Arab Emirates (UAE) and Indonesia. The investigation ultimately led to the arrest and sentencing of six offenders, and the seizure of 72 tonnes of tobacco and several million cigarettes with an estimated potential profit value ranging from AUD 35 million (USD 33.9 million) to AUD 45 million (USD 43.5 million). It was also the catalyst for additional collaboration between the Australian and Indonesian FIUs into the smuggling of illegal tobacco into Australia.

The Investigation

A joint law enforcement investigation identified an Australian syndicate involved in the **ILLEGAL IMPORTATION OF TOBACCO AND CIGARETTES** from the UAE, Indonesia, Singapore and Malaysia. The joint investigation involved a multi-agency task force, comprising Australian law enforcement agencies and AUSTRAC, that worked to detect, deter, and disrupt serious and organised criminal group activities on Australia's waterfronts.

Keywords	account and deposit-taking services, remittance services, illegal tobacco importation
Countries involved	Australia, Indonesia, United Arab Emirates
Sectors involved	banking — authorised deposit-taking institution

The syndicate was assisted by a freight forwarding services company and a transport services company. These complicit entities received cash payments from the syndicate for assisting in the illicit importations. Both the complicit freight forwarding services and the transport services company facilitated the crime by checking the clearance status of containers, alerting the syndicate whether law enforcement had any interest in the containers, and arranging container collection from the wharf. The freight forwarder also provided a storage facility for the illicit imports and helped unpack containers. Law enforcement identified several storage units used to store tobacco and cover loads.

During the investigation, AUSTRAC provided financial analysis relating to the syndicate members and their associates. This analysis identified financial transactions used to purchase the tobacco and cigarettes, specifically involving funds flows to the UAE and Indonesia.

AUSTRAC analysts primarily used internal data holdings consisting of financial transaction reports and suspicious matter reports (SMRs) submitted by reporting entities, including banks. The syndicate was remitting funds via international funds transfer instructions (IFTIs) to companies in the UAE and Indonesia through personal and business accounts. Many of the IFTIs were funded by large cash deposits made by syndicate members.

Details of AUSTRAC's analysis of its own data holdings is provided below, in addition to relevant SMRs that provided visibility of the syndicate's suspicious financial activities. AUSTRAC disseminated its analysis to relevant law enforcement agencies.

FIU Action

Analysis of AUSTRAC Data

AUSTRAC analysed transaction reports submitted by reporting entities and referred them to law enforcement to assist with the investigation. AUSTRAC analysis of IFTIs and threshold transaction reports (TTRs) identified the transactions associated with the purchase of illicit tobacco products from the UAE and Indonesia by the syndicate (see diagram). [Insert diagram somewhere around here] The analysis revealed the following:

- The freight forwarding business was associated with an export company. The export company was linked to businesses and individuals involved in illegal cigarette importations. In one year, the director of the freight forwarding business sent AUD 38,200 (USD 36,960) from personal and business accounts to the export company.
- Over a four-month period, 17 IFTIs were sent to a tobacco company in the UAE totalling approximately AUD 638,000 (USD 617,270). The IFTIs were predominantly valued between AUD 23,000 (USD 22,250) and AUD 47,000 (USD 45,470).
- Most of the 17 IFTIs sent to the UAE tobacco company stated "building materials" as the reason for transfer and eight were remitted from the same branch of a bank, by seven different ordering customers.
- The TTRs showed five of the IFTIs were funded by cash for amounts between AUD 29,000 (USD 28,060) and AUD 49,000 (USD 47,410).
- One IFTI was sent through the account of an Australia-based business operated by a syndicate member. The business was identified as a hairdressing company.
- Over a four-year period, eight IFTIs were sent to a food export company in Indonesia, and to the account of an individual listed as a manager in a tobacco business, totalling AUD 286,620 (USD 277,300). The IFTIs were valued between AUD 7,160 (USD 6,930) and AUD 62,700 (USD 60,660).

Analysis of SMR Data

Multiple SMRs submitted by banks revealed the transaction activity of the syndicate, particularly in relation to unusual cash deposits (some of which were used to fund IFTIs), as well as the destination of the IFTIs. The SMRs revealed the following transaction activity:

- Syndicate members tried to deliberately disguise the origins of funds by making cash deposits and withdrawing the funds as bank cheques.
- The customers made single cash deposits of between AUD 100,000 (USD 96,750) to AUD 260,000 (USD 251,550) and were reluctant to provide information on the origins and use of the funds. On the same day of each deposit, bank cheques were drawn payable to different banks for similar or equivalent amounts as the preceding deposits.
- Large cash deposits totalled over AUD 300,000 (USD 290,250) in a two-week period. The cash was carried into the bank in large garbage bags consisting of AUD 50 and AUD 20 denominations.
- Three IFTIs valued at approximately AUD 30,000 (USD 29,030) each were sent to the same tobacco company in the UAE over a three-day period. The ordering customers of the IFTIs were a syndicate member, his company and an associate.
- An employee of a syndicate member's company made aggregate cash deposits of AUD 100,000 (USD 96,750) over seven months. During this period, the employee sent two IFTIs to tobacco companies in the UAE of AUD 24,780 (USD 23,970) and AUD 49,720 (USD 48,100) respectively.

Evolution of the Case

During this investigation, AUSTRAC provided financial intelligence analysis to Australian law enforcement relating to the syndicate members and their associates. The intelligence included assessments produced by AUSTRAC analysts relating to persons of interest both proactively and at the request of law enforcement partners. The analysis identified financial transactions used for the purchase of the tobacco and cigarettes, including funds flowing from Australia to the source countries.

AUSTRAC monitoring systems identified new targets whose transaction behaviour matched illicit tobacco methodologies noted by law enforcement. These persons were identified as sending large cash transfers to a company in Dubai related to two previous detections. They appeared to be either third parties paid by the persons of interest to send money overseas on their behalf or they were investors in the shipments. This intelligence was proactively disseminated to law enforcement.

AUSTRAC also prepared an intelligence report at the request of law enforcement on one of the key persons of interest, who ran the freight forwarding company. It was alleged this person was notifying importers of the tobacco shipments prior to law enforcement interception. In addition to the intelligence report, AUSTRAC analysts also referred relevant SMRs to law enforcement and provided advice with respect to the transactions.

Outcome/Contribution of the Case

After executing search warrants at various residential and business properties, law enforcement arrested and charged six syndicate members and associates:

- Four offenders were charged with "possessing tobacco products knowing that they were imported with intent to defraud the revenue, contrary to section 233BABAD(2) of the *Customs Act 1901*," receiving prison sentences ranging from 15 to 24 months.
- Three of the above four offenders were additionally charged with "attempts to possess tobacco products knowing that they were imported with intent to defraud the revenue, contrary to section 233BABAD(2) of the *Customs Act 1901* and section 11.1 of the *Criminal Code 1995*," receiving additional prison sentences of 24 months.
- One offender was charged with three counts of "importing tobacco products knowing that they were imported with intent to defraud the revenue, contrary to section 233BABAD(2) of the *Customs Act 1901*," receiving a prison sentence of 18 months.
- One offender was charged with "attempting to defraud the Commonwealth, contrary to section 135.1 of the *Criminal Code 1995*," receiving a prison sentence of six years and two months.

Law enforcement seized nine residential properties as proceeds of crime, approximately 72 tonnes of tobacco, and 64 million cigarette sticks found in a container and property searches. Additional seizures included approximately AUD 224,000 (USD 216,720) in cash, a seven-metre luxury boat valued at AUD 70,000 (USD 67,730), and four cigarette filling machines.

Although this investigation did not directly involve international FIU cooperation, the identification of the syndicate and, in particular, the Indonesian beneficiaries of funds, became the catalyst for joint collaboration between AUSTRAC and its Indonesian counterpart, the Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK).

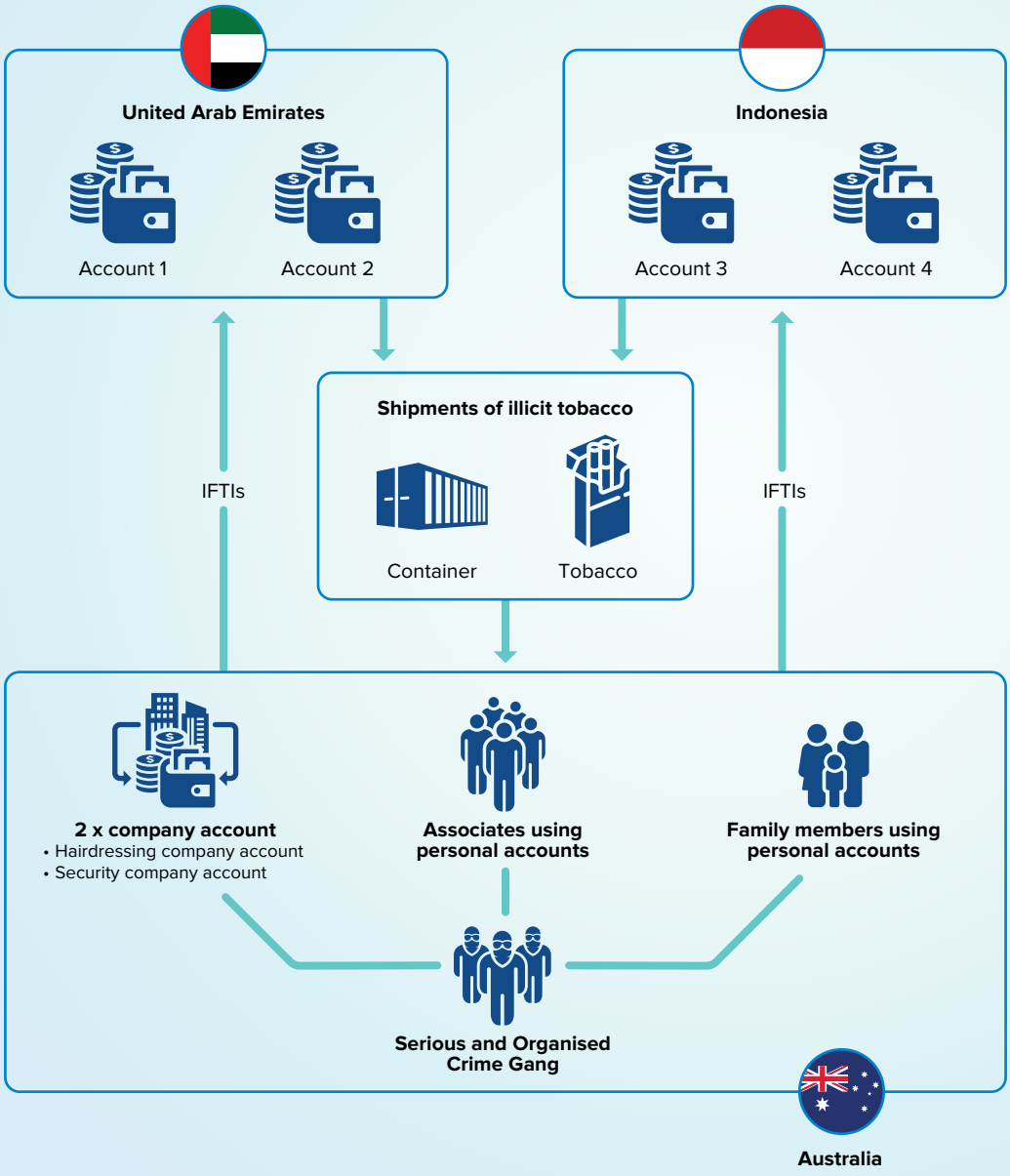
The collaboration led to the production of an intelligence report that was prepared as part of a pilot analyst exchange program between PPATK and AUSTRAC. This AUSTRAC–PPATK analyst exchange program enabled analysts from both agencies to work together to support ongoing Australian and Indonesian law enforcement investigations into the alleged importation of illegal tobacco from Indonesia to Australia.

The report was produced to largely support efforts by Australian and Indonesian law enforcement to disrupt the operations of entities in Australia and Indonesia. It was disseminated widely across domestic law enforcement agencies to support ongoing intelligence work. Based on the successful cooperation between Australia and Indonesia and the mutual benefits realised by both FIUs, AUSTRAC and PPATK analysts have since then, continued to work collaboratively on further investigations and operational matters.

Valuable Indicators of the Case

- Multiple IFTIs in excess of AUD 20,000 (USD 19,350) sent to a South-East Asian or Middle Eastern country, e.g., Indonesia or the UAE
- Multiple ordering customers sending international wire transfers to the same beneficiary customer
- A domestic company remitting funds to an overseas company not in the same industry or business services, e.g., a hairdressing business remitting funds to an overseas tobacco supplier
- The reason for transfer stated on the international wire transfer does not match the business services of the company receiving the remittance (i.e., the IFTIs sent to a tobacco supply company where the reason for transfer states “building supplies”)
- Large cash deposits followed by international wire transfers sent to companies associated with tobacco supply

AUSTRAC'S ANALYSIS DIAGRAM



CASE 18

Gambling with Counterfeit Cards and Counterfeit Customers (Belarus, FIU-Belarus)

Introduction

The founder of a casino somehow obtained counterfeit bank payment cards to generate criminal income. He also was able to produce counterfeit bank cards with special equipment and software. Further, this individual used the payment terminals on the casino premises and counterfeit bank payment cards to transfer money stolen from foreign banks into the casino's account. He "legalized" or laundered the stolen money through fraudulent accounting that made the money appear as the losses of casino customers. Then he entered the false information into the automated system of the tax authority, which tracks the casino payouts.

The Investigation

The Financial Intelligence Unit (FIU) in Belarus received suspicious transaction reports (STRs) from a Belarusian bank with information about 46 financial transactions carried out with 31 bank payment cards connected with transfer of money from accounts of foreign banks (11 U.S. banks, 4 Brazilian banks, 1 Chinese bank) to the account of a Belarusian casino.

Keywords	smuggling, gambling
Countries involved	Republic of Belarus
Sectors involved	banking, gambling

The founder of casino C, Citizen A, obtained counterfeit bank payment cards, though it is unclear how he did so. Citizen A then used the counterfeit bank payment cards to transfer money into the account of the casino C by using the casino's payment terminal. Citizen A ordered his employees, who were not aware of the crime, to doctor the accounting to show that the stolen money was received from casino clients to buy gambling chips.

Through these activities, Citizen A attempted to steal about USD 320,000. The banks that issued the payment cards rejected several transactions, however, so Citizen A transferred money from accounts of foreign banks into the casino's account in amount of USD 107,000.

Citizen A used the stolen money to support the casino — for payment of taxes, fees for advertising services, and alcohol and other goods.

One month after stealing USD 107,000, Citizen A acquired the protected and confidential information about details of bank payment cards, also under unclear circumstances. Citizen A used specialized software and equipment to write the specified information on plastic cards, thus using illegally obtained information and making unauthorized copies.

Citizen A reached an agreement with the owner of casino N to acquire casino N or for casino N to undertake a joint activity with casino C to repay casino's N's tax debt. After this agreement was reached, Citizen A attempted to steal money while inside casino N in the sum of USD 82,000 by using the payment terminal and the details of the bank payment cards. The banks that issued the bank payment cards rejected several transactions, so Citizen A ended up transferring about USD 11,000 to the account of casino N.

Once more, Citizen A doctored the accounting of the transferred funds to be reflected as the purchase of gambling chips by casino customers. This now-laundered money was transferred for repayment of casino N's tax debt.

FIU Action

FIU-Belarus received the STRs from the Belarusian bank because the issuing banks had recognized the transactions as fraudulent when the holders of the cards confirmed that they did not conduct the transactions or authorize them.

FIU-Belarus initiated the investigation and supported the Department of Internal Affairs of the Republic of Belarus by providing information from the STRs and other databases available to FIU-Belarus, as well as its analysis.

Evolution of the Case

The law enforcement authority inspected the casino. Surveillance camera footage was reviewed and mobile activity was analyzed. The inspection found documents showing the transfer of the stolen money to the casino's account. Further, the specified receipts were used as evidence.

The operational search of the casino yielded evidence for the case and inspection of documentation inspections confirmed the facts of the commission of crimes.

Outcome/Contribution of the Case

Citizen A was found guilty of:

- attempting to steal property made in especially large sums;
- using criminal proceeds to conduct financial operations and other transactions; and
- unauthorized copying and obtaining other information illegally.

ПРОИСШЕСТВИЯ

30 МАЯ 2017, 19:03

Владелец брестского казино приговорен к 13 годам за хищения с помощью поддельных банковских карт

30 мая, Минск /Корр. БЕЛТА/. Владелец игорного бизнеса приговорен к 13 годам за хищения денежных средств в особо крупном размере с использованием поддельных банковских платежных карт. Об этом в эфире "Альфа-радио" сообщила

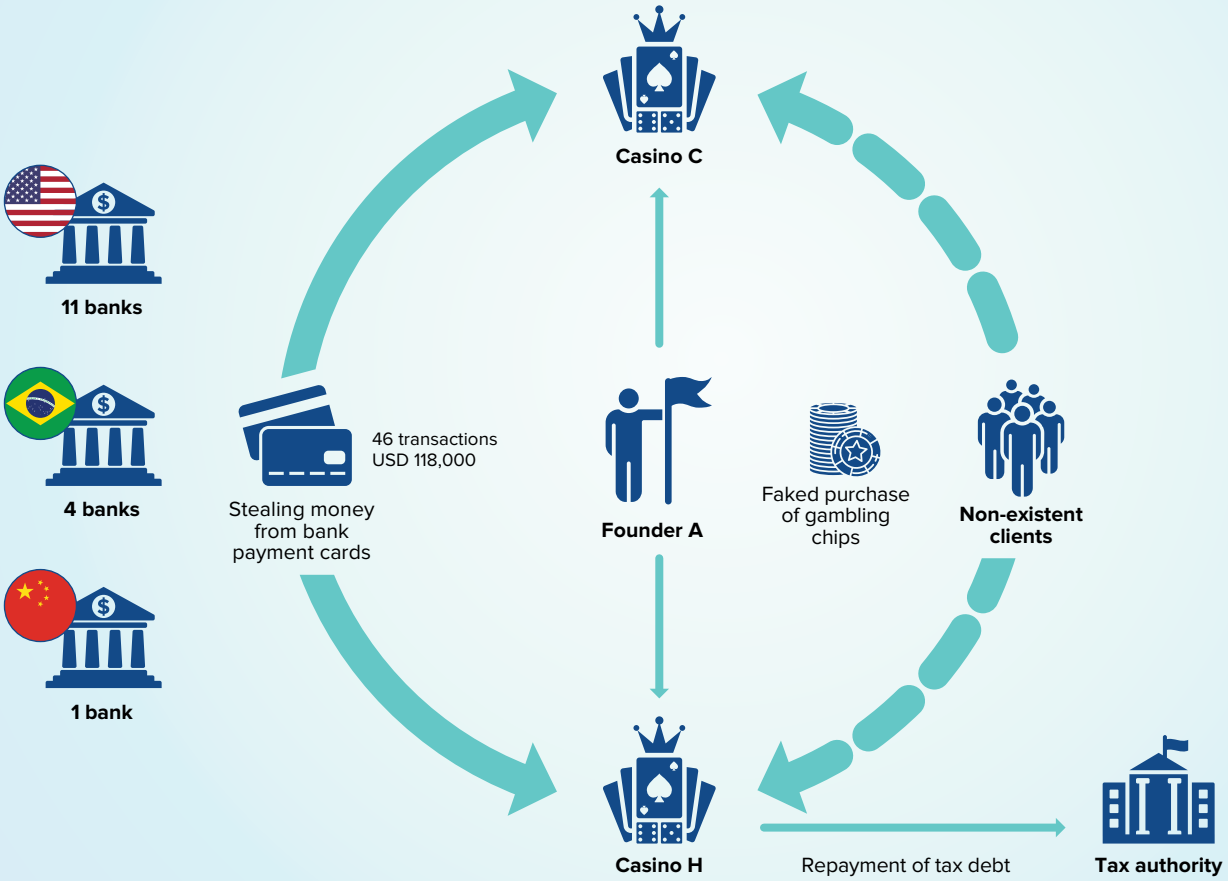
Citizen A was convicted under several articles of the Criminal Code of the Republic of Belarus, including under the article "legalization." He was sentenced to 13 years' imprisonment and the following property was confiscated: 38 gaming machines, a video surveillance system, three game tables, etc. This property was turned over to the state.

Effective collaboration among FIU-Belarus, law enforcement authorities and financial institutions brought the case to a swift four-month conclusion.

Valuable Indicators of the Case

- Transactions using large numbers of payment cards from foreign banks
- Use of casino payment terminal

ANALYSIS OF ML SCHEME



TRADE-BASED MONEY LAUNDERING AND THIRD-PARTY MONEY LAUNDERING

Trade-based money laundering — transactions involving the proceeds of crime disguised as payment for imports, exports and other types of trade to facilitate the movement of illicit money — is the most-used form of money laundering in the world. Further, these schemes often involve professional money launderers that offer specialized expertise and use a range of money laundering techniques to diversify their risk exposure.[14]

According to the Financial Action Task Force (FATF) and the Egmont Group of Financial Intelligence Units (FIUs), the nature of interconnected supply chains

14 Financial Action Task Force (FATF) and the Egmont Group, *Trade-Based Money Laundering: Trends and Developments*, December 2020, pp. 11–12, www.egmontgroup.org/sites/default/files/filedepot/external/Trade-Based-Money-Laundering-Trends-and-Developments%5B1%5D.pdf

stretching around the world make trade inherently complex. Organized criminal groups, professional money launderers and terrorist financing networks exploit these supply chains to facilitate myriad types of financial flows, including: to launder the proceeds of crime, such as from drug trafficking; to finance terrorism; and to evade sanctions. Currently, many customs agencies, law enforcement agencies, FIUs, tax authorities and banking supervisors — that is, competent authorities — have a harder time identifying and combatting trade-based money laundering than other forms of money laundering and terrorist financing. Even authorities with advanced knowledge of trade-based money laundering are impeded by the sophistication and ever-evolving nature of the techniques used.[15]

FIUs play a key role in conducting strategic analyses of their databases to identify ML/TF typologies and emerging phenomena, as well as their ongoing, independent, operative analyses for tracing suspicious targets. In addition, FIUs alert competent authorities to illicit activity that their analyses have identified.

The cases in this section showcase different techniques used by various actors that deal directly or indirectly with trade-based money laundering and third-party money laundering crimes:

- FIU-Bahrain used its swift investigative tools and efficient analytical techniques, supported by domestic and international cooperation, to unravel an international money laundering scheme.
- FIU-Mexico worked with U.S.-based FinCEN to dismantle international money laundering networks involving dozens of entities, a wide range of transactions to dozens of countries and more than 1,500 beneficiaries.
- The Israel Money Laundering and Terrorism Financing Prohibition Authority (IMPA) provided financial intelligence that led to the investigation of a cross-border professional money laundering scheme that piggy-backed on the diamond trade. IMPA's work led to the formulation of the EGMONT/FATF typologies report, *Money Laundering and Terrorist Financing through Trade in Diamonds*,[16] thus contributing to raising awareness of the phenomenon both locally and internationally.
- Korea's FIU furnished the Korea Customs Service with financial information on a fake export/import company that was used to identify various offences, such as false export/import declaration reports, property concealment and money laundering, that were costing Korean import agencies and commercial banks more than KRW 50 billion.

These cases demonstrate how the international nature of these types of crimes demand cooperation from relevant actors, agencies and FIUs, and point to measures that can be implemented to prevent trade-based money laundering and third-party money laundering.

15 FATF and the Egmont Group, *Trade-Based Money Laundering: Trends and Developments*, December 2020, p. 37, www.egmontgroup.org/sites/default/files/filedepot/external/Trade-Based-Money-Laundering-Trends-and-Developments%5B1%5D.pdf

16 FATF and the Egmont Group, *Money Laundering and Terrorist Financing Through Trade in Diamonds*, October 2013, www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf

Indicators

Trade-Based Money Laundering: Trends and Developments lists many red flags, including the following indicators:[17]

- Rapid growth of newly formed companies in existing markets
- Evidence of consistent and significant cash payments, including those directed toward previously unknown third parties
- Numerous cash transactions below a reporting threshold
- Previously established companies specializing in one sector that unexpectedly pivot into an entirely unrelated sector
- Businesses that receive unexplained third-party payments
- Unnecessarily complicated and complex supply chains, involving multiple transhipments
- Companies simultaneously involved in more than one unrelated sector, especially in goods that are difficult for customs to examine or goods with wide pricing margins

17 FATF and the Egmont Group, www.egmontgroup.org/sites/default/files/filedepot/external/Trade-Based-Money-Laundering-Trends-and-Developments%5B1%5D.pdf

CASE 19

Unravelling an International Money Laundering Scheme Tied to Cyberfraud (Bahrain, FID)

Introduction

The Financial Intelligence Directorate (FID), Bahrain's Financial Intelligence Unit (FIU), unravelled an international money laundering scheme after a money exchange institution operating in Bahrain filed a suspicious transaction record (STR). The STR identified an individual who made several overseas cash transfers for amounts that did not match the individual's profile or have a convincing legitimate source. Through domestic and international cooperation, in addition to other investigative techniques, the perpetrators were brought to justice.

Keywords	third-party money laundering, trade-based money laundering
Countries involved	Kingdom of Bahrain, Belgium, India, Denmark, Sweden, Germany, United Kingdom, Norway, United States, France, Canada, the Netherlands
Sectors involved	financial

The Investigation

The initial trigger was an STR filed by a money exchange institution operating in Bahrain, followed by STRs from other institutions. An individual, Subject 1, had been making several overseas cash transfers. The amounts, however, did not match Subject 1's profile and Subject 1 was unable to identify a legitimate source. After analyzing the statements provided by the exchange institutions, it was found that the organization run by Subject 1 and his associates within Bahrain received payments from September 7, 2015, to July 24, 2016, for a total of 179 financial transfers amounting to BHD 105,638 (USD 280,181). The investigation revealed that these payments were the proceeds of CYBER FRAUD crimes in 10 different countries affecting 118 victims. These illegally acquired payments were transferred to 14 different beneficiaries in Bahrain.

The beneficiaries seemed to be of Indian nationality/origin, so a follow-up inquiry was made into the transfer of the funds to the Republic of India. All 14 beneficiaries used eight exchange institutions to make 451 transfers totalling BHD 157,208 (USD 418,107) between January 27, 2014, and May 4, 2017. In checking transfers to India, FID found that eight individuals received them and confirmed that these individuals were under orders from Subject 1 to receive remittances from foreign countries. Subject 1 manages the these transfers on behalf of his friend, Subject 2, and 192 transfers were sent to India between the dates of March 26, 2015, to July 27, 2016, totalling BHD 108,907 (USD 289,647) through seven exchange institutions.

The suspects confirmed that they received a commission of 2% of the amounts received and that some of them handed over their commissions in cash to Subject 1, who transferred these amounts to his bank account in the Republic of India through exchange companies, as well as to the bank accounts of beneficiaries in the Republic of India. Auditing Subject 1's personal bank account in Bahrain found only a deposit of his monthly salary, which is estimated to be BHD 350 (USD 931) and varies according to time spent at work. He sends part of this money to his personal accounts in India.

A further investigation into the organization of the crime of FRAUD through the TalkTalk scam,[18] FID found that two suspects in Bahrain (subjects 3 and 4) received 50 fraudulent electronic transfers between February 17, 2016, and May 21, 2016, from a group of people in the United Kingdom, for a total amount of BHD 82,223 (USD 218,637). Subject 3 received 35 transfers totalling BHD 55,672 (USD 148,064) while Subject 4 received 15 transfers amounting to BHD 26,596 (USD 70,774). These transfers from the United Kingdom were then transferred to three individuals in the Republic of India during the same period through 39 transfers for a total of BHD 87,178 (USD 231,856).

FIU Action

FID pursued further investigative actions:

- The FID database was searched for criminal history, STR records and travel history for all senders and receivers known to that point.
- The accounts of Subject 2 were summoned.
- The phone call registers of both Subject 1 and Subject 2 were obtained.
- The records of all transactions conducted within Bahrain for which Subject 1 and Subject 2 were the main beneficiaries were retrieved.

FID also pursued international cooperation, through the Egmont Secure Web. FID sent requests to five FIUs for the countries of the senders of the transfers. The requests included an inquiry of the funds sent. One FIU responded that multiple senders had filed a complaint with local police regarding an Internet scam that involved hacking personal computers and hoaxing victims into sending funds to one of the subjects in Bahrain, who forwards the money to the original perpetrator, who was located in the Republic of India. FID notified the Republic of India that the origin of the crime is within its jurisdiction.

A meeting was held with other competent authorities within the Bahraini Ministry of Interior, which regularly meets to discuss similar behaviours and trends that are interlinked. From that meeting, a similar case was linked that used the same pattern and a parallel investigation was launched involving FID and INTERPOL.

FID used its authority to question the suspects, which aided in the process of transferring the case to the Public Prosecution Office for investigation.

Public Prosecution investigations uncovered that the suspects' operations were controlled by Subject 1, while the others were forced to conduct these transactions.

Evolution of the Case

The case began with an STR filed by a money exchange institution regarding suspicious transfers of funds by Subject 1, an Indian expat working as a chef in the Kingdom of Bahrain. Subject 1 was flagged because he was transferring funds from different branches of the same exchange house with amounts not exceeding the reporting threshold; in addition, the total amount of the different transactions did not fit Subject 1's financial profile.

FID followed protocol, rating the STR as medium risk, which identified it as needing further investigation. The accounts and records of all transactions conducted by Subject 1 within the Kingdom were summoned, revealing the following:

- Subject 1 received several small-transaction transfers from several other individuals from three countries and then sent similar amounts after a short period to three main individuals in the Republic of India, his country of origin.
- Subject 1 had transferred funds with another individual of same nationality, Subject 2, in Bahrain.

18 BBC News, *Inside the TalkTalk 'Indian scam call centre'*, March 6, 2017, https://www.bbc.com/news/technology-39177981

Outcome/Contribution of the Case

FID was able to locate and trace all of the suspects in Bahrain involved in the case. The suspects were captured and BHD 105,638 (USD 280,952) in illegally obtained funds was seized. The investigation in cooperation with the foreign FIUs helped identify a criminal organization run by Subject 1 and his associates within Bahrain. Under the law in the Kingdom of Bahrain, Article 64 and 111 from Decree-Law No. 4 of the year 2001 regarding the prohibition and combatting money laundering, subjects 1, 2 and 3 were found guilty of MONEY LAUNDERING and CYBER FRAUD and were sentenced to five years in prison and fined BHD 5,000 (USD 13,298).

This case demonstrates the importance of cooperation in solving these types of crimes. Financial institutions are an essential factor to such cases, particularly for raising red flags. It is due to the money exchange institution's vigilance in recognizing probable suspicious activity that FID was first alerted to this case.

The Egmont Group's effectiveness in facilitating smooth and swift channels through which FID could communicate and exchange integral intelligence regarding the case at hand was the crucial factor in untangling this case. The case was no easy feat to investigate considering the sheer size of the cyber fraud network at hand and, thus, cemented Egmont Group's place as an invaluable asset in the war against money laundering.

Foreign FIUs were helpful to the case as their response times allowed for FID to move forward. These FIUs did their due diligence in the intelligence they shared, which was detailed enough for FID to unravel an extensive web of fraudulent transfers. Linking over 10 countries was a group effort that could be achieved only through Egmont Secured Channels and the commitment of each single FIU to providing a thorough report on each request.

Valuable Indicators of the Case

- Individual performing several transactions for amounts below reporting thresholds but, when combined, amount to much more than would be expected for someone of that individual's standing

ANALYSIS OF ML NETWORK

Name	Number of transaction	Total Amount
Receiver 1	48	55,241.359
Receiver 2	18	34,358.360
Receiver 3	18	33,837.932
Receiver 4	2	4,285.050
Receiver 5	3	4,145.925
Receiver 6	77	96,194.560
Receiver 7	14	34,166.654
Receiver 8	12	26,374.348
Total	451	288,604.191

To his personal Account and other Suspected Receiver

3 Money Transfer

1 Cyber Fraud

Subject 1
Managing and Receiving Money Transfers

And 13 individuals receiving money transfer

Through 7 Money Exchange Houses

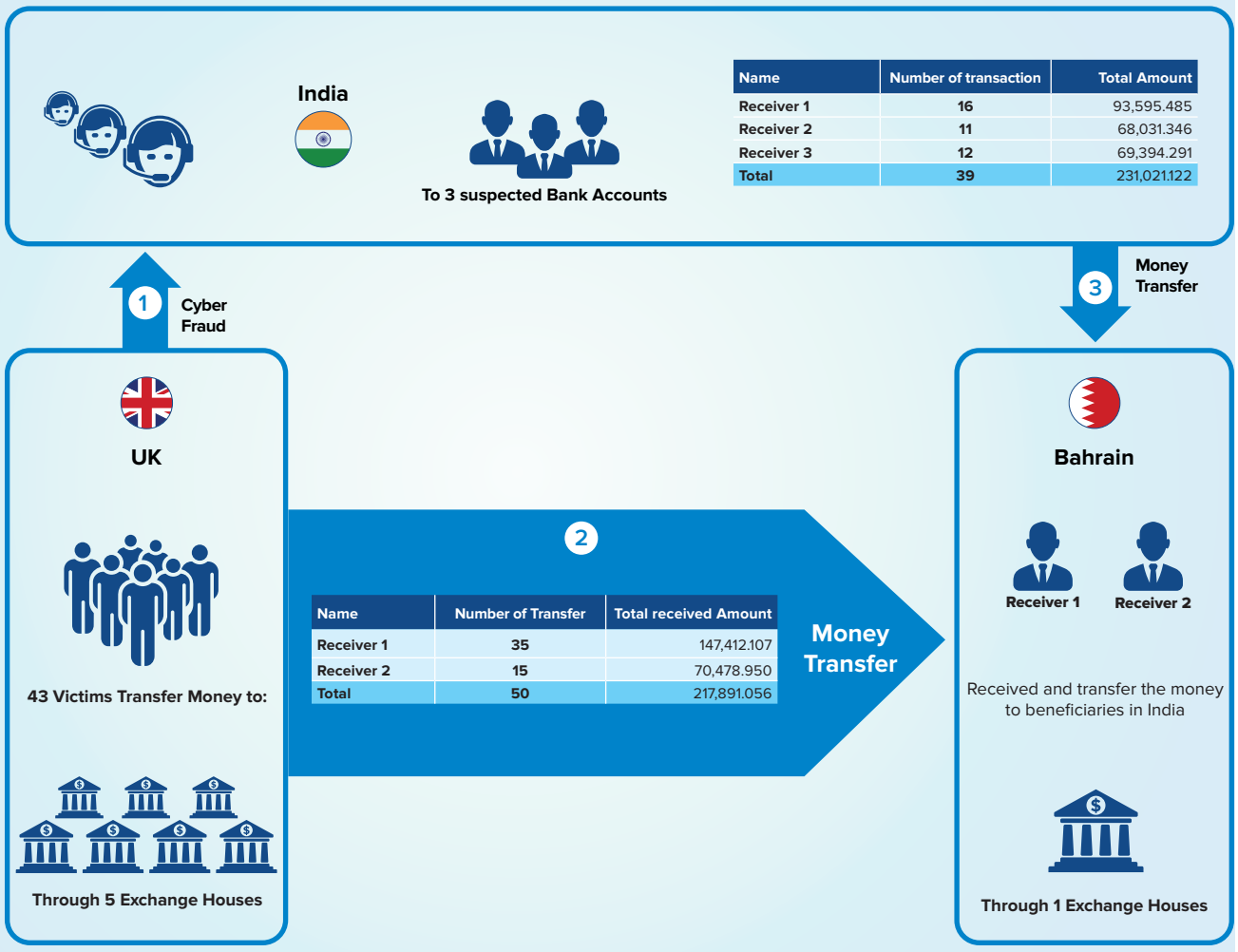
2

Money Transfer

Country	No of Victims	No of Transaction	Total
Denmark	6	6	2375.089
Sweden	5	5	2098.9855
Germany	2	2	2352.4845
UK	9	17	43920.199
Norway	3	3	1012.0615
USA	58	95	184068.2845
Belgium	6	7	3817.325
France	1	1	370.0195
Canada	6	18	29691.6335
Netherlands	22	25	10234.1145
Total	118	179	279940.1965

Through 7 Money Exchange Houses

ANALYSIS OF ML NETWORK



Name	Number of transaction	Total Amount
Receiver 1	16	93,595.485
Receiver 2	11	68,031.346
Receiver 3	12	69,394.291
Total	39	231,021.122

Name	Number of Transfer	Total received Amount
Receiver 1	35	147,412.107
Receiver 2	15	70,478.950
Total	50	217,891.056

CASE 20

Revealing the Many Facets of Cross-Border Money Laundering Scheme Through Diamond Trading (Israel, IMPA)

Introduction

Financial intelligence prepared by Israel's Financial Intelligence Unit (FIU), the Israel Money Laundering and Terror Financing Prohibition Authority (IMPA), led to the investigation of a cross-border professional money laundering scheme through the use of diamonds.

The Investigation

During 2007–2009, IMPA identified a significant growth of several hundred percent in unusual transaction reports (UARs) related to trade in diamonds. These UARs related to very large sums of money, particularly in cash, and international transactions, amounting to millions of New Israeli Shekels for each transaction. IMPA suspected that a scheme involving tax fraud and professional money laundering was taking place within the Israeli Diamond Exchange (IDE). To see if an investigation was warranted, IMPA initiated a comprehensive strategic review and analysis.

Keywords	professional money launderers, diamond industry, TBML, joint task force, underground bank, tax fraud, customs offences
Countries involved	Israel
Sectors involved	MSB, diamond industry

IMPA's research exposed vulnerabilities in the diamond industry due to certain aspects of the trade, including: the extensive use of cash, the transferring of very large sums for each individual transaction, the ease of transferring funds internationally without being detected, and the ease of manipulating the expertise required to evaluate the value of diamonds.

Based on these findings, IMPA analyzed its database and discovered that specific diamond dealers were using their companies to launder funds through different schemes, including: transfers to/from foreign entities that were not related to the diamond industry; use of fictitious invoices made out to entities different from those sending the funds; money service business (MSB) activity by diamond companies under the guise of import/export of diamonds; diamond dealer accounts used solely as a mean to funnel funds; and more. Information also indicated that funds were sent through the accounts of diamond dealers suspected abroad of tax fraud and illegal trade in diamonds. Possible links to criminal organizations were also identified.

The money laundering risks identified by IMPA and subsequent intelligence reports it disseminated brought the IDE to the attention of the relevant Israeli law enforcement agencies (LEAs). A money laundering investigation was launched by the Joint Task Force on Professional Money Launderers, which was established specifically to investigate such activities, including professional money laundering, underground banking through the use of unregistered MSBs, false import/export documentation and false invoices, as well as tax and customs offences, forgery and fraud.

The Task Force brought together permanent representatives from several LEAs (police, tax authority, IMPA and prosecutors) to work jointly on the investigation. The investigation revealed two main intertwined schemes:

- Underground banking — The suspects provided financial services such as cheque clearing, currency exchange, international transfers and loans, though they did not register as MSBs or file any reports with IMPA.
- Fictitious trade — These financial services were carried out under the guise of diamond trade by using false declarations and fictitious diamond export/import documentation and false invoices.

"Customers" of the underground bank gave the suspects illicit cash in a secured room within the IDE complex. The cash was then deposited into the accounts of complicit diamond companies and commingled with their legitimate diamond trade activity. The diamond companies then returned the laundered funds to the customers under the guise of legitimate diamond trade. This was done through several means including cheques, accepted IOU notes, or local or international transfers.

To overcome the requirements imposed by the banks to approve these international transfers, the diamond dealers provided fraudulent customs documentation regarding the value of the diamond deal. This was attained through the following process: the dealers would carry into Israel imported parcels of low-value gems, which they would then replace with real high-value gems taken from another diamond dealer in Israel, then reseal the package to appear as if it had never been opened. The parcel was then declared at the customs station within the IDE and the necessary customs documentation was obtained and provided to the bank, which then approved the transfer, typically in several millions of U.S. dollars.

FIU Action

IMPA was the driving force behind revealing the professional money laundering scheme and eradicating the criminal activity from the IDE.

IMPA played a fundamental role in recognizing the suspicious reporting, researching and analyzing information in its database, alerting relevant LEAs, and providing considerable financial intelligence to the investigation.

The research and analysis methods used by IMPA included:

- conducting an extensive strategic analysis and providing a comprehensive review of the diamond industry, including identifying vulnerabilities and typologies;
- proactively disseminating intelligence reports including suspicions of money laundering offences by suspects prior to the initiation of the investigation;
- during the investigation, conducting further examinations on all of the involved entities in IMPA's database, as well as other databases, to gather more in-depth intelligence information;
- using IMPA's Alert Center to screen the database to identify reports related to the diamond sector and involved entities; and
- searching for keywords to identify entities relating to the diamond industry in UARs.

As part of its participation in the Task Force, IMPA received information requests throughout the investigation regarding the entities involved, and shared the findings with all members of the Task Force. IMPA provided an analysis and evaluation of the financial data, including a description of the suspicious activities, typologies identified, offences committed by the entities involved in the scheme and the amounts laundered.

Information requests were sent to foreign FIUs where financial activity related to the scheme was identified. The information received assisted IMPA in understanding the scope and logic of the scheme, and in detecting other entities involved, as well as contributed to facilitating the process of obtaining evidence by applying for Mutual Legal Assistance. As such, this case serves as an example of the importance of cooperation between FIUs through the Egmont platform.

Evolution of the Case

The professional money laundering scheme facilitated false diamond deals for enormous amounts despite no actual diamonds exchanging hands. Israeli authorities proved that in total approximately USD 800 million was laundered, with intelligence indicating that the total amount of laundered funds was in fact much higher.

A total of 28 indictments were served as a result of the investigation, all ending in convictions. The three main suspects who managed the underground bank were convicted of **MONEY LAUNDERING** and other offences, and their sentences included prison terms of 10 (later reduced to 7.5), 4 and 5.5 years; fines amounting in total to ILS 1,875,000; and asset recovery orders totalling ILS 19 million.

The investigation also provided information used by the Israeli Tax Authority for further criminal investigations for tax fraud and civil proceedings.

Outcome/Contribution of the Case

IMPA's work led to the formulation of the Egmont–Financial Action Task Force Typologies Report on ML/TF Through Trade in Diamonds, thus contributing to raising awareness of the phenomenon both locally and internationally. The case contributed to closing various regulatory and taxation gaps in the IDE and triggered a significant change in Israel's anti-money laundering regime. The case also exemplifies the close cooperation between all relevant LEAs within the framework of a joint investigation conducted by a designated Task Force combatting professional money laundering.

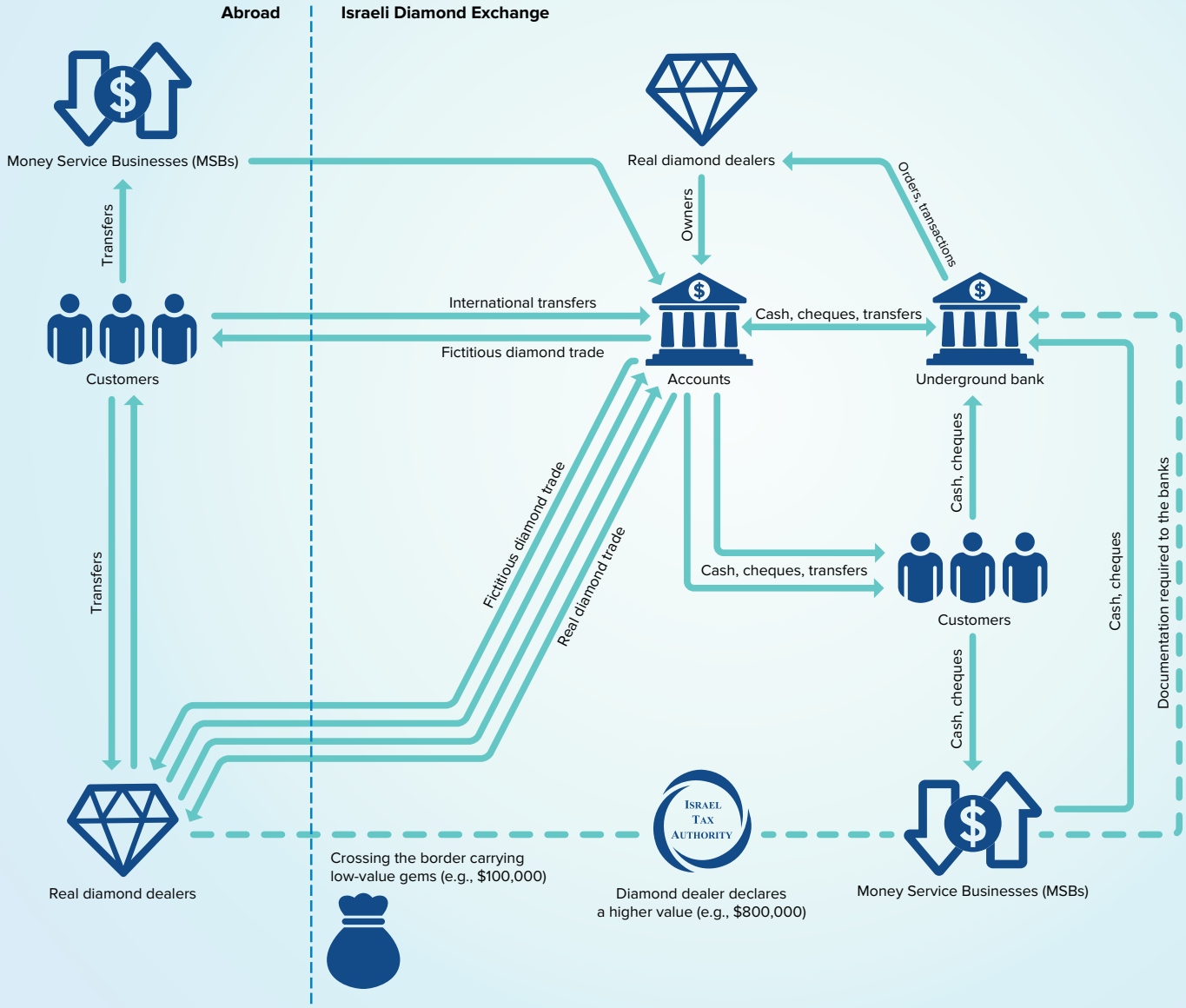
This case demonstrates numerous important takeaways for successfully combatting money laundering and terrorism financing:

- the role of an FIU in conducting strategic analysis of its database to identify ML/TF typologies and emerging phenomena, as well as conducting ongoing, independent, operative analysis of the database for tracing suspicious targets;
- the importance of building early detection models and using advanced monitoring and information technology tools including an Alert Center for ongoing analysis of suspicious actors or activity;
- the central role of the FIU in alerting LEAs to illicit activity and raising their awareness to identified phenomena;
- the significance of financial intelligence as a trigger for launching criminal investigations;
- the contribution of the Task Force as an efficient and effective investigative mechanism for LEAs to pool expertise, legal powers and data together, and ensure successful information sharing and collaboration between relevant authorities;
- the inclusion of prosecutors to accompany the Task Force and ensure adequate understanding of suspicions and evidence-collection procedures for success in subsequent judicial proceedings; and
- the importance of amending regulatory gaps identified within the context of an investigation.

Valuable Indicators of the Case

- Accounts being used to deposit cash in very large amounts, with the origin of the cash being unclear
- International diamond trade transactions amounting to millions of U.S. dollars per transaction, despite the origin and beneficiaries of these transactions not being known to be diamond dealers — UARs indicated that the fund transfers were not related to diamond deals, and supported the suspicion that funds from third parties were being laundered through the underground bank
- Invoices that did not include names of suppliers, or the names on the invoices that were not the same as the name of the entity sending the funds, suggesting fictitious deals

ANALYSIS OF ML NETWORK



CASE 21

Dissecting a Fake Export/Import Money Laundering Scheme (Korea, KoFIU)

Introduction

The Korea Financial Intelligence Unit (KoFIU) furnished the Korea Customs Service (KCS) with financial information on a fake export/import company. With this information, the KCS identified that the fake company was involved in false export/import declaration reports, property concealment and money laundering, causing serious economic losses to a number of Korean import agencies and commercial banks.

The Investigation

This is a case of trade-based money laundering through fraudulent export/import trades between Korea and Country A.

Keywords	trade-based money laundering, embezzlement
Countries involved	Republic of Korea, United Kingdom
Sectors involved	exports/imports

Suspects and Associated Companies

- Suspect S: This CEO of Company K and Company G was engaged in trading high-priced integrated circuit chips (ICs) between Korea and Country A, and established Company K and Company G with the intention of manipulating export/import costs of trading goods and concealing money offshore through carousel fraud.
- Suspect Company K: This Korean company was established by Suspect S. Company K was engaged in illicit trading activities by importing ICs from Country A through Korean import agencies and exporting the ICs to Company G.
- Suspect Company G: This U.K. company was also established by Suspect S and registered as an offshore company in Country A. Company G was engaged in the manipulation of export/import prices of ICs through carousel fraud and was also involved in the concealment of domestic funds.
- Company A, Company B, Company C and Company D: These were shell companies incorporated in Country A and ultimately operated by Suspect S. Companies A/B/C/D were engaged in fake export/imports of ICs for the purpose of manipulating their prices.

Suspect S established multiple shell companies offshore including Company G and Companies A/B/C/D in order to conduct fake export/import trading.

Suspect S operated Company K in Korea to lure a number of Korean import agencies into fake import trades of high-priced ICs and guaranteed them a 3–10% profit margin. The Korean agencies imported ICs from Country A and supplied them to Company K, and then Company K exported them to Company G in Country A without any processing.

The Korean import agencies made payments for the imported goods on Company G's bank account, which was opened by Suspect S. For export payments, the money was transferred back to Company K's bank account, which was also held by Suspect S.

Suspect S rented a warehouse in Country A and hired four to five locals (associates) to pretend that Company G was in active business operation. The associates produced business letters and documents, such as invoices, and stored the ICs imported by Company K in the warehouse. They would then resend the same consignments of the ICs back to Korea as if the ICs were newly produced to deceive the Korean import agencies.

As such, Suspect S planned and ordered to send the same consignments of ICs round and round again to deceive the Korean import agencies.

Using part of the money being transferred back and forth, Company K made payments for the imported ICs to the Korean import agencies and also gave profit margins to them as promised. In addition, as the trades between Company K and the Korean import agencies were conducted on a regular basis, Company K was gaining credibility in their eyes. Based on that credibility, the import agencies often postponed the due dates of import payments. Eventually, 14 of the import agencies failed to receive their credit sales from Company K; the unpaid money was approximately KRW 50 billion (USD 44 million).

Furthermore, Company K fraudulently exaggerated its trade sales and took out a KRW 3.5 billion(USD 3.1 million) loan from commercial banks, using export payments as collateral. However, Company K did not pay the loan back.

FIU Action

During the investigation KoFIU carried out two main activities:

- Analysis of domestic financial transaction data
    - 10 suspicious transaction reports, 34 currency transaction reports and 725 foreign currency transactions regarding Suspect S and Company K were provided to the KCS.
    - It was confirmed that transactions between Subject S and Company K were about KRW 3 billion(USD 2.7 million) and had consistently carried out between 2014 and 2016 with no clear purpose.
    - The transactions were made in large amounts through ATMs, not teller windows. Considering that Subject S conducted the transactions without dividing personal and business funds, Subject S was highly likely to exploit the funds of Company K.
- Analysis of foreign financial transaction data (in cooperation with the FIU in Country A)
    - After identifying the allegations of Company K through the search and seizure warrants, financial transaction information regarding Company G, Company A and Company B located in Country A were requested of the FIU in Country A.
    - It was confirmed that Suspect S opened Company G's bank account; the total number and amount of transactions between Suspect S and Korean companies from March 1, 2012, to April 1, 2016, were revealed.
    - It was discovered that Company A was engaged in trading electronic goods; the total number and amount of transactions between Company G, Company A and Company B from September 1, 2015, to December 31, 2016, were revealed.
    - It was discovered that Company B was a trading company of electronics and communications parts incorporated in the United Kingdom; the total number and amount of the transactions between Company B, Company G and Company B's business partners in Country A and export/import companies in Korea from June 1, 2015, to September 28, 2016, were revealed.
    - KoFIU made a second request to the FIU in Country A for all money transfers and transaction data regarding Company G, for verifying the details of each transaction made.

- KoFIU was able to identify outward/inward transfers of trade payments made in Company G's bank account and the details of the financial transactions conducted within Country A.
- Between 2015 and 2016, Company G's bank account showed a total of USD 74,392,190 in deposits and USD 107,104,405 in withdrawals.
- During the same period, the total amount of deposits/withdrawals conducted between Company G and Companies A/B/C/D was USD 23,340,930. This data was used to identify the route of the deposited money generated by fake export/import activities between Suspect S and his associates residing in Country A.

Evolution of the Case

This meticulously planned crime involved fake export/import trades and illicit domestic transactions performed through victimized companies, which were Korean export/import agencies, in order to move domestic properties offshore.

The KCS asked KoFIU to analyze the financial transaction data as well as to exchange information with foreign FIUs. Furthermore, ongoing cooperation between KoFIU and the FIU in Country A yielded valuable information, including Company G's business registration information, the holder of Company G's bank account, and details of deposits and withdrawals shared among the shell companies in Country A. The KCS conducted its investigation based on the intelligence provided by KoFIU.

A Korean District Public Prosecutor's Office is planned to prosecute Suspect S after obtaining relevant evidence through mutual legal assistance with a foreign prosecutor's office.

Suspect S was charged with:

- conducting **FRAUDULENT EXPORT/IMPORT TRADES** between Korea and Country A and reported fake item names, false trading volumes and costs, which violated the Korean Customs Laws. Specifically, Suspect S manipulated the prices of 3 million ICs, whose market values were estimated at approximately KRW 463.9 billion (USD 410.7 million).
- Suspect S made the Korean import agencies transfer approximately USD 172 million, equivalent to KRW 194.3 billion, to Company G's bank account as import payments, which violated the *Act of Specific Economic Crimes (Flight of Domestic Property)* by **ILLEGALLY MOVING DOMESTIC PROPERTY TO A FOREIGN COUNTRY**.

Outcome/Contribution of the Case

This case shows that collaboration of the FIUs is essential to secure and analyze domestic and international financial information in criminal investigations of money laundering involving both domestic and foreign companies. The intelligence exchange between KoFIU and the FIU in Country A played a vital role in preventing further economic losses from fake trading transactions by Suspect S and the suspect companies.

Through the financial transaction analysis and information exchange done by KoFIU and the FIU in Country A, the relationship between Suspect S, Company K, Company G and Companies A/B/C/D was clearly identified, which led to the arrest of Suspect S as a primary offender for this case.

This case caused considerable economic damage to multiple stakeholders including Korean export/import agencies and commercial banks. The damage to the Korean export/import agencies was estimated at about KRW 50 billion (USD 44 million); the banks were estimated to have lost KRW 3.9 billion (USD 3.45 million). Suspects were also engaged in the embezzlement of business funds, which amounted to KRW 5.6 billion (USD 5.0 million). This investigation also identified a new type of price manipulation crime.

Valuable Indicators of the Case

- KCS analysis, which revealed the declared value of the ICs being exported by Company K were remarkably higher than that of similar businesses, and the unit prices of exported goods (USD 38–52) were higher than those of imported goods (USD 3–9)
- Company K's long-term debt increased rapidly, as well as its sales volume, recording 100% or more growth on an annual basis

CASE 22

Dismantling International Illicit Finance Networks Through Mexico–U.S. Cooperation

(Mexico and the United States, FIU-Mexico and FinCEN)

Introduction

Mexico's Financial Intelligence Unit (FIU) and the U.S. FIU, FinCEN, as part of their work together to dismantle international illicit finance networks, took down an operation that included 42 entities in Mexico and many more abroad. These entities provided money laundering services to all types of criminals (e.g., drug traffickers, white collar), conducting a wide range of transactions involving 42 countries and more than 1,500 beneficiaries.

The Investigation

FIU-Mexico has developed a comprehensive risk-analysis computerized program, which rates the level of risk presented by all individuals and companies identified in every financial report it receives, such as suspicious activity reports (SARs) and currency transaction reports (CTRs).

Keywords	international money laundering scheme, illicit finance networks
Countries involved	Mexico and United States
Sectors involved	securities brokerages

In early 2013, the program detected a series of SARs that were related to each other and one, in particular, contained high-risk elements. This SAR was sent by a securities brokerage firm in Mexico and provided information on transactions made by a Mexican entity, Company A, whose reported economic activity was "retail of textile products." The SAR noted the following about the securities brokerage firm's client, Company A:

- a visit to the client´s office address determined that it was not in operation;
- the client had requested 440 international wire transfers totalling USD 13.1 million within the previous two months;
- the client had asked to send structured international wire transfers to many beneficiaries abroad, with a diverse range of economic activities, including, commercialization or investment of textiles, jewellery, real estate, hotels, airplanes and household products;
- the client had ordered cash transactions, deposits or withdrawals related to an individual, who in turn, had requested a series of international wire transfers for 199 beneficiaries located in Ireland, Israel, Panama and the United States; and
- the financial institution hadn't been able to contact the client's legal representative for questioning.

To further analyze the case, FIU-Mexico undertook a thorough search of Company A in its database and other sources of information and requested all financial institutions provide any information available with regard to this target. Note that FIU-Mexico has the authority to request all financial institutions (and, more recently, all designated non-financial businesses and professions) for all their information available in relation to individuals and entities, included in financial reports that FIU-Mexico has received. This is a characteristic of FIU-Mexico that few other FIUs in the world have, but it is particularly useful for pursuing more proactive and timely investigations. As a result of this new analysis of the database, FIU-Mexico identified three more relevant SARs that had been sent by three securities brokerage firms.

These additional reports allowed FIU-Mexico to determine a strong relationship between Company A and four other entities (Companies B, C, D and E). The links among Company A and Companies B–E included common shareholders or legal representatives, same addresses or phone numbers, interrelated transactions, or similar transaction profiles (i.e., many international transfers to different countries and beneficiaries with no logical connection). Some of the entities also had evident ties with other entities in Mexico and the United States that had been previously involved in drug trafficking and money laundering cases in both countries.

At this stage, FIU-Mexico was convinced that there were enough elements to build a successful case and that U.S. authorities should also be involved. Beyond sharing financial information with FinCEN, FIU-Mexico proposed a more active partnership by establishing a joint investigation and, if applicable, coordinated prosecutions. In the previous months, FIU-Mexico, FinCEN and other competent authorities had discussed the possibility of forming a task force to address cases of common concern, and this seemed like an opportunity to initiate such an endeavour.

FIU Action

FIU-Mexico is convinced that by having direct access to as many databases as possible, it can carry out more complete investigations that in turn will bring better results. In this sense, it has taken very seriously the expansion of its access to different sources of information, especially during the past year. FIU-Mexico has executed multiple memorandums of understanding with other Mexican agencies that have allowed it access to valuable sources of additional information.

The sources to which FIU-Mexico has currently access, and which were consulted consistently in its investigations for this case, were financial databases that contain all the reports received by FIU-Mexico from obligated entities, tax databases, a database that includes information on legal entities, import and export transactions database, civil registry certificate records, and records of all the arrivals and departures of individuals to/from Mexico.

As a result of the analysis of information related to Companies A–E, FIU-Mexico identified three other entities directly involved in the money laundering scheme, Companies F, G and H.

At this point in the investigation, FIU-Mexico made additional requests for information from specific banks and securities brokerage firms, with regard to all the identified companies. Also, the exchange of information between FIU-Mexico and FinCEN through the Egmont Secure Web (ESW) began. Both FIUs made sure that all the information they shared, either financial or non-financial, was always done through the ESW, recognizing the benefits that such a platform offers.

The information provided by FinCEN confirmed the identity of the leader of the illicit finance network. The investigations continued with the quantification of the most relevant international wire transfers and the identification of important elements for initiating prosecutions.

Evolution of the Case

FIU-Mexico, with the office of the Mexican Attorney General (PGR) and in coordination with FinCEN and the U.S. Department of Justice, determined that FIU-Mexico would proceed with requests for prosecution. FIU-Mexico therefore made its first request for prosecution on September 4, 2013.

On October 1, 2013, the Federal Prosecutor asked the court for authorization to wiretap eight phones of relevant targets.

Meanwhile, the investigation continued to identify more individuals and entities involved in the money laundering scheme. FIU-Mexico sent a special request to the financial institutions in which Companies A–H used to operate.

FIU-Mexico and PGR determined to proceed with a second request for prosecution on October 29, 2013, involving an additional 34 target companies.

On October 30, 2013, the Federal Prosecutor requested a search warrant for the two addresses identified as the operating offices for all the companies.

During the search of warrant actions to two addresses, 38 individuals were taken into custody. Two of them, the leader of the money laundering scheme and one of his collaborators, were held in custody and later arrested.

On October 30, 2013, the same day the search of warrant actions were executed, the court also authorized the Federal Prosecutor's request for the seizure of USD 13.4 million deposited in 39 accounts at seven banks, plus the two properties where the search warrants were executed.

Outcome/Contribution of the Case

This case provides an example of the level of sophistication and international outreach that some money laundering schemes can develop, pointing to the importance of having FIUs and other competent authorities coordinate with their international peers at all or most stages of a case, in order to dismantle the illicit finance networks.

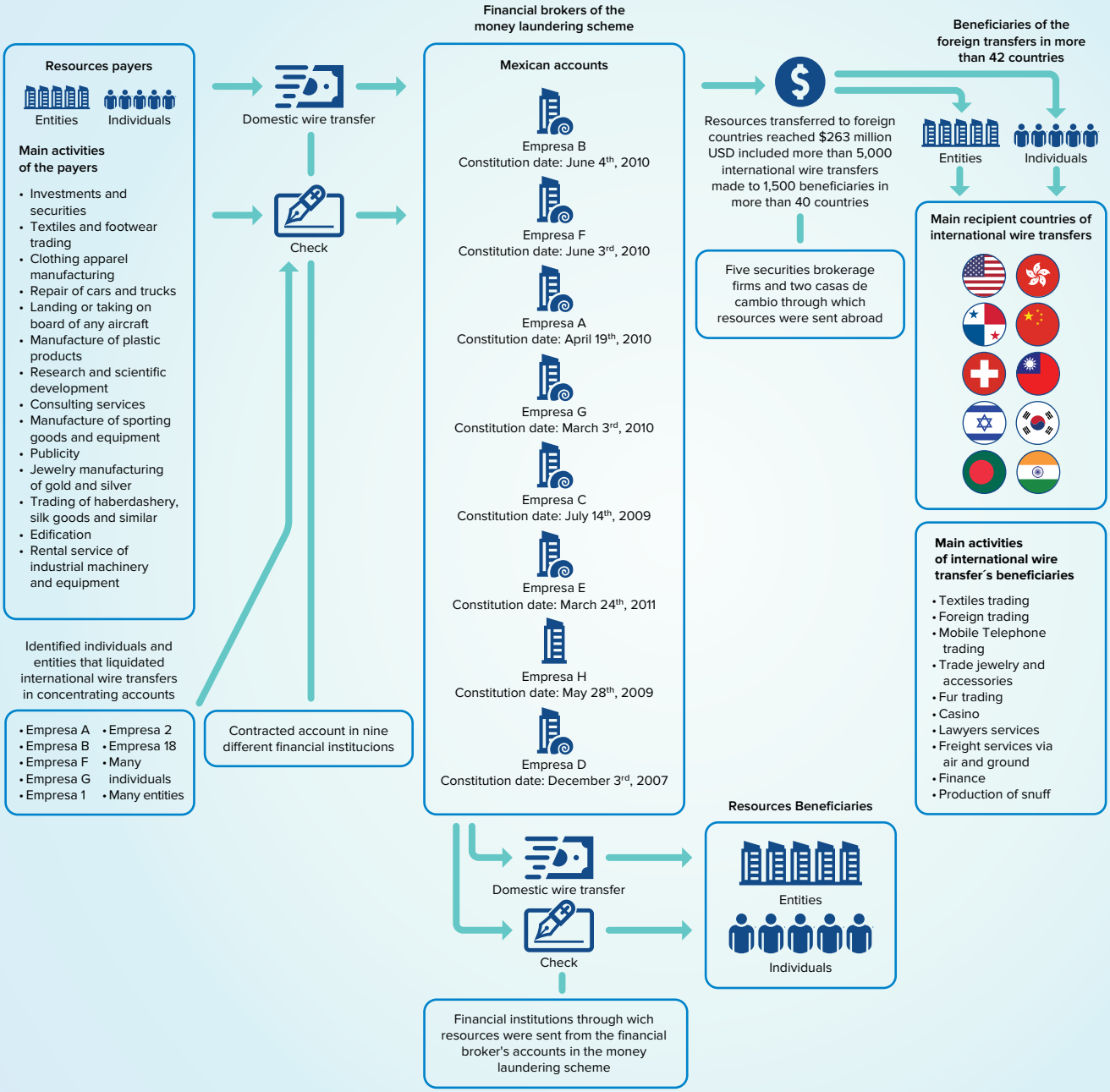
Both FIUs have broadly institutionalized their internal procedures and joint collaboration. FIU-Mexico was able to identify the initial relevant SARs for this case out of thousands of other SARs, not by coincidence, but because of its well-established protocols, a team of professional analysts and suitable technology.

FIU-Mexico and FinCEN have decided to document this case as soon as possible and with as many details as can be shared at the time, taking into account that this is still an open case in both Mexico and the United States. The goal is to share their knowledge on a specific major money laundering scheme that can be easily replicated in other countries, together with their experience in combatting this type of case and any other with an international perspective.

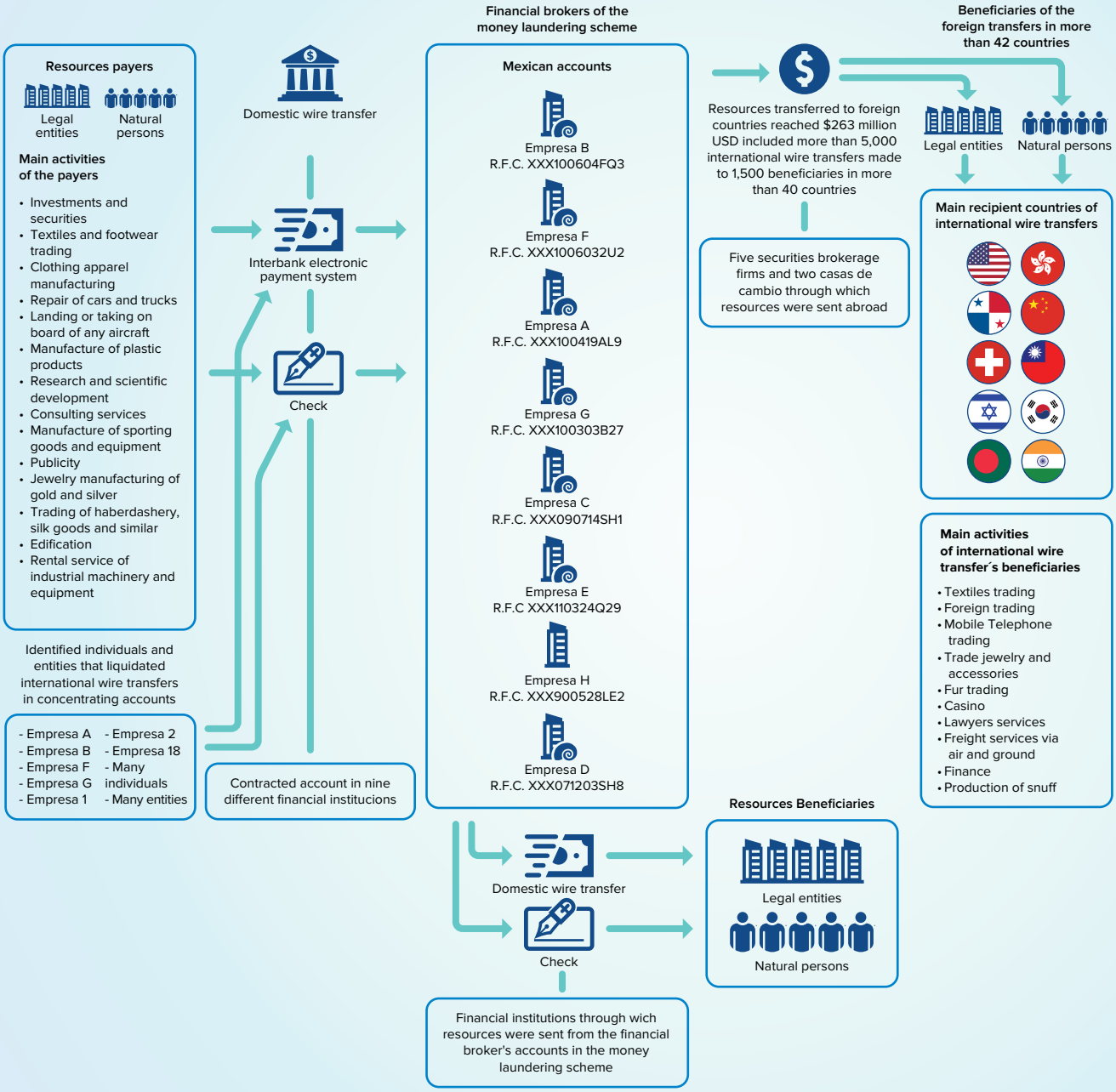
Valuable Indicators of the Case

- Company transactions related to activities outside its reported economic activity
- Several large transactions that immediately get transferred to another beneficiary
- Same contact information for several companies

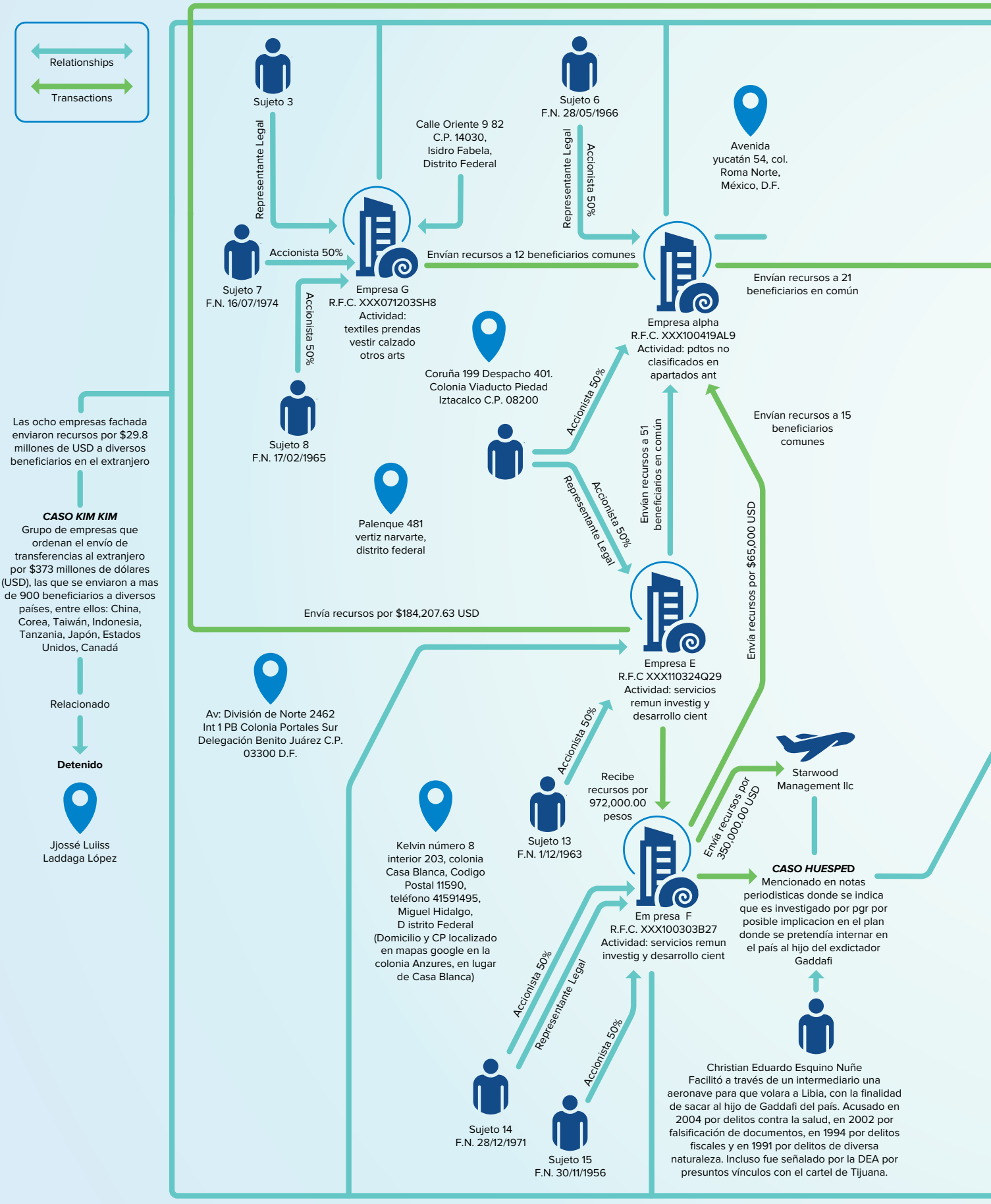
ANALYSIS OF ML NETWORK

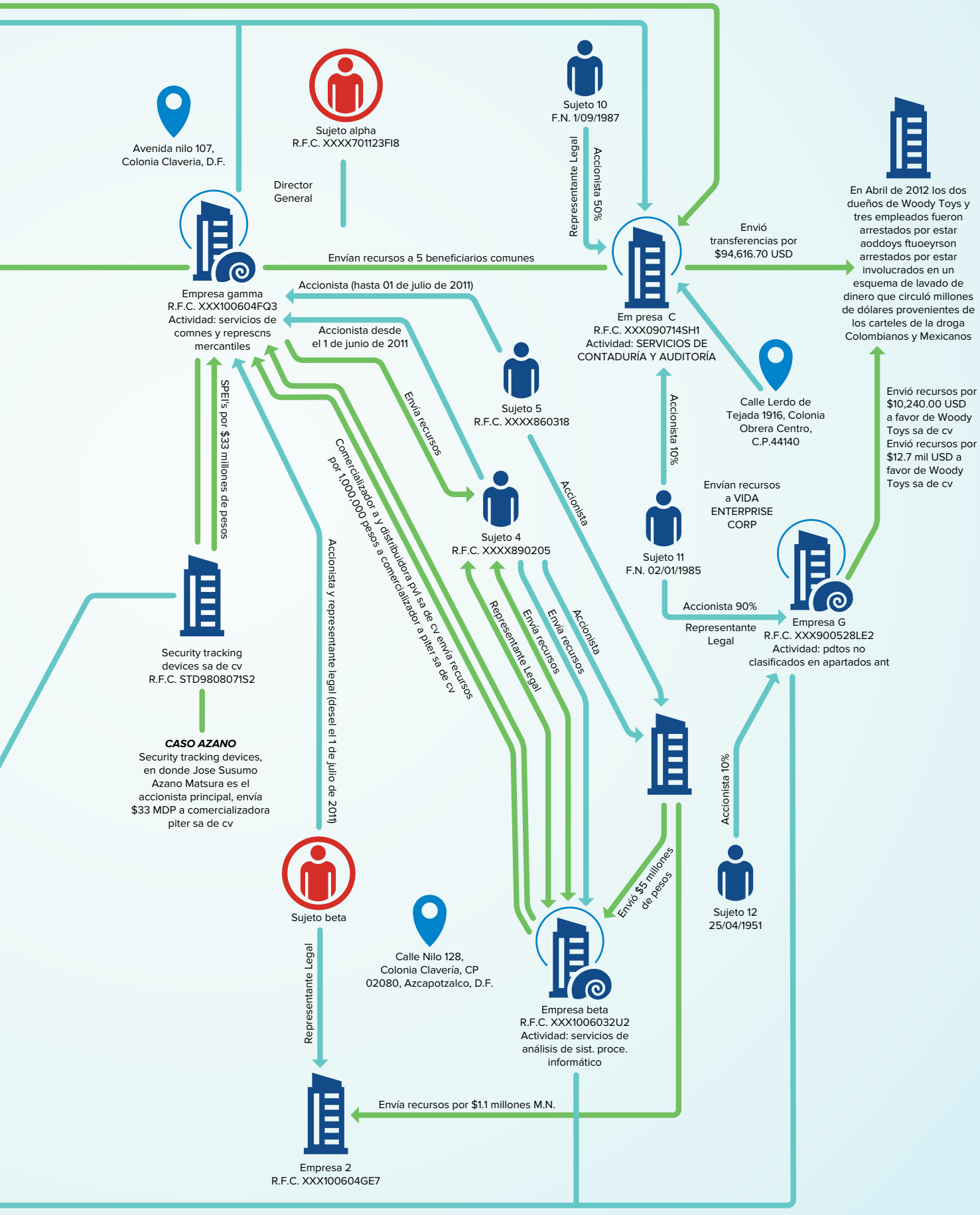


ANALYSIS OF ML NETWORK

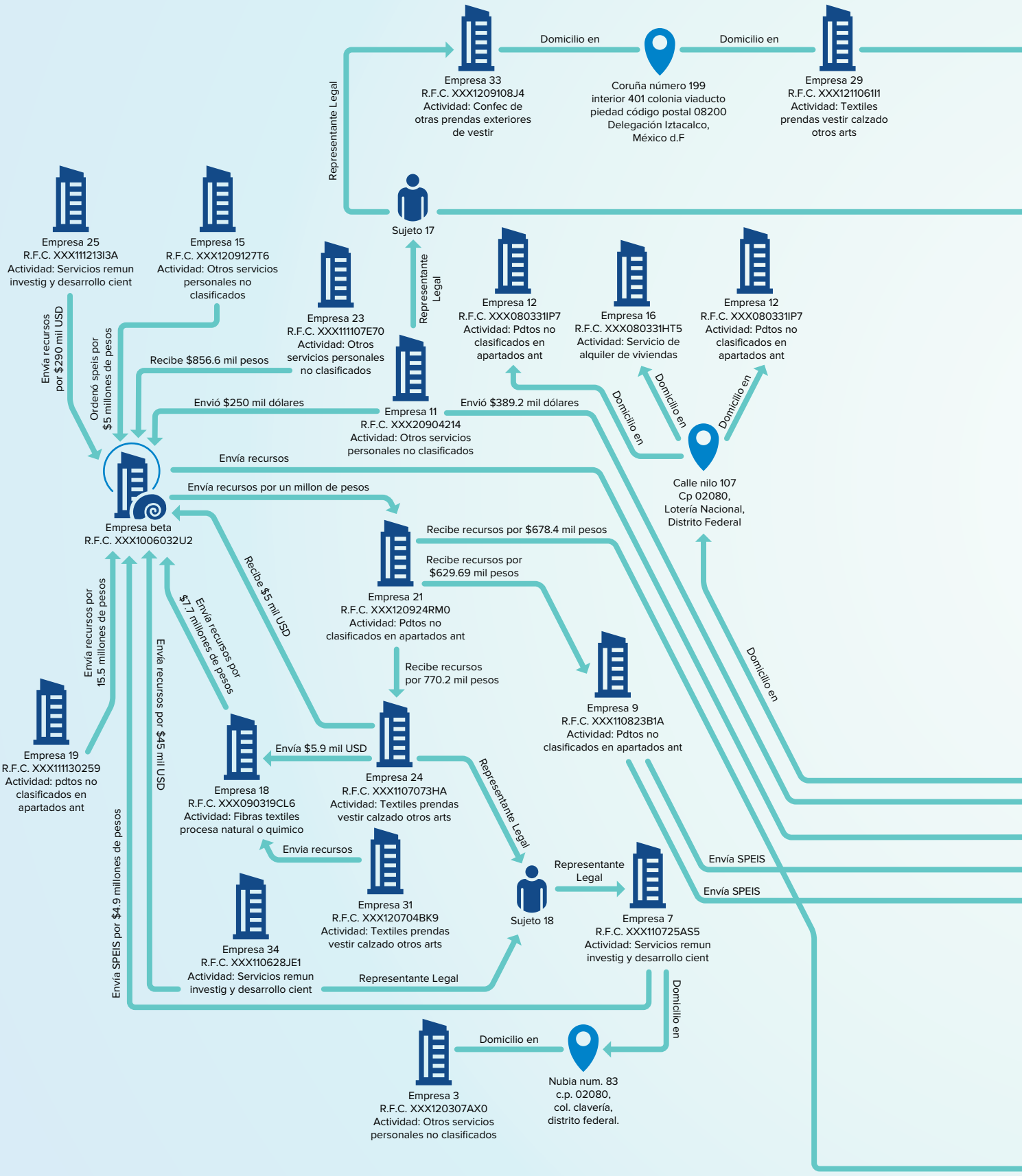


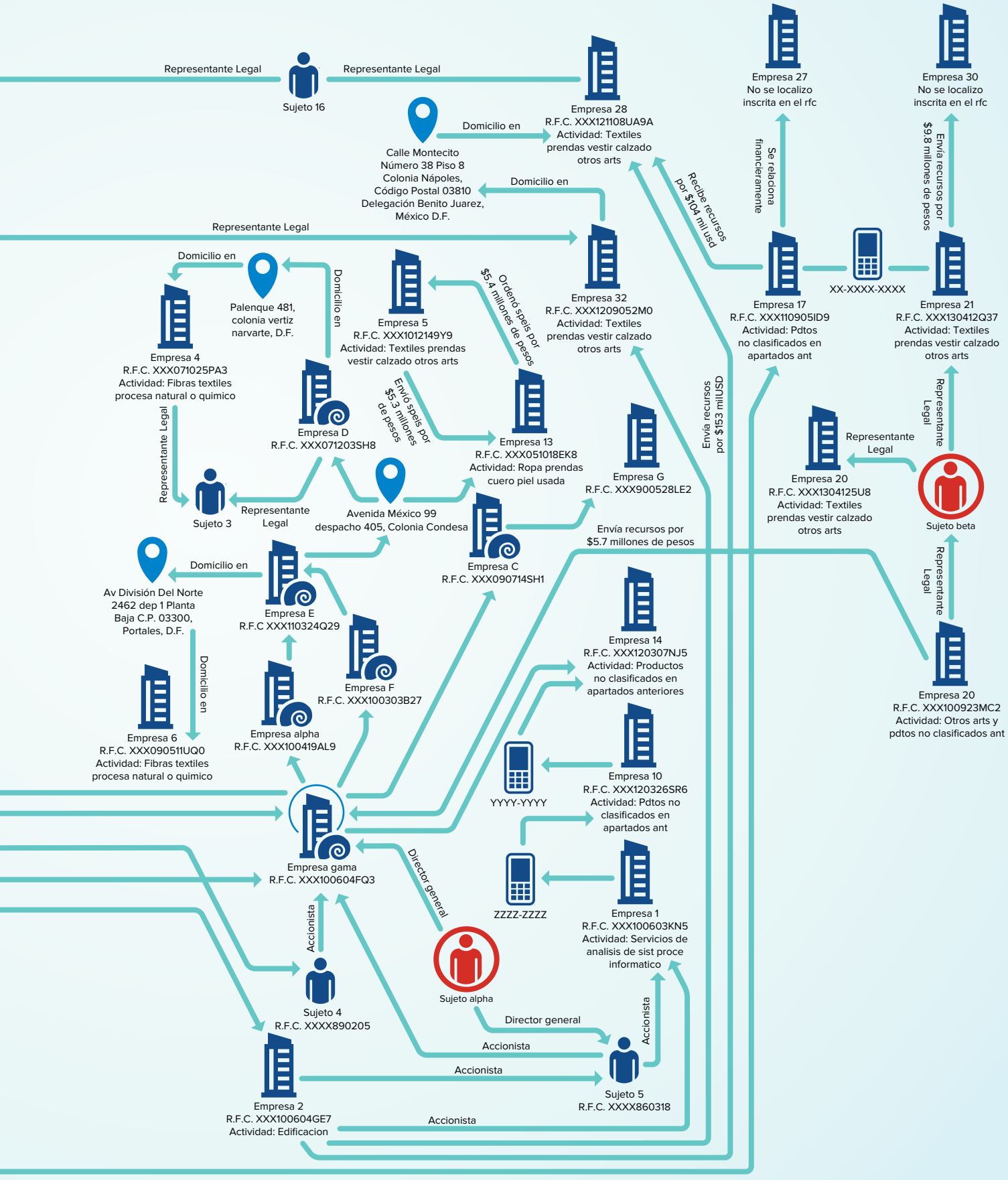
ANALYSIS OF ML NETWORK




Avenida nilo 107, Colonia Claveria, D.F.
Sujeto alpha R.F.C. XXXX701123FI8
Director General
Sujeto 10 F.N. 1/09/1987
Representante Legal
Accionista 50%
En Abril de 2012 los dos dueños de Woody Toys y tres empleados fueron arrestados por estar aoddoys ftuoeyrson arrestados por estar involucrados en un esquema de lavado de dinero que circuló millones de dólares provenientes de los carteles de la droga Colombianos y Mexicanos
Envió transferencias por $94,616.70 USD
Envían recursos a 5 beneficiarios comunes
Empresa gamma R.F.C. XXX100604FQ3 Actividad: servicios de comnes y represcns mercantiles
Accionista (hasta 01 de julio de 2011)
Accionista desde el 1 de junio de 2011
Em presa C R.F.C. XXX090714SH1 Actividad: SERVICIOS DE CONTADURÍA Y AUDITORÍA
Sujeto 5 R.F.C. XXXX860318
Calle Lerdo de Tejada 1916, Colonia Obrera Centro, C.P.44140
Envió recursos por $10,240.00 USD a favor de Woody Toys sa de cv
Envió recursos por $12.7 mil USD a favor de Woody Toys sa de cv
Envía recursos
Comercializador a y distribuidora pvl sa de cv envía recursos por 1,000,000 pesos a comercializador a piter sa de cv
Accionista
Accionista 10%
Envían recursos a VIDA ENTERPRISE CORP
Sujeto 4 R.F.C. XXXX890205
Sujeto 11 F.N. 02/01/1985
SPEI's por $33 millones de pesos
Accionista y representante legal (desel el 1 de julio de 2011)
Accionista 90%
Representante Legal
Empresa G R.F.C. XXX900528LE2 Actividad: pdtos no clasificados en apartados ant
Security tracking devices sa de cv R.F.C. STD9808071S2
CASO AZANO
Security tracking devices, en donde Jose Susumo Azano Matsura es el accionista principal, envía $33 MDP a comercializadora piter sa de cv
Representante Legal
Envía recursos
Envió $5 millones de pesos
Accionista 10%
Sujeto beta
Calle Nilo 128, Colonia Clavería, CP 02080, Azcapotzalco, D.F.
Sujeto 12 25/04/1951
Empresa beta R.F.C. XXX1006032U2 Actividad: servicios de análisis de sist. proce. informático
Representante Legal
Envía recursos por $1.1 millones M.N.
Empresa 2 R.F.C. XXX100604GE7

ANALYSIS OF ML NETWORK




Representante Legal
Sujeto 16
Representante Legal
Empresa 28
R.F.C. XXX121108UA9A
Actividad: Textiles prendas vestir calzado otros arts
Domicilio en
Calle Montecito
Número 38 Piso 8
Colonia Nápoles,
Código Postal 03810
Delegación Benito Juarez,
México D.F.
Domicilio en
Empresa 27
No se localizo inscrita en el rfc
Empresa 30
No se localizo inscrita en el rfc
Se relaciona financieramente
Envía recursos por $9.8 millones de pesos
Recibe recursos por $104 mil usd
Representante Legal
Domicilio en
Palenque 481,
colonia vertiz
narvarte, D.F.
Domicilio en
Empresa 4
R.F.C. XXX071025PA3
Actividad: Fibras textiles procesa natural o quimico
Empresa 5
R.F.C. XXX1012149Y9
Actividad: Textiles prendas vestir calzado otros arts
Ordenó speis por $5.4 millones de pesos
Empresa 32
R.F.C. XXX1209052M0
Actividad: Textiles prendas vestir calzado otros arts
Empresa 17
R.F.C. XXX110905ID9
Actividad: Pdtos no clasificados en apartados ant
XX-XXXX-XXXX
Empresa 21
R.F.C. XXX130412Q37
Actividad: Textiles prendas vestir calzado otros arts
Representante Legal
Empresa D
R.F.C. XXX071203SH8
Envió speis por $5.3 millones de pesos
Empresa 13
R.F.C. XXX051018EK8
Actividad: Ropa prendas cuero piel usada
Empresa G
R.F.C. XXX900528LE2
Envía recursos por $153 milUSD
Representante Legal
Empresa 20
R.F.C. XXX1304125U8
Actividad: Textiles prendas vestir calzado otros arts
Representante Legal
Sujeto beta
Representante Legal
Sujeto 3
Representante Legal
Avenida México 99
despacho 405, Colonia Condesa
Empresa C
R.F.C. XXX090714SH1
Envía recursos por $5.7 millones de pesos
Domicilio en
Av División Del Norte
2462 dep 1 Planta
Baja C.P. 03300,
Portales, D.F.
Empresa E
R.F.C XXX110324Q29
Empresa F
R.F.C. XXX100303B27
Empresa 14
R.F.C. XXX120307NJ5
Actividad: Productos no clasificados en apartados anteriores
Representante Legal
Empresa 20
R.F.C. XXX100923MC2
Actividad: Otros arts y pdtos no clasificados ant
Domicilio en
Empresa 6
R.F.C. XXX090511UQ0
Actividad: Fibras textiles procesa natural o quimico
Empresa alpha
R.F.C. XXX100419AL9
YYYY-YYYY
Empresa 10
R.F.C. XXX120326SR6
Actividad: Pdtos no clasificados en apartados ant
Empresa gama
R.F.C. XXX100604FQ3
Director general
ZZZZ-ZZZZ
Empresa 1
R.F.C. XXX100603KN5
Actividad: Servicios de analisis de sist proce informatico
Accionista
Sujeto alpha
Director general
Accionista
Sujeto 4
R.F.C. XXXX890205
Accionista
Accionista
Sujeto 5
R.F.C. XXXX860318
Empresa 2
R.F.C. XXX100604GE7
Actividad: Edificacion
Accionista

TERRORISM, ORGANIZED CRIME AND HUMAN TRAFFICKING

Terrorist Financing

Terrorism is generally understood as acts of violence directed against civilians in the pursuit of political or ideological goals.[19] Terrorist organizations may be involved in or own legitimate businesses, which provides them a legitimate source of funding. However, terrorism can also be funded through illegal activities, and therefore may appear similar to other criminal organizations. Terrorism financing plays a crucial role in the preparation and implementation of terrorist attacks, which is why it is critical to identify trends, methods and indicators related to terrorism financing.[20] One case shows how a non-profit organization was used to finance terrorism.

19 Office of the United Nations High Commissioner for *Human Rights, Human Rights, Terrorism and Counter-terrorism*, Fact sheet no. 32, 2008, www.ohchr.org/documents/publications/factsheet32en.pdf

20 Information Exchange Working Group (IEWG), Counter Terrorist Financing Project: Lone Actors and Small Cells, 2019, https://egmontgroup.org/en/content/new-publication-counter-terrorist-financing-project-lone-actors-and-small-cells-public

Indicators

- Purchase of large amounts of foreign currency
- An account opened in the name of a legal entity, a foundation or an association, which may be linked to a terrorist organization and shows movement of funds above the expected level of income
- Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements
- The use of nonprofit organizations to generate and/or transfer funds

Organized Crime

The main goal of organized crime is financial gain. Moreover, organized crime affects all states, whether as countries of supply, transit or demand. As such, modern organized crime constitutes a global challenge that must be met with a concerted, global response.[21] In the organized crime case described in this section, tracing the illicit funds from trafficking in protected species led to the identification of an international criminal organization.

Globalization and improved technology has contributed enormously to the growth and internationalization of organized crime. Law enforcement authorities are also observing a nexus between organized crime and terrorist financing: each of these activities tries to seize the opportunities presented by the other.

While it is difficult to assign a value to the income generated by organized crime alone, its magnitude is suggested by the estimate that about USD 2 trillion is laundered for all types of crimes each year.[22]

Indicators

- Use of foreign banks
- Use of foreign currency
- Use of nominees, fronts or other devices to hide the ownership of assets, businesses or bank accounts
- Known criminal associations
- Deposits followed by immediate transfers to countries of concern
- Deposits of large amounts of cash
- Payment of air tickets by a third party
- Large cash withdrawals
- Interconnection with seemingly independent businesses
- Use of "ghost" employees by businesses
- Presence of silent partners
- Ownership of hidden assets

Human Trafficking

One way organized crime groups make their money is to take away a person's freedom. Human trafficking violates one of the most fundamental rights, attacking human dignity at its core. The human trafficking cases presented were both initiated by a single complaint — one from a victim's mother and one from a victim herself.

The income generated by these activities has grown so much that it now competes with traditional sources of funding used by organized criminal groups, such as drug trafficking. This is the reason why specialists in anti-money laundering and counter terrorism financing study ways to leverage the anti-money laundering system to detect, deter, disrupt and investigate human trafficking.[23]

21 United Nations Office on Drugs and Crime, *Organized Crime*, https://www.unodc.org/unodc/en/organized-crime/intro.html

22 United Nations Office on Drugs and Crime, *Overview*, https://www.unodc.org/unodc/en/money-laundering/overview.html

23 IEWG, The Role of FIUs in Combatting Illicit Finance Associated with Human Trafficking, 2020.

Indicators

- Establishment of companies with the alleged purpose of offering tourism or employment services in a foreign country:
- International money transfers using money service providers traditionally used for remittance purposes (such as Western Union, Contakt, MoneyGram) from countries with a high risk of receiving illegal traffic of persons
- The number of remittance senders is considerably larger than the number of recipients
- Remittances sent are split among different related accounts
- Funds received through remittances or transfers are withdrawn in cash from ATMs in short periods of time or through consecutive transactions
- Money transfers are inconsistent with the economic activities of the senders themselves
- Individuals receive transfers of funds or remittances from senders with whom there is no apparent connection
- Companies registered as providers of telecommunications or Internet services receive funds supported by invoices with undisclosed or poorly described "services"
- Legitimate offshore companies are acquired and then used to open bank accounts for said companies in countries different from those where the companies are registered
- Use of online credit card systems, such as CC Bill, to transfer money to open accounts for offshore companies or credit card accounts

Developing methods and strategies to detect, disrupt and prevent terrorism, organized crime and human trafficking, as well as exchanging information and international cooperation, is key to fighting money laundering as a whole and saving victims from cruel destinies.

The role of FIUs in this area is extremely valuable, with many successful in handling cases of human trafficking. The cases presented here offer some eye-opening examples.

CASE 23

Successful Dismantling of a Human Trafficking and Money Laundering Organization (Argentina, UIF-AR)

Introduction

A nationwide investigation involving several agencies was kickstarted by the mother of a woman who was abducted by a human trafficking network. After members of the criminal organization involved were acquitted in 2012, the mother approached the Financial Intelligence Unit (FIU) for Argentina, UIF-AR, with information about key elements of this organization's money laundering scheme. This scheme involved three main vehicles that were operated by the criminals and through which the funds were laundered: a company running games of chance, a chauffeur-driven car agency and a football club management company. Some of the money laundering typologies and transactions conducted by these individuals involved fake invoices, cash deposits into accounts with no economic background, fake prizes allegedly obtained through games of chance, and the purchase of luxury goods. Those details triggered a new criminal investigation, and support an ongoing investigation into human trafficking.

The Investigation

On October 3, 2002, a 23-year-old woman was abducted by a human trafficking network that operated in the northern region of Argentina. This woman is still missing.

Keywords	trafficking, sexual exploitation, organized crime
Countries involved	Argentina
Sectors involved	gaming industry, private urban transport (fixed-rate cab service), football club management, hospitality industry

The criminal investigation ended in 2012 with the acquittal of all the defendants of the case. The missing woman's mother reacted by disclosing key elements of this organization's money laundering scheme to UIFAR. Her disclosure kickstarted a nationwide investigation involving cooperation among several agencies.

In March 2013, UIF-AR received a formal request from the Attorney General's Office for assistance with the ongoing human trafficking investigation. As part of this assistance, UIF-AR analysts provided support to other law enforcement agencies to conduct several searches, where key documents, firearms and significant amounts of cash were seized. After the searches were finished, several agents from UIF-AR and the Border Patrol combed through this evidence in an intensive task that lasted about three weeks.

Analyzing this new information, together with existing suspicious activity reports (SARs) and information provided by other agencies, UIF-AR was able to establish that this criminal organization had a three-pronged strategy to launder the proceeds of crime: a company running games of chance, a company providing a fixed-rate cab service and a football club management company.

With these findings, six individuals were remanded in custody in December 2013, while several others were sentenced to prison.

UIF-AR analysts took part in several hearings and provided witness testimony. In December 2017, many key players of this criminal organization were convicted in Federal Court. Rubén Eduardo Ale was convicted of **MONEY LAUNDERING**, **USURY**, **EXTORTION**, **PROFITING FROM SEXUAL EXPLOITATION**, **DRUG TRAFFICKING AND LEADING A CONSPIRACY**. For these charges, he was sentenced to 10 years' imprisonment and fined ARS 8 million. Adolfo Ángel Ale was convicted of the same crimes, receiving the same sentence and fine. Five other defendants were convicted as accessories, receiving sentences that ranged between 6 and 7 years of imprisonment. Finally, six defendants were convicted of **CONSPIRACY TO COMMIT CRIME** and **DRUG TRAFFICKING**, receiving sentences of 3 to 4 years of imprisonment.

This sentence is under appeal in the National Court of Cassation in Criminal Matters. Initially, the key defendants were granted house arrest while awaiting the results of the appeal. But this house arrest was revoked and the defendants were moved back to a federal prison as they await the ruling on the appeal.

FIU Action

The initial disclosure submitted to UIF-AR by the mother of the missing woman in 2012 led to several SARs that were processed by FIU analysts. Combining this information with what was obtained through searches and through collaboration with other government agencies, UIF-AR produced intelligence reports that established a money laundering hypothesis.

The reports showed that the members of this criminal organization used several firms to conceal the proceeds of crime.

First, a company that ran games of chance and betting, and through which payment papers related to non-existing prizes were issued to the shareholders of the firm (i.e., the criminals themselves). This same firm entered a voluntary tax amnesty program established in 2008 for a total of ARS 3 million. In fact, by entering this tax amnesty program this firm was making a formal statement to the Argentinian tax authorities expressing that it possessed ARS 3 million for which it had not paid taxes before. This sum, however, could not be justified by the firm's economic activity.

Second, another company provided a fixed-rate cab service. It acquired many assets and received many cash deposits in its bank accounts. These deposits were made without documentation on the origin of the funds.

Third, a company named GD managed a local football club and was run by members of the organization. This firm raised several flags, including inconsistencies regarding business concessions and the sale and purchase of football players. One of GD's partners also managed a hotel in which there was over-invoicing for accommodation services that were provided to the general public. The firm GD was also used as a shell company to purchase real estate, jewellery and luxury vehicles.

Evolution of the Case

This case began with the raw material disclosed by the mother of one of this organization's victims. UIF-AR turned this data into intelligence and provided judicial authorities with findings that propelled the investigation and made it possible for the criminals to be charged with money laundering.

Several assets were identified during the investigation, including luxury cars, real estate and jewellery. All these assets, along with firearms and large sums of cash, were seized, enabling millions of Argentine pesos of illicit proceeds to be applied to a good cause. Furthermore, the sentences delivered specified that the fines should be paid with the assets of the key players of the organization until the full amount is paid off.

Outcome/Contribution of the Case

The present case constitutes a significant contribution to the fight against organized crime, money laundering, and one of the most heinous and abhorrent crimes — human trafficking. Not only did this investigation lead to the conviction of several criminals and to the seizure of assets worth millions of Argentine pesos, but it also halted development of a trafficking ring in northern Argentina. It is also worth noting that the seizure of the assets creates a deterrent for future money launderers.

Valuable indicators in the case

- SARs regarding large cash transactions
- Purchase of a large number of real estate properties and luxury motor vehicles by individuals with little or no economic background
- Large sums of cash deposited into bank accounts for recently created firms. The shareholders of the firms also submitted their first tax returns at the same time such firms were created
- Inconsistencies regarding tax filings
- Application for a tax amnesty benefit — one of the key criminals in this case applied for a benefit in a tax amnesty regime that allowed Argentine taxpayers to declare assets for which they had not paid taxes, while Argentinian authorities guaranteed them that they would not be prosecuted for tax evasion, but the fact that this individual applied for this benefit and especially the sum of funds declared raised doubts about the economic source of such wealth, triggering an in-depth analysis carried out by the FIU

CASE 24

Following the Trail of Animal Trafficking to Take Down an International Criminal Organization (Côte d'Ivoire, CENTIF CI)

Introduction

Animal trafficking often goes hand in hand with other forms of criminality. An operation to take down organized wildlife crime involving Côte d'Ivoire's Financial Intelligence Unit (FIU) — the National Financial Information Processing Unit of Côte d'Ivoire (CENTIF CI) — became a full-scale investigation of money laundering and international organized crime. The case, whose many facets involved several investigation units and some foreign FIUs, identified different actors of a national criminal chain, and led to arrests, asset seizures and criminal convictions.

The Investigation

This case was triggered by a non-governmental organization for protecting wildlife, EAGLE Côte d'Ivoire (a branch of the EAGLE international network), which raised the alarm about trafficking in protected species in Côte d'Ivoire.

Keywords	animal trafficking, international trade, money laundering
Countries involved	Burkina Faso, Cote d'Ivoire, Mali, Vietnam, China
Sectors involved	agricultural and forestry sectors, import/export

The government responded by launching operation "STOP à Ivoire," which included various activities from January 18, 19, 20 to 21 and on March 21, 2018, with the assistance of EAGLE Ivory Coast.

An investigation initiated by the Transnational Crime Unit (UCT), an Ivorian investigation office, led to the arrest of the head of the criminal network, Tran Van Tu, a Vietnamese national. This arrest was the beginning of a lengthy series of arrests and seizures.

At the request of UCT, CENTIF CI got involved and set up a plan that assigned roles to every actor in the analysis process to coordinate efforts efficiently.

The case took more than a year because of the different origins of the main actors involved in the case: Vietnamese, French-Chinese, Birkinabé and Ivorian.

When closing the file on May 31, 2019, CENTIF CI recorded seizures of 469.15 kg of worked ivory, pangolin scales, 22 elephant tusks amounting to 87.55 kg, 307 kg of teeth and claws of panthers. Accounts that held about USD 116,900 in Côte d'Ivoire and about USD 728,506 abroad were frozen because they were identified as proceeds of crime.

During the arrest, the suspects were found to be in possession of illegal firearms, as well as files and other elements related to an international procuring network. This aspect of the case is still under way.

The key predicate offences are **CORRUPTION** and **FRAUD**, in addition to offences against the environment.

Eight suspects — perpetrators and accomplices — received maximum sentences: 12 months' imprisonment and a fine of XOF 200,000.

FIU Action

At the opening of the file, the UCT sent an information request to CENTIF CI, putting the FIU at the centre of the investigation, especially in terms of intelligence and analysis.

CENTIF CI sent requests for information through the EGMONT Secure Web to the FIUs of the countries of the suspects who were foreign nationals. As for the accused Ivorian, requisitions against persons subject to anti-money laundering were sent to certain administrations.

Through an innovative application called FILTRAC, CENTIF CI was able to process the investigation file quickly.

Domestically, CENTIF CI collaborated fruitfully with the police, gendarmerie, customs and UTC, as well as and, notably, with the EAGLE organization. Internationally, CENTIF CI worked in cooperation with several countries, such as China, Cameroon, Mozambique, Kenya, Uganda, Cambodia, Taiwan and, especially, Vietnam.

Evolution of the Case

After EAGLE Côte d'Ivoire first raised the alarm of about trafficking in protected species in Côte d'Ivoire, CENTIF CI spent more than a year to solve the case.

The investigations and analysis provided a lot of information on international criminal mapping related to this form of crime. But quantitatively, CENTIF CI saw that the statistics available did not contain any significant criminal facts recorded in money laundering from wildlife crime. CENTIF CI concluded that either this type of criminal activity existed but was not reported because of a lack of awareness of this form of crime or simply because that phenomenon was unknown in Côte d'Ivoire.

Outcome/Contribution of the Case

From this case, CENTIF CI noted the following:

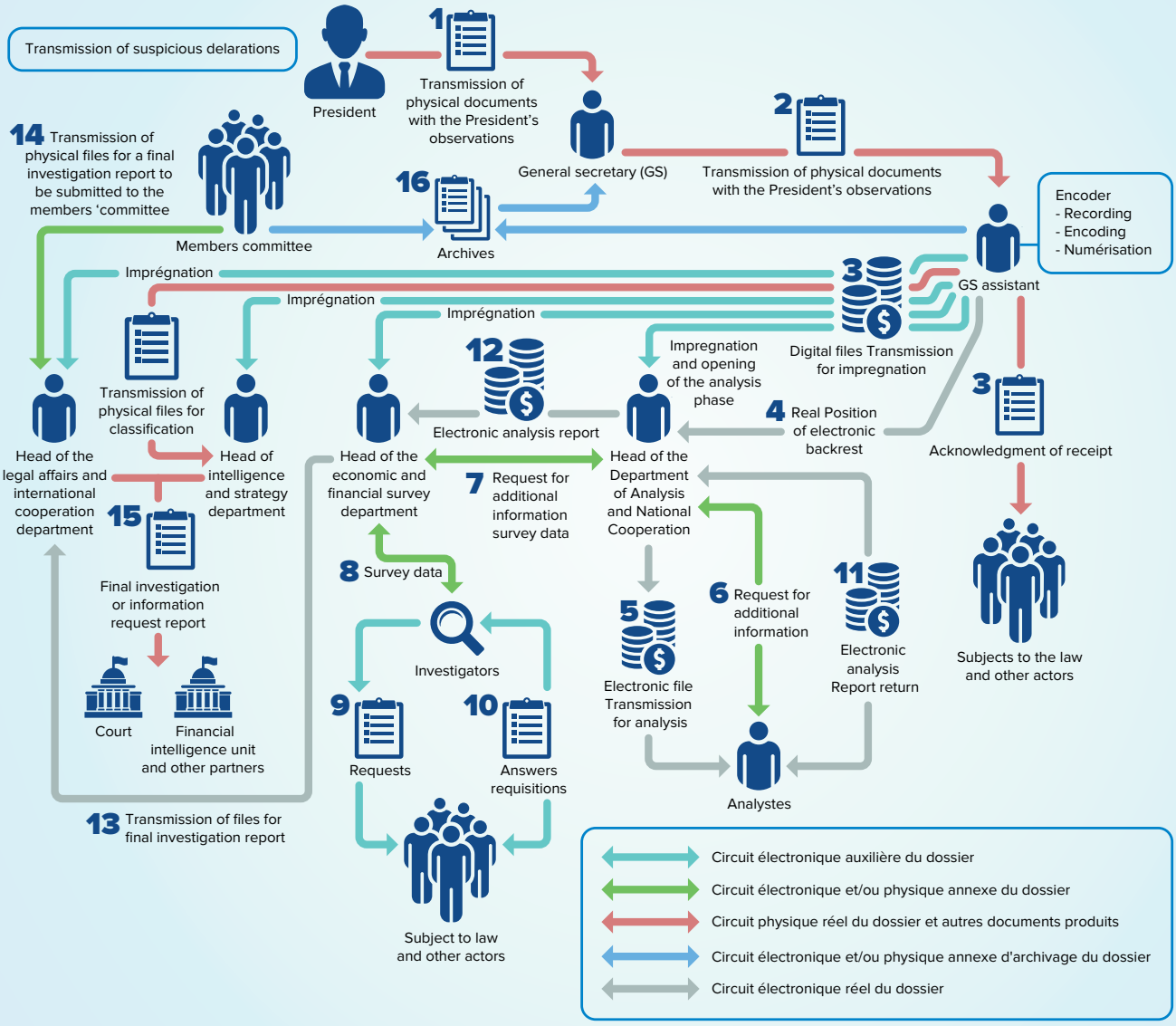
- the existence of frank collaboration among all the anti-money laundering actors
- the importance of CENTIF CI coordination of information on a national and international level, as well as private and public;
- the positive role played by the NGO EAGLE;
- failures of the preventive and repressive anti-money laundering systems;
- the links of illegal wildlife trade to poaching, smuggling, illegal hunting and the use of unconventional means of transport;
- the problem of access to information and frank collaboration with some national/local administrations;
- CENTIF CI's lack of budget to buy some materials useful for investigations;
- the existence of wildlife crime in the subregion, which had not been recognized there before and, therefore, its impact may be greater than uncovered so far; and
- the problem of frank cooperation with the criminal chain services.

The CENTIF CI is still looking for criminal assets to be seized, both domestically and abroad.

Valuable Indicators of the Case

- Smuggling of animal parts
- The massive exchange of cash between the various actors involved
- The absence of convincing links between the various people and companies implicated

J-24 CASE PROCESSING CIRCUIT ML/TF — CENTIF CI << FILTRAC >>



CASE 25

The Use of Money Remittance Systems and Non-Profit Organizations to Finance Terrorism (Indonesia, PPATK)

Introduction

The Indonesian Financial Transaction Reports and Analysis Centre (PPATK), which is Indonesia's Financial Intelligence Unit (FIU), formed a special team to provide a nimble response to terrorism and terrorism financing cases. Working with law enforcement authorities, this team identified a non-profit organization (NPO) that had a number of transactions that were not consistent with its mandate. Further investigation revealed the NPO also had links to some parties identified as members of a terrorist network, and that the NPO's transactions included funds being sent to or received from high-risk countries. The arrests resulting from PPATK's proactive analysis may have saved hundreds of lives from terrorist attacks.

The Investigation

In 2015, Indonesia conducted a National Risk Assessment on Terrorist Financing that found that the misuse of funds from NPOs has become a high-risk terrorism financing method.

Keywords	HF, Hendro Fernando, MIT, money remittance systems, terrorism financing
Countries involved	Philippines, Syria
Sectors involved	Non-profit, financial service providers (banking, money remittance)

In the same year, Jakarta was the site of the Thamrin bombing attack. Responding to this incident, PPATK formed a special team to handle terrorism and terrorism financing cases. The function of this team is to provide a quick response to any terrorism case and to support any terrorism and terrorist financing investigation. Thus, this team proactively exchanges information with the respective investigator of a terrorism case. Another function of this team is to create a map of terrorist financing networks in Indonesia based on information exchange and PPATK databases.

Based on the Jakarta attack and the findings of the risk assessment, PPATK began an operational analysis, especially on any subject listed on the terrorist financing network map and NPOs.

ABC Foundation was chosen as an example because it made transactions that were inconsistent with its purpose; this NPO also had links to some parties identified as members of the terrorist network. An anomaly was found in ABC Foundation's transaction remarks such as "love suriah," "syuhada," "mujahid," and "the syuhada's widow, wife or children." In addition, ABC foundation was being promoted on two provocative radical websites.

PPATK became aware of suspect HF due to several outgoing transactions from the foundation linked to his accounts. HF held accounts at several banks. These accounts received cash deposits related to money transferred from high-risk parties tied to terrorism financing, transfers to the owner of a mobile phone counter, purchases at a herbal shop and an electronic shop, for wives, and cash withdrawals via ATMs located in areas that are known to be connected to terrorism.

The parties that received funds from HF were identified as foreign terrorist fighters, and the funds were suspected to be used to buy communication devices to support HF's group in coordinating the January 2015 Thamrin bombing attacks. The international funds transfer instruction (IFTI) reports database revealed that HF received and transferred funds from and to high-risk countries.

HF was also matched with the PPATK mapping of the terrorist financing network. In addition, PPATK obtained open-source information that HF committed vandalism in Bekasi District Court during the demonstration of the release of the ISIL commander for Indonesia in 2014. However, no information concerning HF was requested from PPATK.

The analysis of the case was initiated when PPATK optimized its database to look for links with NPOs. Once ABC Foundation was identified, an analyst used a variety of analytical tools, including an on-site examination. The financial analysis also involved open sources of information, combined with cooperation and coordination with the relevant domestic and foreign authorities. After establishing a task force for mapping the terrorist financing network associated with this case, PPATK proactively gave the intelligence to the Indonesian National Police.

On a prosecution level, PPATK identified the beneficial owner of those funds as BN, who was on the designated individuals list and declared himself as an ISIL Southeast Asian leader. The purpose of the transactions was to send an individual, IF (deceased), to join ISIL in a Middle East country. Apart from the money HF sent to BN, HF also sent money to a Southeast Asian country through a money remittance service located at the post office in Bekasi.

Prisons weak link in terror fight

Jakarta's police chief has admitted the country's prison management is a weak link in its security apparatus, after revealing an Islamic State-affiliated militant was arrested following the January 14 attack with nine guns stolen from Tangerang Prison on the city's fringes. Tito Karnavian said Hendro Fernando, an intermediary funnelling terror funding from Syria to extremist groups in Indonesia and with links to the Jakarta attack, confessed to plotting an attack on the Jakarta airport, an international school or Bali after he was arrested with nine guns a day after the Jakarta attack.

The Australian.com.au

FIU Action

To trace suspicious flows of funds and other information related to indicators of terrorist financing related to the HF case, PPATK used the following sources to gather information:

- **The Integrated Customer Information System (SIPESAT)** is electronically administered and integrated into customers' specific information provided to the financial service provider. The system tracks the flow of funds of criminals who attempt to hide or disguise money or the proceeds of crime into various financial services. SIPESAT can conduct this analysis more efficiently and effectively, in shorter time, and at a lower cost.
- **IFTI reports** contain instructions of transfers to and from abroad reported to PPATK by banks and other financial service providers that conduct international money transfer services. Indonesian anti-money laundering law gives the mandate to implement this regulation started in 2014 and there is no threshold in this report. Based on the IFTIs database, the analyst identified that HF sent/received funds to/from high-risk jurisdictions for terrorism.
- **Open-source information** from the Internet found a similarity between the name of HF in the citizenship database and the open source information, which considered him as a radical martyr.
- **The citizenship database** contains identity numbers, date and place of birth, addresses, and spouses' and children's names. In the HF case, the citizenship database was used to confirm that the subject being analyzed is the same person with the name found in the media related to terrorist acts.
- **On-site examination** analyzes or examines reports and information as intended.

PPATK also analyzed relevant suspicious transaction reports (STRs) that were submitted by the reporting parties as a result of the exploration of databases related to HF and the networks, and worked with feedback from investigators.

From database checks, PPATK found HF and other individuals involved in cash deposits to the NPO. They also received money purportedly for social activities that was actually used for terrorism financing and cash withdrawal in areas that are widely known to be red zones for terror attacks. Related to these findings, PPATK partnered with domestic stakeholders.

PPATK also involved other countries in the case to make them aware of the threat posed by HF and the network. The incoming and outgoing funds looked to be related to terrorist activity involving some individuals in other jurisdictions. HF's international transactions involved three countries, which PPATK alerted regarding HF's affiliation and as a trigger for those countries to monitor the transaction. PPATK also exchanged information about this case with related FIUs in the Financial Intelligence Consultative Group forum. This forum was created to facilitate coordination including the exchange of information among FIUs in Southeast Asian countries, Australia and New Zealand related to money laundering and terrorism financing issues.

Evolution of the Case

Based on the intelligence reports PPATK submitted, the Indonesian National Police carried out an investigation related to terrorism and terrorist financing, with HF as the suspect.

The Indonesian National Police then submitted the case files to the Attorney General's Office of the Republic of Indonesia for prosecution. HF was charged with **TERRORISM** and **TERROR FINANCING** and found guilty by the District Court of East Jakarta in December 2016. HF was sentenced to prison for six years for **ILLEGAL WEAPONS POSSESSION**.

The court seized evidence related to HF's illegal weapons charge: a black bag of the Virago essential package containing seven firearms of V. Bernardelli Gardone, a 32-calibre Smith & Wesson revolver, one gun of P-3A Kal. 7,65 mm, one magazine containing 7 bullets GFL Cal. 7.65 mm, five magazines containing 18 bullets GFL Cal. 7.65 mm, black gloves, a video recorder, sunglasses and a flash drive.

Outcome/Contribution of the Case

This investigation led to the arrest of a terrorist who had planned several terror attacks in Indonesia. The cooperation between PPATK and the Indonesian National Police to initiate the investigation of HF was essential. The analysis of STRs prevented HF and related parties from carrying out terrorist attacks. This case demonstrates PPATK's ability to identify and link suspects. Based on this information, the suspects were arrested and sentenced to prison, possibly saving hundreds of lives.

Valuable Indicators of the Case

- PPATK mapping of the terrorist financing network
- NPO transaction inconsistent with its purpose
- NPO ties to terrorist networks and websites
- Multiple transactions in areas known to be connected to terrorism or with high-risk countries

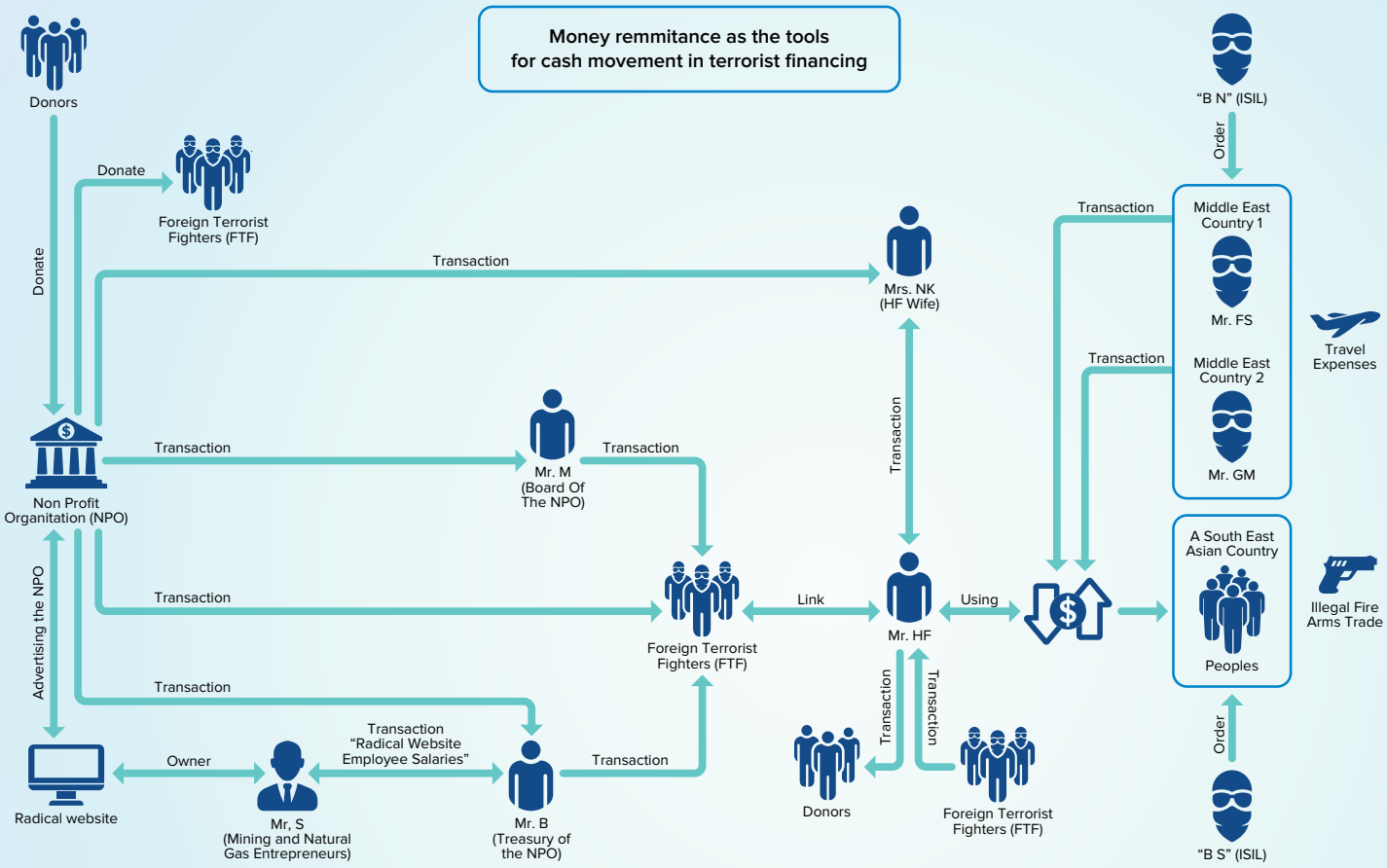
Terror in Indonesia

ISIS 'funded attack in Jakarta'

Police uncover money trail; funds also sent to finance two other cells plotting similar attacks

Police officers on guard inside a terminal of the Soekarno-Hatta international airport in Jakarta, which was one of the other planned terror targets, apart from police posts and stations, an international school, as well as Bali and other places frequented by Westerners and Shi'ites. PHOTO: EUROPEAN PRESSPHOTO AGENCY

ANALYSIS OF ML NETWORK



CASE 26

Following the Money in a Human Trafficking Case (Senegal, CENTIF)

Introduction

Effective coordination at the national level of the National Financial Intelligence Processing Unit (CENTIF), Senegal's Financial Intelligence Unit (FIU), with other stakeholders in anti-money laundering and combatting terrorism helped to stop transnational organized crime. This human trafficking case extends beyond the borders of West Africa. When CENTIF was brought on board to investigate the possible proceeds of these crimes, it was able to also uncover a money laundering scheme.

The Investigation

A victim identified Person A, owner of Nightclub 1, to police. According to the accuser, Person A recruits girls from the Maghreb and Eastern Europe via the Internet, promising them decent work and good wages in Senegal. Once in Senegal, these girls have their passports confiscated and are forced into prostitution with the clientele of Person A's nightclub.

Keywords	human trafficking, prostitution, corruption, money laundering
Countries involved	Senegal and three other countries
Sectors involved	banking, law enforcement, notaries, judicial

After a careful investigation, the police arrested Person A. The results of the police investigations were thus communicated to the judicial authority.

The national media coverage about the dismantling of a procuring ring by police alerted a bank. As part of its duty of vigilance vis-à-vis its customers, the bank noted useful information in its portfolio that indicated that one of the legal persons held an account that had been opened by Person B and for which Person A had been appointed proxy.

Because of the case before the courts, bank officials theorized that the funds being credited to this account could have come from procuring, and so deemed it necessary to file with CENTIF two suspicious transaction reports (STRs) on its client and the company managers.

CENTIF began its investigation when it received the STRs.

FIU Action

To collect information, CENTIF:

- sent requests to national stakeholders;
- sent requests to international partners via Egmont Secure Web; and
- used an environmental investigation to identify people and their relationships.

Evolution of the Case

The information CENTIF received back revealed the following:

- Person A opened, in the name of Nightclub 1, another account whose operating mode is similar to that of the first.
- Person A is the majority shareholder of another business, Company H. The other shareholder of Company H is Person B, who was also the subject of another STR.
- A transfer from the Nightclub 1 account to a third business, Company C, showed that the money from the prostitution is partly recycled in other investments, such as real estate, as evidenced by a cheque of XOF 39 million issued to the order of a notary.

From the environmental investigation, CENTIF was able to establish the following links:

- Two nightclubs are located in the same area.
- Nightclub 2 is adjacent to Nightclub 1, where the prostitutes work, and Person A is the owner of the premises and Person B, his son, is the manager.

A close collaboration between the FIUs and other national stakeholders through the exchange of information resulted in assets and bank accounts being frozen. Internationally, the information exchange with foreign FIUs revealed that the suspects were not well known to the intelligence services in charge of investigating terrorism and its financing.

Outcome/Contribution of the Case

At the end of the police investigations, Person A was arrested and procecuted.

A judicial investigation was also opened before an investigating judge of the Dakar Special Court. Person A was then held in custody.

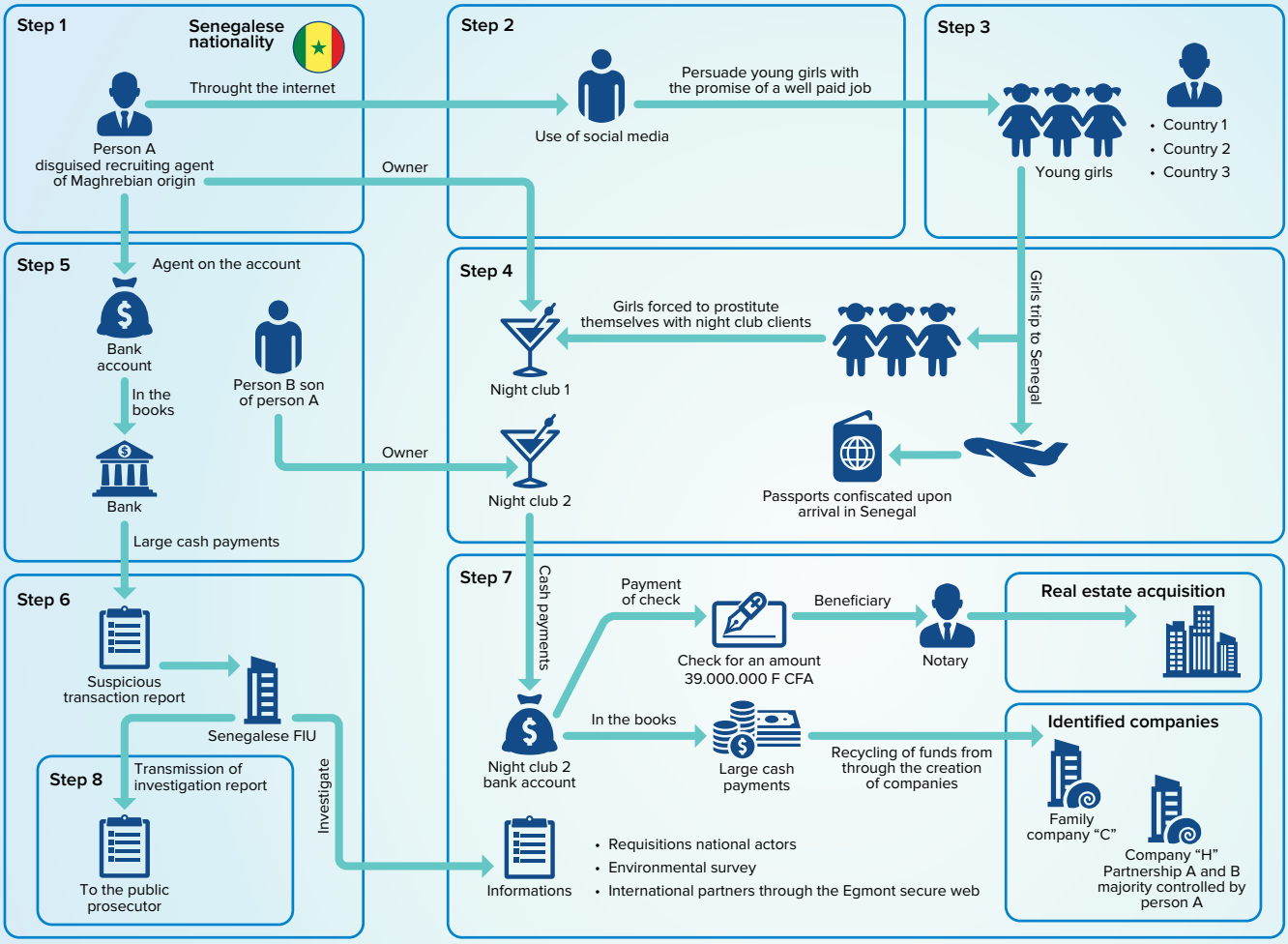
CENTIF forwarded the case to the Public Prosecutor in the appropriate jurisdiction, with a report on facts likely to constitute an offence of **MONEY LAUNDERING** in real estate from illicit funds generated by **PROCURING** and **HUMAN TRAFFICKING**.

The bank funds have been frozen and the proceedings are ongoing.

Valuable Indicators of the Case

- Massive cash deposit followed by massive cash withdrawal, for a legal person
- A significant difference between the volume of payments made into the account and the amount of financial income generated by the standard activities of a nightclub the size of that managed by Person A
- Systematic deposit of all funds in an account opened only for this purpose
- Creation of a construction company to recycle funds from the nightclub, an unrelated business

J-26 HUMAN TRAFFICKING AND MONEY LAUNDERING SCHEME — SENEGAL



What Makes a Good Case

The Best Egmont Case Awards (BECA) competition is one of the highlights of the Egmont Group annual activities. It provides an opportunity for members to share examples of exceptional work. The large number of cases submitted are judged against a set of established criteria that consider facets of what makes a case interesting and educative.

The cases were judged according to their complexity and results achieved. Although the cases considered took place over the last six years, the lengthiness of judicial procedures meant that some were yet to be concluded as of time of publication and others had actually commenced before 2016 and were completed only recently. Those that were still under court proceedings were sanitized so as to not jeopardize cases. The complexity of cases was judged according to intelligence gathering procedures, challenges, the use of open source criteria, and the gathering of intelligence from within jurisdictions and from foreign jurisdictions through the Egmont Secure Web. Most importantly, the selected cases demonstrated superior levels of skills on the part of Financial Intelligence Unit (FIU) analysts as they used their knowledge to gather information from private and public sources and pieced together complex financial, legal and corporate obfuscation using their analytical prowess.

In each case, the FIU played a crucial role in uncovering the criminal scheme and bringing the perpetrators to justice and in confiscating illicit assets through judicial procedures. As criminals have continued to show ingenuity in developing new schemes to elude financial regulators and law enforcement, FIU analysts time and time again have proven their importance in analyzing complex data and putting together the pieces of puzzles that quite often would confound criminal investigators. FIU analysts used their unique position in being able to cooperate with financial institutions, domestic law enforcement agencies and foreign FIUs to uncover novel schemes that otherwise might have gone unnoticed.

Success in these cases is measured in effective sanctioning of criminals and the retrieval of their hidden stolen assets. As such, the FIU has worked hand in hand with law enforcement to uncover which financial and non-financial instruments were used. This often took the form of coordinating activities by police, prosecutors, judges, taxation and customs officials, and others so as to create a complete picture of complex money laundering (ML) schemes. The FIU was often placed in the position of advising and supporting prosecutors and police to help them build strong cases that would stand up before judicial review.

Financial crime continues to be perpetrated internationally in many, if not most, instances. As such, it is the FIU that plays the most important role in gathering information and intelligence from other Egmont members and using this source to help with mutual legal assistance requests and eventually the freezing of criminal assets hidden abroad. Although seldom in the limelight, these cases clearly illustrate how FIUs play a central role in garnering effective coordination domestically and internationally that lead to the arrest, conviction and sentencing of criminals, and the return of stolen assets.

Of exceptional note in many of these cases is the ability of FIUs to successfully work with the private sector through public-private partnerships. Notably, banks and other financial and non-financial institutions demonstrated willingness to assist in cases through gathering information on their suspected clients with the FIU's guidance and proactivity in sharing valuable information that may indicate possible criminal activity. These forms of public-private partnerships demonstrate how the public and private sectors can work together to clean up the financial system, remove bad apples and ensure a level playing field for all.

Criteria for BECA Case

An Effective Case Example

- Cases should have been concluded within the last five years.
- Effective case examples should be submitted providing the most value to Egmont member FIUs as an informative case example.
- Cases should highlight new or sophisticated ML schemes, innovative techniques and methods, the number of agencies and jurisdictions involved, and the amount of funds.

A Focus on FIU Work and Analysis

- Cases should elaborate on the work of the FIU and its paramount role in the case development; for instance, the FIU initiated the case and/or developed intelligence and was able to draw on international connections that may not otherwise have been easily accessible.
- Cases should demonstrate value added by FIU analysis.

An Identification of Domestic and International Cooperation

- Cases should provide examples where effective international and/or domestic collaboration contributed to a more successful outcome.
- Cases could indicate where they have included other jurisdictions and how they have demonstrated effective international cooperation.

A Clear Demonstration of the Evolution of the Case

- Cases should illustrate how feedback enhanced the development of the case and contributed to a positive outcome.
- Cases describe challenges faced in identifying the ML scheme; and/or identify new ML techniques or trends.
- Cases demonstrate a successful outcome.

Other Results

- A case can show how it influenced changes to domestic legislation; policies and procedures of FIU and/or domestic and/or international partners.
- A case can support conclusions of a national risk assessment.

Special Recognition

Despite the challenges we have had to face, as a result of the COVID-19 pandemic, the BECA Project Team successfully advanced with the publication of this Book through virtual meetings.

Top left to right: *Meriton Shoshi (FIU-Kosovo), Alvaro Mauricio Torres Ramirez (FIU-Colombia), Aldo Farfán (FIU-Ecuador), Leopoldo Quirós (FIU-Ecuador);* ***Middle left to right:*** *Paola Gabriela Torres Velez (FIU- Peru), Elza Robert (FIU-Seychelles), Mikko Värri (FIU-Finland), Andrey Krankov (FIU-Russia), Soraya Jesus Cardoso (FIU-Angola);* ***Bottom left to right:*** *Karina Uribe (FIU-Chile), Tafsir Hane (FIU-Senegal), Maria Paz Ramírez (FIU-Chile), Nathalie Kläy (FIU-Switzerland);* ***Bottom right:*** *Michelle Ouyang (EGS)*

Egmont Group
of Financial
Intelligence Units

THE EGMONT GROUP SECRETARIAT

Tel: 1 647-349-4116

E-mail: mail@egmontsecretariat.org

Website: www.egmontgroup.org