EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

Egmont Group
of Financial
Intelligence Units

BEST EGMONT CASES

Financial Analysis Cases 2021–2023

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

CONTENTS

REMARKS BY THE CHAIR OF THE EGMONT GROUP

The BECA (Best Egmont Group Cases Award) is a cherished initiative here at the Egmont Group. It provides FIUs (Financial Intelligence Units) a powerful platform to enrich the global AML/CFT (anti-money laundering and combating the financing of terrorism) community by sharing insights, expertise and experiences in combating money laundering and terrorist financing. Despite the challenges posed by the aftermath of the global pandemic, the BECA competition persevered during the past several years, culminating in the submission of an impressive 78 cases spanning from 2021 to 2023.

The meticulous efforts of the Project Team led to the selection of 24 exemplary Egmont cases across six distinct categories of predicate offenses and associated ML (Money Laundering) typologies. The exceptional quality of these submissions promises to make choosing a winner a formidable one for delegates, ensuring the BECA competition remains a highlight of the upcoming Egmont Group Plenaries.

The publication of this 2021–2023 BECA Case Award book is a significant milestone. It offers readers a comprehensive view of the evolution of money laundering and terrorist financing typologies and predicate offenses through the lens of 24 diverse cases from jurisdictions worldwide. This compilation is an important resource for our community, presenting real-world scenarios where cooperation among FIUs was pivotal in achieving results. It encapsulates the essence of the Egmont Group of FIUs.

I extend heartfelt gratitude to all FIUs who contributed to the BECA over the past three years, and congratulations to the Technical Assistance and Training Working Group for the successful publication of the 2021–2023 Best Egmont Case Award book.

Elzbieta Frankow-Jaskiewicz
Chair Egmont Group of Financial Intelligence Units
Deputy Director of the Polish FIU

INTRODUCTION

The Best Egmont Case Award (BECA) annual competition was established in 2011 by the Training Working Group, now known as the Technical Assistance and Training Working Group (TATWG). The primary goal of the BECA initiative is to inspire Egmont members to contribute to the Egmont Group's database on money laundering and terrorist financing cases. Doing so benefits the Financial Intelligence Units (FIUs) and stakeholders in anti-money laundering/combatting the financing of terrorism (AML/CFT). The BECA offer FIUs a valuable opportunity to share their knowledge, expertise and experiences within the global AML/CFT community.

The competition begins with issuing a call letter by the BECA Champion, inviting all Egmont member FIUs to submit their finest cases. To foster active engagement and enhance the BECA database, there are no restrictions on the number of cases that an FIU member can present. Moreover, FIUs can either submit cases independently or collaborate on joint submissions, thereby encouraging collective efforts that exemplify close collaboration among Egmont Group members.

At the end of the submission period, a panel of four to six judges assesses all entries against a predefined set of criteria to identify the top two cases. Finalist FIUs are invited to present their cases during the plenary session, where the Heads of FIU cast their votes for the case deemed most outstanding. The winner is bestowed with the prestigious BECA trophy. The BECA has evolved into a cherished tradition and a focal point of the Egmont Group Plenary, symbolizing our community's commitment to excellence and collaboration.

With the support of the Egmont Group Secretariat, the first BECA Book was published in 2015, containing 22 best case submissions between 2011 and 2013, and has since become a valuable reference for case studies and best practices of FIUs globally.

In 2020, this vital tradition continued. That year marked the 10th Anniversary of the BECAs. Despite the global pandemic's impact on the organization's ability to conduct a face-to-face Egmont Plenary meeting, the 2020 BECA competition proceeded successfully. There were 24 case submissions from 19 FIUs, and for the first time and last time, the winner was selected through virtual voting.

Simultaneously—with the support of the Egmont Group Secretariat—the development of the second BECA publication was prioritized. It contained the best case submissions between 2014 and 2020. In June 2020, a subgroup of 12 FIUs was formed to review all case submissions. This challenging task involved balancing regional representation and the diversity of predicate offenses associated with money laundering typologies. From 117 case submissions, the subgroup selected 26 best cases and established seven targeted categories of predicate offenses and related money laundering typologies.

In October 2023, a team of nine FIUs came together to assess all case submissions for the third BECA book. This task was complex. It required considering all regional representation and the various predicate offenses linked to money laundering typologies. Out of 78 submissions, the team chose 24 top cases and identified six specific categories of predicate offenses and related money laundering typologies:

1. Bribery, Corruption & Tax Evasion
2. Cybercrime, Virtual Assets & Child Pornography
3. Drug Smuggling & Gambling
4. Fraud & Embezzlement
5. Trade-Based & Third-Party Money Laundering
6. Terrorism, Human Trafficking & Organized Crime

Case Submissions 2021–2023

YEAR	#CASES / #FIUs	FINALISTS	WINNER
2021	24 cases from 17 FIUs	• UIF Italy and FIU Hungary • IMPA (FIU-Israel)	**IMPA (FIU-Israel)**
2022	32 cases from 20 FIUs	• UIF (FIU-Italy) • FID (FIU-Latvia)	**FID (FIU-Latvia)**
2023	22 cases from 12 FIUs	• PPATK (FIU-Indonesia) • TRACFIN (FIU-France)	**PPATK (FIU-Indonesia)**

ACKNOWLEDGEMENTS

I'd like to express my gratitude to Meriton Shoshi, the Vice Chair of TATWG, for his leadership of the BECA project from 2023 to 2024. Additionally, I appreciate the judges for dedicating their time and meticulous efforts in reviewing cases for the BECA competitions.

2021 BECA Panel of Judges

- Elzbieta Frankow-Jaskiewicz (GIFI-FIU Poland)
- Sinclair White (FIA-FIU Bermuda)
- Najmina Latif (BDCB-FIU Brunei Darussalam)
- Iole Chiaverelli (UIF-FIU Italy)
- Dominic Offor (NFIU-FIU Nigeria)

2022 BECA Panel of Judges

- Sin Chor-ka Christopher (JFIU-Hong Kong S.A.R., China)
- Meriton Shoshi (NJIF-K / FIU Kosovo)
- Mike Lan (AMLD-FIU Taiwan)
- Lulwa Al Musalam (FINC-FIU Bahrain)
- Soraya Jesus Cardoso (UIF-Angola / FIU Angola)

2023 BECA Panel of Judges

- Mira Atias (IMPA-FIU Israel)
- Mohamed Al Ghatam (FINC-FIU Bahrain)
- Jade Chan (JFIU-Hong Kong S.A.R., China)
- Mary Campbell (FIUTT-FIU Trinidad & Tobago)
- Mohammed Shahid AHMED (NFIU-FIU Nigeria)

Furthermore, I'd like to recognize the dedication and hard work of the following FIU officials in helping create this third BECA book:

- Diana Rocco (FIU Vatican)
- Ervin Koci (FIU Albania)
- Fernanda Veloso Naves de Lima (FIU Brazil)
- Meriton Shoshi (FIU Kosovo)
- Ken O'Brien (FIU United States)
- Shardul (FIU India)
- Soraya Cardoso (FIU Angola)

Additionally, I thank Jérôme Beaumont, Executive Secretary, as well as Alyssa Habraken and Emilia Wei (the Senior Officers of the Egmont Group Secretariat) for their invaluable support throughout this process. I trust you will find these exceptional case studies engaging and that you will derive significant insights from the successful outcomes and remarkable cases investigated by the contributing jurisdictions.

Amr Sayed Rashed
Chair
Technical Assistance and Training Working Group
Egmont Group of Financial Intelligence Units
2022–2026

UNVEILING FINANCIAL CRIMES: **INSIGHTS FROM EXCEPTIONAL FINANCIAL ANALYSES BY FIUS**

The selected cases in this book share a common theme: exceptional financial analyses conducted by the Financial Intelligence Units (FIUs) involved. These cases demonstrate how analysts use financial data to uncover complex, illicit schemes. Often the information was obtained through suspicious activity reports or suspicious transaction reports, which provided fragmented details. However, FIU analysts pieced together these fragments to reveal intricate schemes involving numerous financial transactions and layered corporate and legal structures. Remarkably—despite having limited data to work with—analysts successfully traced and unraveled multimillion-dollar frauds and other financial crimes across multiple countries and continents.

This publication features 24 cases that showcase the outstanding financial analytical capabilities of the FIUs in uncovering various money laundering schemes and predicate offences worldwide.

The selection process involved evaluating the quality and range of analytical tools used, as well as the clarity of the planning, data collection, evaluation and presentation methods employed. These cases are meant to educate others about successful techniques for solving complex problems.

Leveraging Lessons Learned

There is no one-size-fits-all approach to financial analysis. These cases highlight the different approaches taken, including: analyzing financial data from open sources, collaborating with other FIUs, gathering data from the private sector and using criminal and financial information from justice and regulatory bodies. This helps readers extract ideas on the most effective tools for their own investigations and to better understand how meticulous financial analysis planning can yield excellent results. This publication also serves as an educational tool for FIUs, financial regulators and the entire anti-money laundering community in both the public and private sectors.

By sharing these cases, it demonstrates to anti-money laundering authorities which financial analysis tools were successful in uncovering crimes and how these methods can be replicated or adapted to suit local circumstances. The following cases illustrate how FIUs used investigative and analytical techniques to build successful cases, resulting in confiscation of stolen assets and punishment of the offenders. Crucially, they show how FIUs used intelligence to gather evidence from a wide range of sources and piece together a fact-based narrative of how crimes were committed.

It is possible that some anti-money laundering authorities and FIUs who read these cases may encounter these types of money laundering cases for the first time. Therefore, this helps them analyze those cases with the purpose of preparing for the potential introduction of similar illicit schemes within their jurisdictions. Adopting this hands-on mindset may help these readers detect such criminal schemes more easily and mitigate potential financial and other damages.

Meriton Shoshi (FIU Kosovo)

1

Bribery, Corruption and Tax Evasion

Bribery, corruption and tax evasion each poses a threat to states worldwide today. While globalization promotes economic transparency and the unrestricted movement of capital, goods and labour across borders, that openness also allows for the criminalization of national economies.

Personal gain, as well as the consolidation and retention of power are motivations behind such misdeeds. It creates a vicious circle: corrupt officials establish a network in which each individual's involvement in bribery serves as the foundation for a corrupt structure. Corruption undermines trust in governments and weakens the social contract.

The World Bank Group recognizes corruption as a significant obstacle to ending extreme poverty and promoting shared prosperity for the poorest 40 percent of people in developing countries. Studies show that the poor bear the brunt of corruption, as they often pay the highest percentage of their income in bribes. In some cases, the poor may be deliberately targeted due to their perceived lack of power to voice complaints.

Every embezzled or misused dollar, euro, peso, yuan, rupee or ruble denies the poor equal opportunities in life and prevents governments from investing in their human capital. In the public sector, corruption goes beyond officials accepting bribes to award contracts or favouring acquaintances when approving projects.

Corrupt officials may intentionally delay bureaucratic processes to increase their chances of personal enrichment. Lengthy queues for services or complex paperwork create incentives for citizens to offer bribes to jump the queue or bypass administrative hurdles.

These factors highlight the need to intensify the global fight against corruption. This is crucial for economic recovery, to ensure efficient use of taxpayers' money and to restore public trust worldwide. International organizations and governments around the world have introduced measures to combat Money Laundering (ML), specifically targeting the conditions that help legitimize illicit funds.

Addressing corruption—whether it's within government ranks, political organizations or businesses—often requires determined efforts to overcome vested interests. The countervailing effect of transparency and open governance is seldom sufficient. When public discontent with corruption and cronyism reaches a tipping point, the political benefits of addressing corruption often outweigh the costs of disrupting vested interests.

Examples showcased in this section demonstrate the vital role of Financial Intelligence Units in uncovering increasingly sophisticated corruption schemes. Those schemes include profiting from the misfortune of bankrupt individuals, using complex offshore accounts to launder bribes, disguising multimillion-dollar pork barrel scams as non-governmental organizations, and using corrupt government officials to secure government tenders and embezzle public funds.

To eradicate corruption, it is necessary to establish strong, legal and democratic practices within states. An absence of corruption is indicative of a society where the majority of the population is free, responsible and innovative.

The global community is committed to combating corruption: raising the standards for those employed by or appointed to governmental bodies, and implementing regulations to improve the relationship between state institutions and the population.

Tax evasion refers to the illegal act of deliberately avoiding paying taxes owed to the government by underreporting income, inflating deductions, hiding money or assets, or other fraudulent means. It involves intentionally deceiving tax authorities to reduce the amount of tax owed, thereby violating tax laws. Tax evasion is considered a serious offense and can result in severe penalties, including fines, imprisonment and forfeiture of assets. It differs from tax avoidance, which involves using legal methods to minimize tax liability within the bounds of the law.

Indicators

- **Suspicious cash-based transactions**, such as buying expensive items, paying off credit card debt, making large deposits into personal accounts and subsequently transferring them to overseas accounts, or primarily using cash through intermediaries to hide the audit trail.
- **Engaging in multiple financial transactions** to obscure the source of funds.
- **Using currency exchanges to send money abroad.**
- **Employing multiple offshore companies** to hide the true owner and complicate the audit trail.
- **Justifying the receipt of large sums of money** through the use of fraudulent contracts.
- **Embezzlement of state funds** through fraudulent NGOs.
- **Corrupt government officials** receiving kickbacks or commissions for facilitating the transfer of state funds.

CASE 1

One of the biggest fraud cases in the history of the Italian Republic —Italy UIF (Unità di informazione finanziaria per l'Italia)

Introduction

The Italian FIU (Unità di informazione finanziaria per l'Italia, or UIF), with the help of law enforcement and Italy's tax revenue agency, brought to light a multi-billion euro fraud and money laundering scheme involving the generation of fictitious fiscal credits in connection to legitimate measures introduced by the Italian government during the global pandemic. Collaboration with foreign FIUs was key in discovering a cross-border network that was creating false tax credits and laundering its illicit proceeds. As a result, assets abroad were successfully frozen. This case involved complex investigative activities, which led to tax legislation reforms, enforcement controls and national/supranational regulation to prevent further fraudulent behaviours.

Investigation

To foster economic recovery from the global pandemic, Italy's government introduced a series of fiscal incentives that provided tax credits to homeowners who renovated their properties. Risks associated with these incentives involved credits that were possibly fictitious nature and tax crimes (e.g., false invoices).

The UIF played a key role in the investigation, from its initiation to its conclusion, and in drawing attention of those involved.

To foster prompt detection of criminal activities connected to tax incentives, the UIF issued several communications calling reporting entities' attention to the risks associated with these measures. As a result, the Italian FIU received many Suspicious Transaction Reports (STRs) concerning newly established building companies selling to Italian financial intermediaries fiscal credits of a disproportionate amount compared to their structural organization.

Through operational analysis—carried out with the support of foreign FIUs and several Italian authorities—the UIF uncovered a large-scale network of natural and legal persons that, by means of complex financial schemes, were able to create and market a large amount of fictitious tax credits to various unaware intermediaries. Illicit proceeds were then laundered through cross-border transactions.

In particular, a considerable amount of money was transferred to companies incorporated in different EU member states, operating in sectors typically involved in fiscal frauds. These funds were immediately re-transferred to companies located in Asia (i.e., those already involved in other types of fiscal frauds to the detriment of the EU and Italy). Another part of the funds was invested in cryptocurrencies through virtual asset service providers (VASPs), located in Italy and other EU member states. A significant amount came back to Italy and was used for repeated cash withdrawals carried out from Italian ATMs. These were located near the legal offices of suspicious companies and involved foreign prepaid/credit cards linked to East European bank accounts. It also involved transfers to natural persons already known to the UIF to be affiliated with crime organizations and/or wire transfers used for capital deposit of newly incorporated companies, as well for as the purchase of luxury goods.

From UIF analysis, it emerged that large, suspicious flows were intermediated by the same EU-based E-Money Institution (EMI). Strategic analysis conducted by the UIF led to a deeper analysis of the foreign EMI, whose owners were found to be two Italians living abroad and subjects to pre-trial investigations for ML in three different countries. Proper information flows were implemented between the UIF, the competent FIU and the Supervisory National Authorities. The EMI's license was revoked for anti-money laundering deficiencies.

The UIF immediately shared its outcomes with national law enforcement agencies, which initiated investigations on several suspicious transaction reports. There was a subsequent judicial seizure of a large amount of credits sold and a successful freezing of assets abroad as a result of fruitful cooperation between FIUs.

The UIF played a strategic role in promoting regulatory amendments on trade of tax credits aimed at avoiding abuses. The UIF also significantly contributed to the development at international level of higher levels of awareness, with respect to further financial anomalies observed in this context (i.e., misuse of foreign credit cards, virtual assets financial activities and foreign EMIs).

FIU Action

The UIF focused its analysis on the authenticity of tax credits and on the ultimate destination of their sales proceeds.

The major acquiring financial institutions—obliged entities under Italian money laundering legislation—were invited by the UIF to verify any inconsistencies emerging from the documentation relating to the works underlying the tax credits. The following most frequent anomalies emerged: overpricing of the alleged renovation works with respect to average market prices, incorrect/non-existing building addresses to be restored, customers not corresponding with the owners of the buildings.

Italian Revenue Agency officials provided the UIF with full details on tax credit transactions recorded in its database.

Bank statement analysis performed by the UIF—benefitting from the exchange of information with approximately ten foreign FIUs—played a key role in tracking the use of funds from these tax credits. Experimental use of a data-mining software in this case highlighted the main hubs (i.e., natural/legal persons and flows) of the money laundering scheme, and was essential in identifying extended networks in a system characterized by multiple, complex transactions.

Evaluation

The results of analysis by the UIF on the improper use of tax credits and on the international money laundering scheme were immediately transmitted to Italy's finance authorities, its Anti-Mafia Investigation Department and to the National Anti-Mafia Directorate, due to the involvement of mafia-style organized crime in this illicit scheme. UIF intelligence was key for Italian law enforcement and judicial authorities in launching formal investigations and in supporting existing ones.

The large number of criminal proceedings regarding this fiscal fraud—mostly coming from STRs analysis—was reported in national and international press, leading to the Italian Finance Minister to refer to it as "one of the biggest frauds in the history of the Italian Republic." A total of (EUR) 4.4 billion in credits was estimated to come from non-existent building refurbishments.

Outcome/Contribution

Italian finance authorities further investigated the majority of the cases analyzed by UIF. Consequently there were several prosecutions and 35 people were arrested.

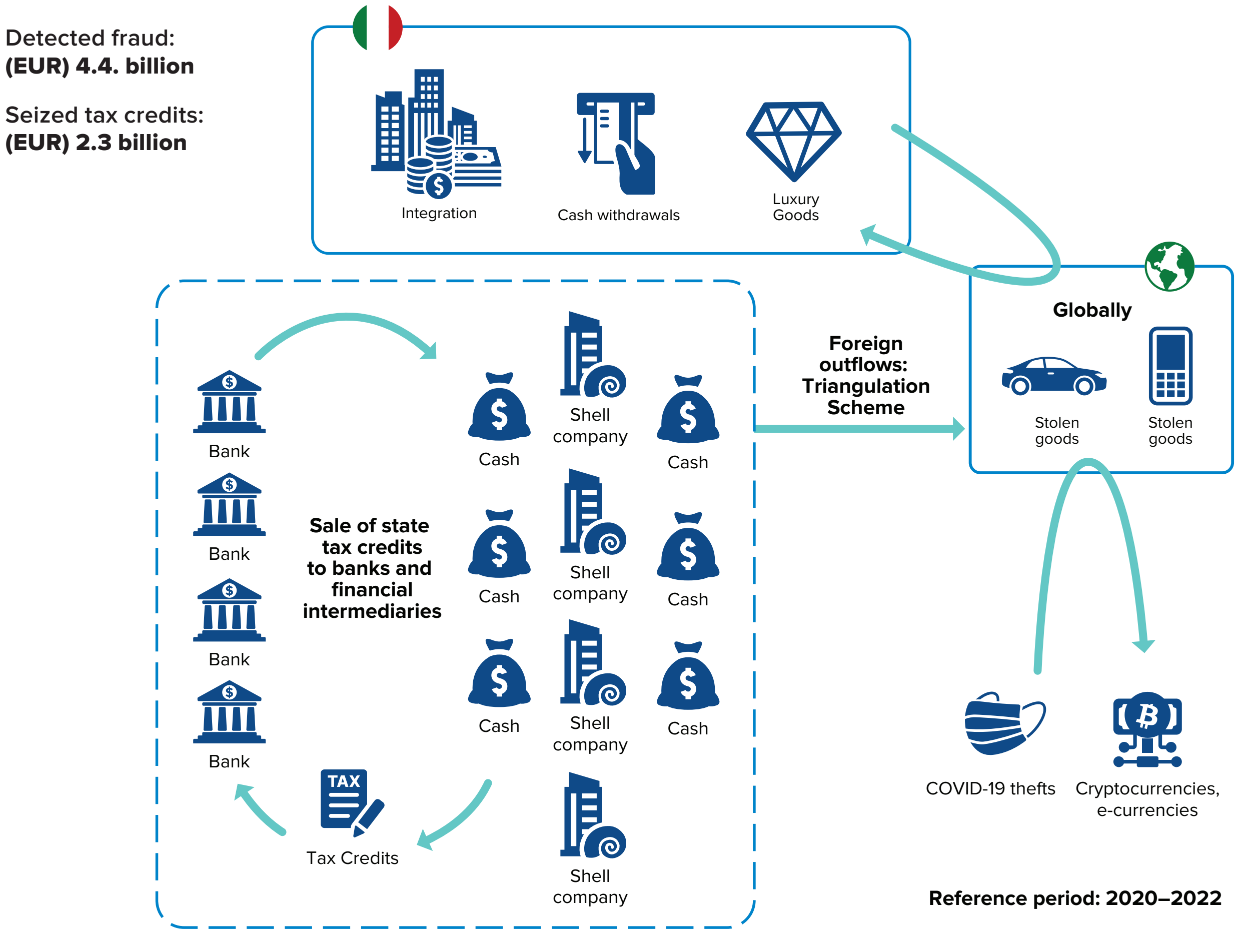
Measures taken by Italian law enforcement agencies included temporary freezing of bank accounts credited with the proceedings of sales. Judicial authorities also seized a total of (EUR) 2.3 billion in tax credits.

In the wake of the Italy's FIU analysis, the number of STRs and investigations, as well as the large amount of illicit funds moved abroad, the Italian government updated its legislation on tax credits transfers, involving the UIF in its definition.

Indicators

- **Recurrent anomalies in new vendors** of fiscal credits, including registered offices concentrated in limited geographical areas, capital contribution exclusively in cash, the use of frontmen, bank statements showing no charges for salaries or purchases of materials but only credits related to transfer price of fiscal incentives.
- **Significant amount of cash withdrawals** carried out from Italian ATMs with foreign prepaid credit cards.
- **Possible misuse of a foreign EMI**, whose license had been recently revoked for AML deficiencies, which resulted involved in this and further ML schemes and therefore subject to an extensive exchange of information between the UIF, the foreign FIU and supervisory authorities of both countries.
- **Increasing recourse for money laundering purposes to investment in cryptocurrencies** and decentralized finance applications.

CHART 1: FIU Italy, Misuse of tax relief



CASE 2

Youth with million-dollar government contract linked to corruption —Bolivia UIF (Unidad de Investigaciones Financieras)

Introduction

This case study involved contracts between an entity of the Bolivian government and a recently created company, Tu Auto. It was awarded a million-dollar contract for the acquisition of 41 ambulances, despite not having the necessary experience or track record and not providing the means to guarantee a contract of this magnitude.

Published complaints and the ensuing investigation revealed that the company in question had previously been awarded two other vehicle contracts by the same state entity.

The case achieved notoriety due to the profile of those involved, including Governor "J," who signed the awarded contracts. Among a series of events in this case includes government officials signing a receipt document for the ambulances without them being physically on site.

Investigation

The Bolivian FIU (Unidad de Investigaciones Financieras, or UIF) carried out a financial and asset analysis of those involved, indicating that Governor "J" was linked to acts of corruption for being the one with highest executive authority who signed the contracts.

Information sent by Bolivian Customs indicated that 87 vehicles were imported by "HT," the owner and legal representative of Tu Auto. However, the individual did not record significant movements in their personal accounts that could justify the payment for that number of imports. Likewise, it was identified that this person had opened bank accounts shortly before the events described between November and December 2021, as well as the signing of the contracts.

As a result of the investigation carried out by UIF, it was identified that Mrs. "MT" was the sister of the legal representative of Tu Auto. That individual formed a separate company, Car United, with two other people in April 2021.

During an eight month period from June 2021 to February 2022, Bolivian Customs registered 307 imported vehicles to Car United for an FOB value of (USD) 7,813,294.42 and a CIF value of (BOB) 58,631,380. The origin of the funds for these imports is unknown. The company in question was established two months before these imports began. Additionally, among the warning signs identified was a partner, 20 years old, who did not register operations within the financial system. It was established that this individual became the frontman in the case.

FIU Action

- The FIU requested information from subjects of the public and private sector, considering that these were state resources.
- As a result of the financial and patrimonial analysis, four reports were prepared that involved three companies and five individuals, as this was a case of management of public resources linked to corruption involving the crime of Legitimation of Illicit Gains.

Evaluation

The investigation took approximately three years to complete.

The case resulted in the apprehension of the main actors, including the executive authority of the Bolivian government. In addition to this case receiving media attention, the contract involving the acquisition of ambulances was annulled.

Outcome/Contribution

The apprehension of the individuals in this case and deepening analysis served as an important precedent for authorities in charge of public resources.

Indicators

- Suspicious transactions and operations identified with people who previously had **no records in the Bolivian financial system**.
- **The age of the individuals** who, despite being young and inexperienced, managed to form companies that were later awarded million-dollar contracts with the state.
- **Creation of companies** shortly before signing contracts.
- **Large number of vehicle imports** shortly after the formation of the companies without being able to identify the origin of the resources for the imports.

CASE 3

Nigeria’s former oil minister charged after $20 billion goes missing from petroleum agency —Nigeria FIU

Introduction

The result of a Nigerian FIU investigation revealed that former Nigerian Petroleum Minister, Diezani Alison-Madueke, leveraged her position to appoint her associate, Haruna Momoh, as Managing Director of Pipelines and Products Marketing Company Limited (PPMC), a subsidiary of the Nigerian National Petroleum Corporation (NNPC). Momoh misappropriated funds through his wife via various companies. Alison-Madueke directed NNPC subsidiaries to award (USD) $1.7 billion contracts to her associates, Aluko and Omokore. Offenses include bribery, corruption, fraud, forgery and tax evasion. Funds were laundered across multiple jurisdictions through shell companies. Collaboration between Nigerian FIU and law enforcement agencies led to asset forfeiture and US civil suits. Efforts continue to extradite individuals involved and repatriate stolen funds.

Investigation

The investigation of Alison-Madueke and her associates was a multi-faceted effort, delving into various aspects of corruption, fraud and money laundering.

It began with the receipt of Suspicious Transaction Reports (STRs) by the Nigerian FIU from financial institutions regarding transactions related to entities associated with the accused. The reports highlighted unusual patterns of cash withdrawals: just below the reporting threshold, totaling a significant amount within a short period. This raised suspicions of potential money laundering (ML) activities.

The FIU launched an analysis into the reported accounts, uncovering links between the account holders and high-level government officials, including Alison-Madueke. Further scrutiny revealed that Alison-Madueke had used her ministerial position to facilitate the appointment of her associate, Haruna Momoh, as Managing Director of PPMC.

A financial investigation was conducted on the activities of Haruna Momoh and his wife, Ochuko Eileen Momoh. They were found to be involved in suspicious transactions exceeding their known income. Transactions exhibited repetitive patterns of cash deposits followed by large withdrawals, often used for extravagant purchases globally, indicating potential money laundering.

The analysis also uncovered a complex network of shell companies spanning multiple jurisdictions, including Nigeria, the United Arab Emirates, the United States and the United Kingdom. These companies were used to funnel and launder illicit proceeds from corrupt contracts awarded by NNPC subsidiaries, facilitated by Alison-Madueke.

One of the pivotal points in the investigation was the identification of predicate offences such as bribery, corruption, contract fraud, forgery and tax evasion perpetrated by the accused individuals. These offenses formed the basis of the legal framework underpinning the investigation.

As the investigation progressed, collaboration between the Nigerian FIU and other domestic law enforcement agencies, such as the Economic and Financial Crimes Commission (EFCC) and the Independent Corrupt Practices Commission (ICPC), proved crucial. Information sharing and coordination between these entities help with evidence gathering and the initiation of legal proceedings against the perpetrators.

The case garnered international attention, leading to cooperation with foreign counterparts, particularly in the United States. The US Department of Justice filed a civil suit against Alison-Madueke, accusing her of benefiting from corrupt contracts awarded to entities associated with her associates.

The investigation also uncovered links between the accused individuals and high-value assets acquired with laundered funds, both within Nigeria and abroad. Properties purchased with illicit proceeds were identified and subject to asset forfeiture proceedings within the country. Efforts were also initiated to trace and recover offshore assets acquired through the laundering scheme.

Ongoing efforts by law enforcement agencies focused on extradition proceedings to bring the accused individuals to justice. Collaboration with foreign jurisdictions aimed to repatriate looted funds back to Nigeria, further demonstrating the commitment to combatting transnational financial crimes.

FIU Action

The Nigerian FIU employed innovative methods, including the Crime Records Information Management System (CRIMS) and Open-Source Intelligence (OSINT) analysis, alongside link analysis to efficiently gather and analyze data. Access to Nigeria's corporate registry database helped identify entities linked to contracts awarded by the NNPC, exposing connections to Mrs. Diezani and [confirm?] suspicions of fund misuse during elections in Nigeria.

Collaboration with domestic partners like the EFCC and ICPC facilitated further investigation, leading to arrests, prosecutions and asset seizures. The FIU provided timely information support to these agencies throughout the process.

Internationally, the Nigerian FIU collaborated with a European FIU on the Haruna Momoh and Ochuko Eileen Momoh case: aiding in identifying properties purchased with laundered funds. This led to a Mutual Legal Assistance Treaty request. Intelligence exchange with a Caribbean FIU concerning Kola Aluko revealed insights into companies registered under his name, enhancing the depth of the case.

The Nigerian FIU's innovative investigative techniques, domestic partnerships and international cooperation all contributed significantly to unravelling the complex laundering scheme involving Alison-Madueke and her associates, resulting in arrests, asset seizures and ongoing efforts for extradition and recovery of offshore assets.

Evaluation

In 2016, the Nigerian FIU received an STR regarding a company, Princess Jewelry, in which multiple cash withdrawals totaling (NGN) 113 million were conducted over two days: just below the reporting threshold. Analysis revealed the account owner, Ochuko Eileen Momoh, was the wife of Haruna Momoh, the former Managing Director of PPMC, who was appointed by then-Minister of Petroleum, Alison-Madueke. Further analysis of their accounts unveiled transactions exceeding their public servant profile, with suspicious patterns of cash deposits and withdrawals used for lavish purchases globally. The repetitive transaction pattern led to the inclusion of PPMC and NNPC in the analysis: expanding the case, alongside open-source information on Alison-Madueke's tenure as Minister.

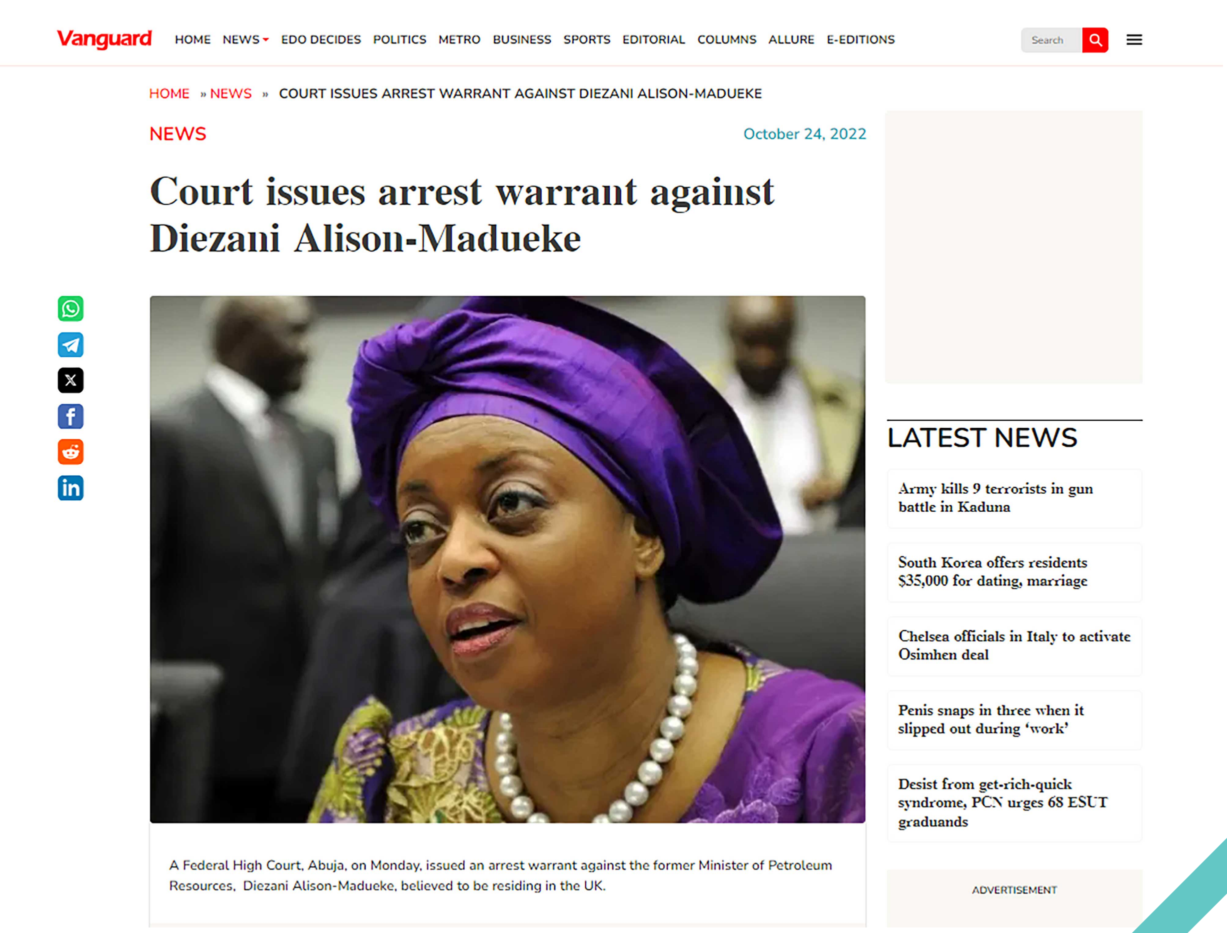
Outcome/Contribution

The case resulted in asset forfeiture for properties acquired with illicit proceeds within Nigeria, and initiated a civil suit by the US Department of Justice against Alison-Madueke. Collaboration between Nigerian FIU and law enforcement led to unravelling the complex laundering scheme, exposing bribery, corruption and contract fraud. Efforts are ongoing to extradite individuals involved and repatriate looted funds. This case is a testament to international cooperation in combating transnational financial crimes. It highlights the importance of robust financial intelligence units and cross-border collaboration in combating corruption and money laundering.

Indicators

- **Use of cash below threshold—**Multiple cash withdrawals below the reporting threshold, indicating an attempt to avoid detection.
- **Unusual transaction patterns—**Outflow rate from a bank account, patterns of cash deposits followed by withdrawals for extravagant purchases globally, suggesting potential money laundering activity.
- **High-value transactions—**Those exceeding the known profile of individuals as public servants, indicating possible illicit funds.
- **Rapid asset acquisition—**Occurring with high-value assets, such as luxury properties and yachts, potentially indicative of laundering proceeds from illicit activities.
- **Complex financial structures—**These involved shell companies and offshore accounts, used to obscure the origin and destination of funds.

ANNEX 1: Newspaper article on arrest of Diezani Alison-Madueke



HOME » NEWS » COURT ISSUES ARREST WARRANT AGAINST DIEZANI ALISON-MADUEKE

NEWS October 24, 2022

Court issues arrest warrant against Diezani Alison-Madueke

A Federal High Court, Abuja, on Monday, issued an arrest warrant against the former Minister of Petroleum Resources, Diezani Alison-Madueke, believed to be residing in the UK.

LATEST NEWS

Army kills 9 terrorists in gun battle in Kaduna

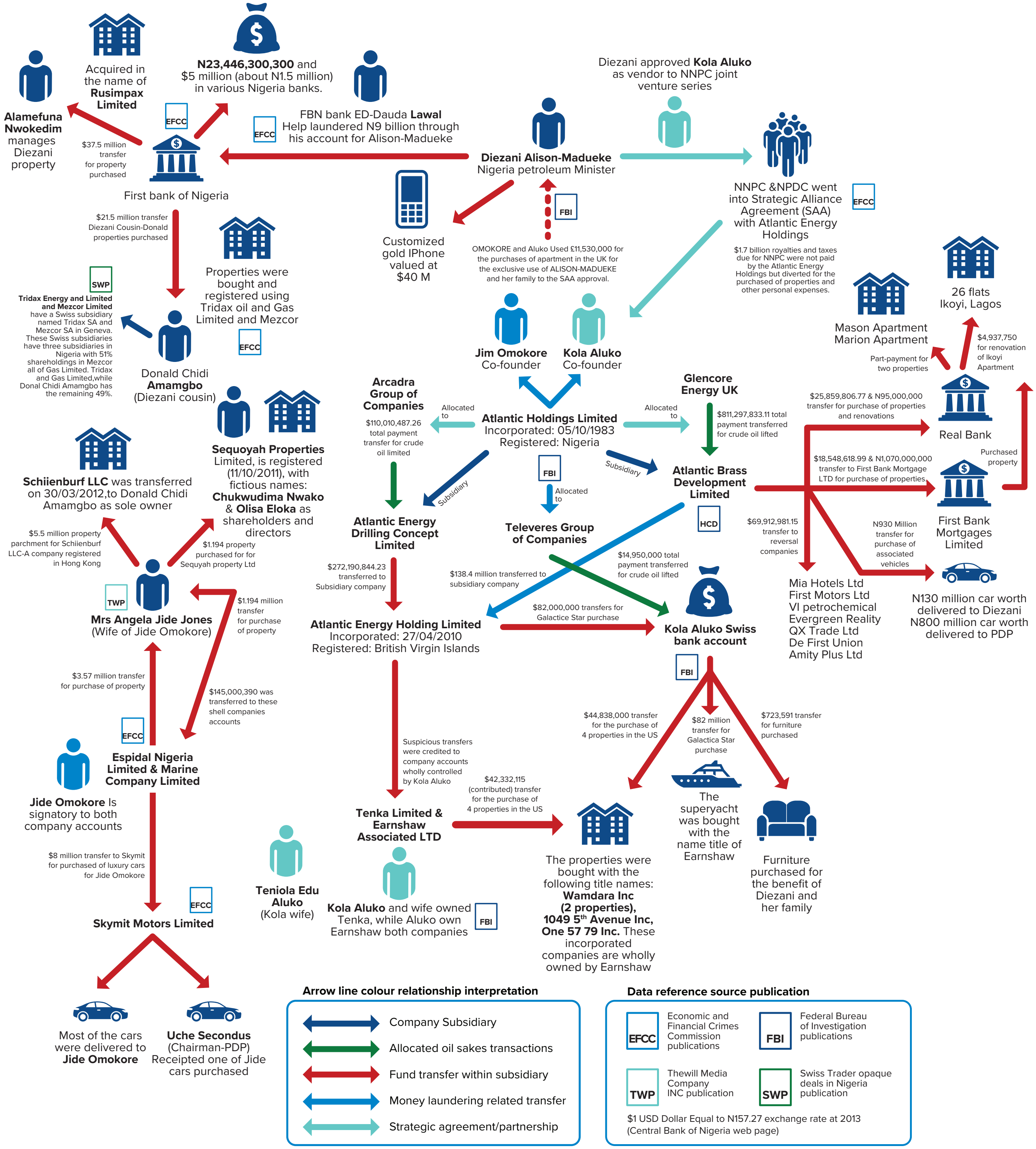
South Korea offers residents $35,000 for dating, marriage

Chelsea officials in Italy to activate Osimhen deal

Penis snaps in three when it slipped out during 'work'

Desist from get-rich-quick syndrome, PCN urges 68 ESUT graduands

ANNEX 2: Schematic representation of the case of former Nigerian Petroleum Minister, Diezani Allison-Madueke[1]



Alamefuna Nwokedim manages Diezani property

Acquired in the name of **Rusimpax Limited**

N23,446,300,300 and $5 million (about N1.5 million) in various Nigeria banks.

EFCC

$37.5 million transfer for property purchased

First bank of Nigeria

EFCC

FBN bank ED-Dauda **Lawal** Help laundered N9 billion through his account for Alison-Madueke

Diezani Alison-Madueke
Nigeria petroleum Minister

Diezani approved **Kola Aluko** as vendor to NNPC joint venture series

NNPC &NPDC went into Strategic Alliance Agreement (SAA) with Atlantic Energy Holdings

EFCC

$1.7 billion royalties and taxes due for NNPC were not paid by the Atlantic Energy Holdings but diverted for the purchased of properties and other personal expenses.

Customized gold IPhone valued at $40 M

FBI

OMOKORE and Aluko Used £11,530,000 for the purchases of apartment in the UK for the exclusive use of ALISON-MADUEKE and her family to the SAA approval.

$21.5 million transfer Diezani Cousin-Donald properties purchased

Properties were bought and registered using Tridax oil and Gas Limited and Mezcor

EFCC

SWP

Tridax Energy and Limited and Mezcor Limited have a Swiss subsidiary named Tridax SA and Mezcor SA in Geneva. These Swiss subsidiaries have three subsidiaries in Nigeria with 51% shareholdings in Mezcor all of Gas Limited. Tridax and Gas Limited,while Donal Chidi Amamgbo has the remaining 49%.

Donald Chidi **Amamgbo** (Diezani cousin)

Jim Omokore Co-founder

Kola Aluko Co-founder

26 flats Ikoyi, Lagos

Mason Apartment Marion Apartment

Part-payment for two properties

$4,937,750 for renovation of Ikoyi Apartment

Arcadra Group of Companies

$110,010,487.26 total payment transfer for crude oil limited

Allocated to

Atlantic Holdings Limited
Incorporated: 05/10/1983
Registered: Nigeria

Allocated to

Glencore Energy UK

$811,297,833.11 total payment transferred for crude oil lifted

$25,859,806.77 & N95,000,000 transfer for purchase of properties and renovations

Real Bank

Purchased property

Schiienburf LLC was transferred on 30/03/2012,to Donald Chidi Amamgbo as sole owner

Sequoyah Properties Limited, is registered (11/10/2011), with fictious names: **Chukwudima Nwako** & **Olisa Eloka** as shareholders and directors

Subsidiary

FBI

Subsidiary

Atlantic Energy Drilling Concept Limited

Allocated to

Televeres Group of Companies

Atlantic Brass Development Limited

HCD

$18,548,618.99 & N1,070,000,000 transfer to First Bank Mortgage LTD for purchase of properties.

First Bank Mortgages Limited

$5.5 million property parchment for Schiienburf LLC-A company registered in Hong Kong

$1.194 property purchased for for Sequyah property Ltd

$272,190,844.23 transferred to Subsidiary company

$138.4 million transferred to subsidiary company

$14,950,000 total payment transferred for crude oil lifted

$69,912,981.15 transfer to reversal companies

N930 Million transfer for purchase of associated vehicles

TWP

Mrs Angela Jide Jones (Wife of Jide Omokore)

$1.194 million transfer for purchase of property

$82,000,000 transfers for Galactice Star purchase

Atlantic Energy Holding Limited
Incorporated: 27/04/2010
Registered: British Virgin Islands

Kola Aluko Swiss bank account

Mia Hotels Ltd
First Motors Ltd
VI petrochemical
Evergreen Reality
QX Trade Ltd
De First Union
Amity Plus Ltd

N130 million car worth delivered to Diezani N800 million car worth delivered to PDP

FBI

$3.57 million transfer for purchase of property

$145,000,390 was transferred to these shell companies accounts

$44,838,000 transfer for the purchase of 4 properties in the US

$82 million transfer for Galactica Star purchase

$723,591 transfer for furniture purchased

EFCC

Suspicious transfers were credited to company accounts wholly controlled by Kola Aluko

Espidal Nigeria Limited & Marine Company Limited

Jide Omokore Is signatory to both company accounts

$42,332,115 (contributed) transfer for the purchase of 4 properties in the US

Tenka Limited & Earnshaw Associated LTD

The superyacht was bought with the name title of Earnshaw

$8 million transfer to Skymit for purchased of luxury cars for Jide Omokore

EFCC

Teniola Edu Aluko (Kola wife)

Kola Aluko and wife owned Tenka, while Aluko own Earnshaw both companies

FBI

The properties were bought with the following title names: **Wamdara Inc (2 properties), 1049 5th Avenue Inc, One 57 79 Inc.** These incorporated companies are wholly owned by Earnshaw

Furniture purchased for the benefit of Diezani and her family

Skymit Motors Limited

Most of the cars were delivered to **Jide Omokore**

Uche Secondus (Chairman-PDP) Receipted one of Jide cars purchased

Arrow line colour relationship interpretation

🟦 Company Subsidiary
🟩 Allocated oil sakes transactions
🟥 Fund transfer within subsidiary
🟦 Money laundering related transfer
🟦 Strategic agreement/partnership

Data reference source publication

EFCC Economic and Financial Crimes Commission publications

FBI Federal Bureau of Investigation publications

TWP Thewill Media Company INC publication

SWP Swiss Trader opaque deals in Nigeria publication

$1 USD Dollar Equal to N157.27 exchange rate at 2013 (Central Bank of Nigeria web page)

[1] Harvey, J., Bello, A. U., Doig, A., van Duyne, P. C., Gonul, M. S., van Koningsveld, J., Shehu, A., Sittlington, S., Sproat, P., Turner, S., & Ward, T. (2021). Final Report: Tracking beneficial ownership and the proceeds of corruption—evidence from Nigeria (Global Integrity) https://ace.globalintegrity.org/projects/benowner/

CASE 4

Family responsible for $20 million of tax fraud —Panama UAF, Unidad de Análisis Financiero)

Introduction

This case demonstrates how the Panama's FIU (Unidad de Análisis Financiero, or UAF) adapted to a new role during challenging times. Identified a potential tax crime committed abroad. Valuable information was provided to criminal prosecutors, resulting in a successful outcome.

The ability to analyze these kinds of cases became possible only after new legislation came into effect in 2020 (after tax crimes became a predicate offence in Panama). The tangible results of this investigation and an ensuing judgment in 2022 demonstrates that Panama is now capable of analyzing and investigating these crimes.

Investigation

Two Panamanian banks sent SARs about a Panamanian corporation (Corporation 1), created in 2014 to protect the assets of the "Golden" family in a country in the Americas Region (Country 1). Those SARs were supported by open sources, where two of Corporation 1's board members and members of the Golden family were mentioned in Country 1 newspapers in connection with a tax fraud case.

Corporation 2's income was not declared in Country 1 between 2017 and 2019. That conduct represented a tax fraud of approximately (USD) $20 million.

The individuals cited in this investigation also created other corporations in Country 1 to hide those assets. A member of the Golden family also had an Interpol Red Notice for arrest and extradition related to the tax fraud case (Subject 3).

There are two main bank accounts involved in this analysis:

- Bank account No. 1, belonging to Corporation 1 in Panama. This account is closed, but previously received international transfers from Country 1 of Corporation 1. This account also received transfers from Corporation 2 and Corporation 3. One of the Golden family members is a majority shareholder of Corporation 2. That same person also appears in open source news related to the tax fraud case.
- Bank account No. 2 is Subject 3's savings account, where he only received deposits from an account held by Corporation 1 in another Panamanian bank. This savings account was created to pay for Subject 3's personal expenses in Panama.

FIU Action

- UAF Panama initiated the analysis of the STRs by compiling information from our available databases.
- The intelligence analysis showed that another member of the Golden family (Subject 2) is a signatory and beneficiary of Bank Account No. 1. Similarly, Subject No. 2 is linked to the tax fraud case in Country 1 as the legal representative of the Corporation. The information gathered from the bank showed that Corporation 2 changed its name. As a result, Corporation 2 appeared in the Panamanian records under a different identity.
- The intelligence analysis also identified a vehicle linked to Subject 3. Subject 3 transferred this vehicle to a person unrelated to the Golden family in 2021.

- The UAF used an in-depth open source approach to identify the elements of its analysis.
- UAF Panama's analysis was used to provide an intelligence report to the Panama Attorney General's Office. This report helped identify a complex scheme in which Corporation 2 in Country 1 created other corporations for temporary use.
- UAF Panama collaborated with multiple government agencies such as the Transportation Authorities, Immigration and Public Registry to identify information on the subjects and corporations under analysis.

Evaluation

- UAF Panama initiated the analysis of the STRs by compiling information from our available databases and requesting information related to their bank accounts from the banks.
- UAF Panama's analysis was used to provide an intelligence report to the Panama Attorney General's Office.
- As a result of the UAF intelligence report, the Prosecutor's Office initiated a formal criminal investigation in July 2021.
- In January 2022, the Public Prosecutor's Office filed criminal charges against Corporation 1.
- In September 2022, the formal indictment is filed.
- In October 2022, the judge issued 26-month imprisonment sentence to Subject 3.
- In addition, information from the FIU contributed to the freezing of approximately $450,000. A vehicle was also seized.

Outcome/Contribution

- Subject 3 was arrested in July 2021.
- In October 2022, the Judge issues sentence giving 26 months' imprisonment to Subject 3.
- $450,000 and a vehicle were seized.

Indicators

- **Bank accounts created** to manage the funds of a foreign corporation whose main activity is developed in that country.
- **Negative news** related to a foreign beneficiary of a Panamanian corporation.
- **Payments identified with services rendered**, but with no refund of the cost of managing such payments abroad.
- **Accumulation of funds** after investments in real estate instead of the decrease of those funds.

Cybercrime, Virtual Assets & Child Pornography

Despite increased global regulation and enforcement, the use of crypto currencies in illegal trade and money laundering continues to grow every year. Preventing cyber criminals from exploiting the global financial system is a top priority for the Egmont Group and its members.

In the past, money laundering was primarily associated with organized crime and illegal drug trade. However, the increasing use of new technology and crypto currencies has not only made illicit online trade easier, it has also fueled cyber-based fraud.

Gaps in government regulation and control have led investors and criminals alike to view these markets as a potential safe haven for investment and as a means to commit cybercrimes while avoiding asset forfeiture in case of intervention by law enforcement agencies. Governments worldwide are struggling to develop regulatory frameworks to address the growing popularity of crypto currencies and determine how to handle digital currency in terms of taxation, assets and monetary policies.

The Financial Action Task Force revised its standards to mitigate money laundering and terrorism financing risks posed by virtual assets. Now, virtual asset service providers are required to implement a comprehensive range of preventive measures against these crimes. Meanwhile, criminals have been exploiting virtual assets to commit fraud, carry out SWIFT heists and engage in business email compromise schemes—among other activities.

These actions not only affect financial institutions, but also expose the global financial sector to substantial losses. They compromise business and personal email accounts by sending false payment instructions and other fraudulent information. Financial institutions can play a crucial role in identifying, preventing and reporting these fraudulent schemes by improving communication and collaboration with law enforcement agencies.

Financial Intelligence Units (FIUs) are encouraged to work together with financial institutions and law enforcement to quickly disseminate information related to suspected financial fraud and help recover funds for victims. Prompt action by victims, financial institutions, law enforcement agencies—and the subsequent international exchange of information—all contribute to successfully retrieving funds for victims.

The FIU plays a vital role in this process: not only in freezing funds, but also in identifying the appropriate authorities within their jurisdiction to engage with. Given the unique nature of cybercrimes and the ever-evolving use of virtual assets, the exchange of information between FIUs is crucial in combating these types of crimes.

Indicators

- **Crimes that span multiple jurisdictions.**
- **Use of smaller financial institutions.**
- **Weaknesses in regulations.**
- An **extended statutory holiday** that attracts cybercrime.
- **International cooperation aids in the timely detection and mitigation** of financial crimes.
- **Fraudsters often register a domain** that closely resembles their target.
- **Business email compromise schemes typically mimic communications from high-ranking executives**, such as the chief operating officer or chief executive officer, to prompt fund transfers into a changed bank account.
- **Funds are transferred to an unfamiliar recipient** within the company.
- **Transfers are initiated at the end of the day** or just before weekends or public holidays.
- The **receiving account has no previous record** of receiving large fund transfers.
- The **receiving account is a personal account**.

CASE 5

Financing terrorism with pre-paid vouchers—FIU France, Tracfin

Introduction

Between 2019 and 2023, investigations by France's FIU (Traitement du renseignement et action contre les circuits financiers clandestins, or Tracfin) demonstrated how crypto assets can be used as an effective terrorism financing tool, in which anonymously purchased vouchers are converted into crypto assets. As a result of Tracfin's analysis, a complex new terrorism financing scheme (mixing various financial tools) was identified; contributing to several convictions for terrorism financing and resulting in toughened domestic and European legislation.

Investigation

Triggering information—Tracfin initiated the case based on a Suspicious Transaction Report (STR) that mentioned a possible terrorist financing (TF) scheme, submitted by an e-money company that provides e-money accounts and prepaid vouchers.

First-level analysis—Thanks to direct access to law enforcement databases, Tracfin cross-checked the names of two suspects and established they had been sentenced in absentia to 10-year prison sentences for conspiracy to commit terrorism. They were identified as at risk of returning to France to commit terrorist attacks.

Suspected new TF scheme—After analyzing this information, Tracfin identified a potential new terrorism financing typology. The scheme uncovered by this first-level analysis was short-lived as it was blocked by financial institutions at the KYC ("Know Your Customer") phase. However, the suspects found new techniques to circumvent KYC checks, using digital tools to avoid the supervisory mechanisms of traditional cash transfer channels. In this new scheme, vouchers were purchased on French territory to fund crypto wallets held by jihadists in a war zone.

Detailed process—Through a France-wide network of retailers (e.g., tobacconists, news agents), Company Y was selling prepaid vouchers bearing a flash code or a PIN, allowing conversion into bitcoin. Vouchers sold by Company Y and convertible into bitcoins could only be "primo-credited" into a portfolio managed by Company Y.

Financial circuit (see diagram in Annex):

- A European e-money institution would issue e-money in Country A.
- An e-money distributor established in another European Union country (Country B) would distribute the e-money by loading it onto vouchers.
- A virtual asset service provider (VASP) established in France (Company Y) would distribute these vouchers to retailers.
- Retailers would collect customers' payments using a cash register software provided by Company Z that records the payment method used by the customer, but not their identity.
- Company Z would remit the funds to the e-money distributor in Country B.
- The e-money distributor would then transfer the funds to Company Y.

Since the e-money on the customer's voucher was used exclusively to purchase bitcoins held by Company Y, Company Y only fulfilled its due diligence obligations when it transferred those bitcoins to either the customer's crypto-asset wallet or to the one created by Company Y.

Tracfin uncovered the central role played by two collectors (referred hereinafter as "the suspects") affiliated with a jihadist group. They had opened two crypto-asset wallets in which they collected the bitcoins converted from the vouchers. Using a network of intermediaries and exchange offices, they would—for a fee—send money to jihadists in war zones.

This was done in the following manner:

- A customer would buy a voucher from a retailer, in cash.
- The customer would send the voucher's details (flash code or PIN) via encrypted message to a combatant in a war zone.
- The combatant would present these details to a local exchange office.
- The exchange office would check the validity of the voucher with the help of a suspect's relative.
- Once confirmed, the value of the voucher would be credited to one of the suspect's crypto-asset wallets. The money credited to the crypto-asset wallet would be routed through different bitcoin address clusters before being sent to a VASP.
- The VASP would clear the transaction with an exchange office in the war zone, using the hawala system.
- The funds would be paid out in cash, minus a commission, to the combatant.

Through this scheme, more than (EUR) 250,000 was transferred to the terrorist organisation over 10 months.

FIU Action

Tracfin adapted its investigative methods by combining the expertise of two of its teams: counter-terrorism investigations and crypto-asset analysis. The latter team used blockchain analysis to help uncover financial information about several of the individuals involved.

It also relied on:

- **Coordination with national administrative and judicial authorities.** This included having direct access to law enforcement databases and the engagement with judicial authorities via mutually exchanged information throughout the case. This was instrumental to all parties in their respective investigations.
- **Cooperation with the private sector.** The case led to multiple contacts with reporting entities (100 requests for information were sent to 15 reporting entities) and calls for vigilance on the typology. The quality of the public-private partnership played a decisive role in the success of this case.
- **Cooperation with FIUs**. More than 15 requests for information were sent to five foreign FIUs (Luxembourg, Belgium, UK, Malta and Germany). They were essential in identifying the financial methods used to collect funds (i.e., information on vouchers and timestamp, e-money or bank accounts and VASPs activity).

Evaluation

Tracfin received its first STR related to crypto assets in 2014. The number of such STRs continued to grow, reaching 518 in 2018. At that point, Tracfin created a specialized unit in charge of virtual assets related cases and assigned it the role of raising awareness among stakeholders and handling cases involving crypto assets.

To identify this new TF scheme, Tracfin made the most of the replies from its reporting entities and the exchanges with its counterpart FIUs. As a result, Tracfin was able to provide French judicial authority and LEAs with accurate and timely information to allow the exploitation of video surveillance records and set up targeted police operations aimed at identifying the anonymous purchasers of vouchers.

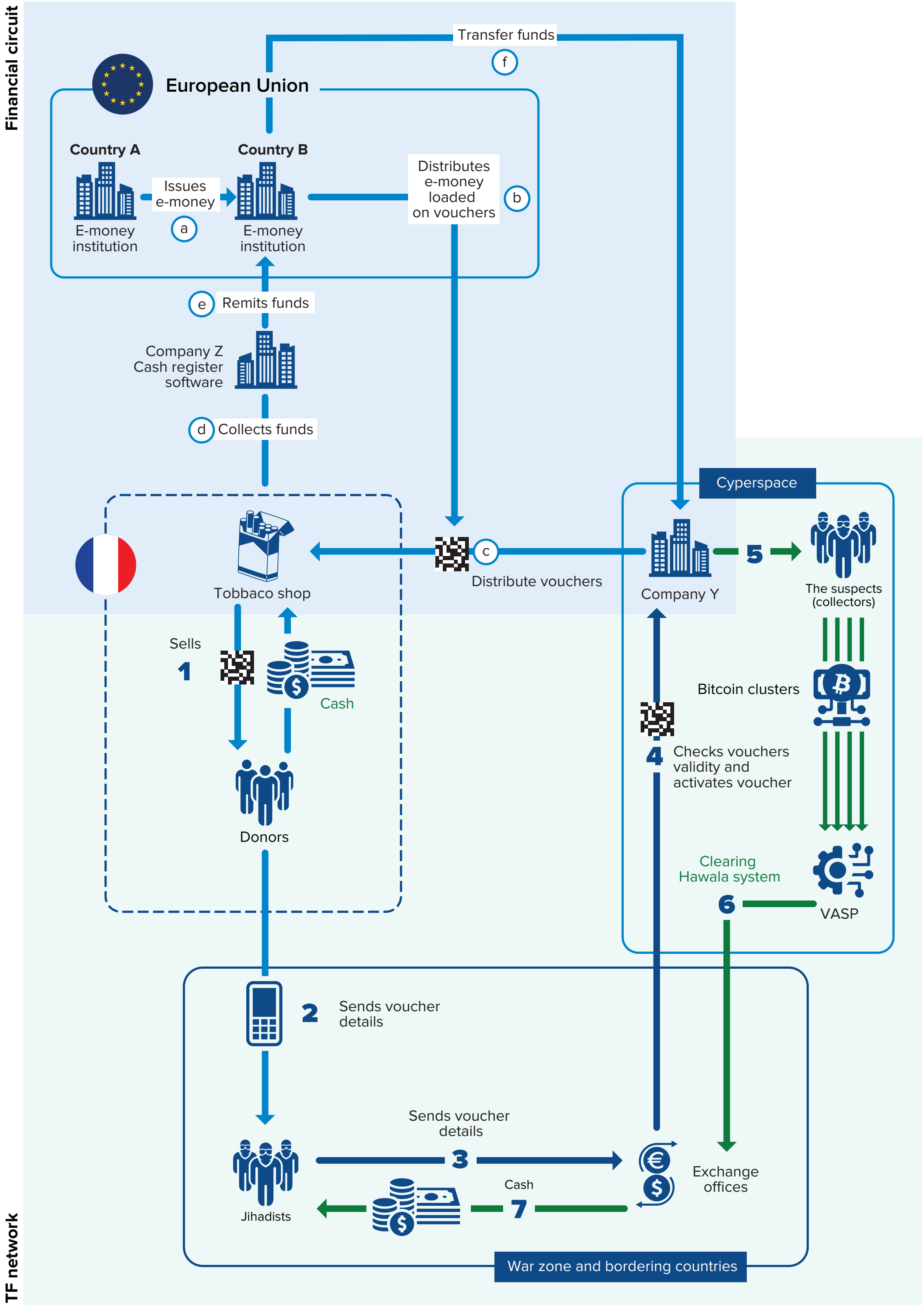
Outcome/Contribution

Tracfin contributed directly to the identification and arrests of 29 donors in France in 2021 (63 donors later in total), and of two individuals suspected of being the facilitators of the financial network in France. It also led to the seizure of crypto-asset wallets opened with the VASPs, adding the main suspect to the EU sanctions list for terrorist activity, thus freezing assets belonging to the main suspect's relatives. It also resulted in several sentences (including suspended ones) totaling 130 months in prison.

The case developed by Tracfin also had a strong, lasting influence on domestic legislation in France. After September 2020, changes were introduced to domestic laws on the anti-money laundering and combating the financing of terrorism (AML/CFT) obligations of VASPs. In 2021, legislation banned the use of anonymous e-money to buy crypto assets and made it mandatory for VASPs to identify customers for all transactions—even if occasional and from the first Euro. In addition, European legislation was adopted in April 2023 to better address this risk.

Indicators

- **Tracfin identified a new typology of TF** combining several assets enabling anonymity.
- The case confirmed that the **prepaid voucher sector and the crypto asset sector present a heightened TF risk**. The latter was considered in the September 2019 French National Risk Assessment, which mentions the use of new types of financing methods (e.g., prepaid cards) as a high-risk vehicle for terrorism financing, as well as in national and EU legislation.
- The **combination of traditional FIU investigative methods** (e.g., AML or CTF analysis through requests for information to reporting entities and foreign FIUs, exchanges with domestic authorities) and newer techniques (e.g., blockchain analysis) can produce highly successful results.


Financial circuit
Transfer funds
f
European Union
Country A
Country B
Issues
e-money
a
E-money
institution
E-money
institution
Distributes
e-money
loaded
on vouchers
b
e
Remits funds
Company Z
Cash register
software
d
Collects funds
Cyperspace
c
Tobbaco shop
Distribute vouchers
Company Y
5
The suspects
(collectors)
Sells
1
Cash
Bitcoin clusters
4
Checks vouchers
validity and
activates voucher
Donors
Clearing
Hawala system
6
VASP
2
Sends voucher
details
Sends voucher
details
3
Exchange
offices
Cash
7
Jihadists
War zone and bordering countries
TF network

CASE 6

Members of a narco organization sentenced to prison terms for drug smuggling using steel rolls —Argentina UIF (Unidad de Información Financiera)

Introduction

This case describes the dismantling of an international organization of Mexican, Canadian and Argentine citizens involved in drug trafficking using exported goods (steel coils) from Argentina to Spain and Canada. The organization relied on shell companies, which appeared to be engaged in licit commercial business. A broker provided services, placing money in the financial market by trading currencies, which were moved through transfers of virtual assets.

Investigation

Argentina's FIU (Unidad de Información Financiera, or UIF) received intelligence information associated with the detection of exports and unjustified banking movements, forming the basis of their investigation.

A collaboration request was later received regarding a court case initiated as a result of a spontaneous collaboration with the US Drug Enforcement Administration (DEA), in which a large-scale criminal organization purportedly dedicated to drug trafficking/smuggling was being investigated.

On receipt of intelligence information by the Argentine FIU, an investigation began on foreign trade transactions regarding the sale and shipment of steel rolls to a company located in Mexico, with its final destination being Spain and Canada. Of note was the unusual nature of the export, carried out by someone who was neither in charge of manufacturing nor commercializing the exported goods.

The investigation was supplemented by other information available in the FIU databases. That information was requested to analyze the links between the individuals under investigation and the detected holdings of equity, leading to a presumption of the existence of an economic group and the flow of funds channeled through bank accounts.

Based on the analysis of all the intelligence information gathered (aside from the exporter), other natural and legal persons involved in the maneuver were detected participating in the export activities and/or financial and/or exchange movements carried out for amounts exceeding the economic capacity with no justification of the source of funds. Those activities included the purchase of airplanes in the border zone.

Information was also obtained regarding border crossing, which allowed for the verification of the connection with the boss(es) or organizers of the criminal organization.

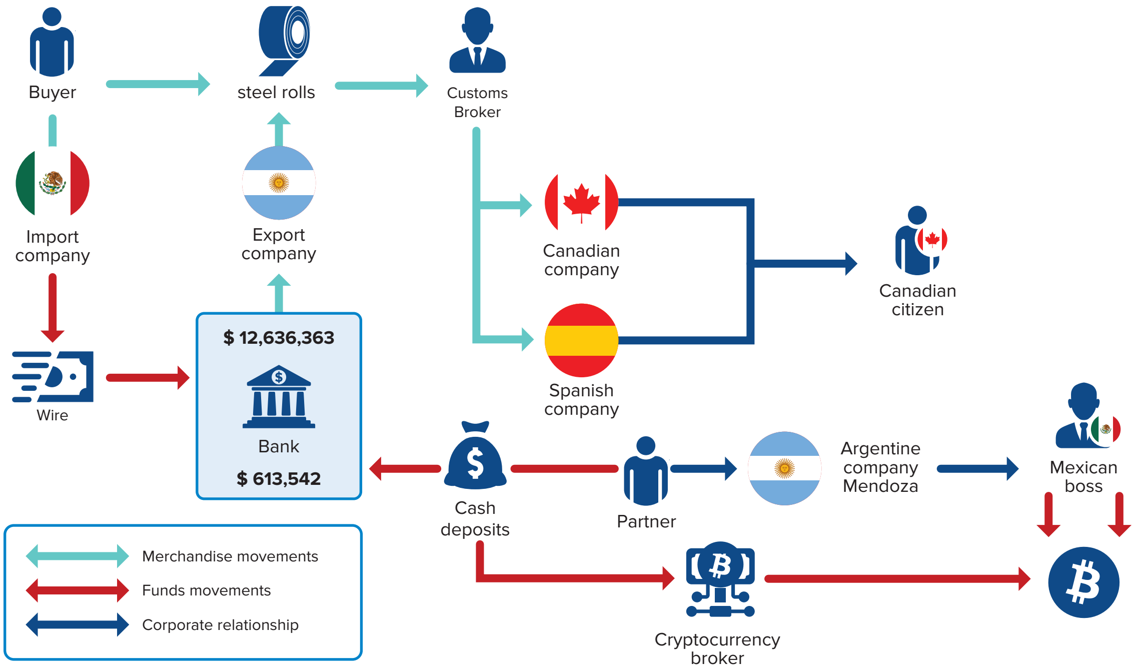
Regarding the broker that operated virtual and fiat assets—an Argentine citizen—it was determined his bank account was funded with cash and bitcoins, liquidated in US dollars (in cash) in Argentina. In his court statement, the broker indicated there were approximately eight transactions for a total amount of approximately (USD) 400,000. The assets were provided by the criminal organization and those amounts exceeding the broker's economic profile.

During the course of the judicial investigation, it was then proven the intervening broker made his knowledge and resources available to transfer the assets received in cash to Mexican citizens belonging to the criminal organization.

As a result of the investigation, the link between the companies recently created by Argentine citizens (used as shells by the criminal group) was established.

The result of the operation under analysis is shown in the flowchart below.

CHART 2: Result of the Operation



Link related to the case: https://www.fiscales.gob.ar/criminalidad-economica/bahia-blanca-condenaron-a-la-organizacion-narcocriminal-de-la-causa-bobinas-blancas-con-penas-de-entre-5-y-15-anos-de-prision/

FIU Action

As a result of a request for information from a foreign counterpart (i.e., by virtue of the lead of a citizen of that country with a drug-trafficking investigation in Argentina), the Argentine FIU was able to identify the individuals under investigation by a foreign country as the owner of the Argentina-based companies receiving the adulterated steel coils.

In turn, the foreign FIU provided Argentina's FIU with intelligence information, verifying that a partner from the shell company under investigation in Argentina carried out business with the economic group under investigation. This means that as a result of the information shared by the foreign counterpart, Argentina's FIU was able to detect one of the main heads of the criminal organization and confirm his links to Argentine companies.

The investigative tasks carried out in the Analysis Division of the Argentina FIU were useful for the ensuing judicial investigation.

Information was requested by various entities with a duty to report to the Argentine FIU regarding the individuals under investigation and in connection with the foreign trade transactions and the movements of funds verified in their bank accounts.

In addition, information was gathered regarding the involved companies and their shareholders and regarding the economic patrimonial status of the members of the criminal organization.

Simultaneously, the Argentine FIU received a request for collaboration from the local court. As a result, all new information regarding some of the subjects was gathered and analyzed in depth. Transactions were detected that could be deemed as money-laundering suspicious transactions. Among these were amounts credited to the bank account of the criminally charged assets broker.

The conclusions reached and the information gathered regarding assets of the criminal group were made available to the court.

Evaluation

Argentina's FIU collaborated with the judiciary through the submission of several reports elaborated by the FIU's Analysis Division, containing intelligence information related the economic-patrimonial-financial transactions/profiles. That work resulted in the identification of the group of companies, the criminal maneuvers and the assets belonging to the criminal organization.

The broker involved (acting as a facilitator) was convicted of **MONEY LAUNDERING**: a precedent in Argentina regarding a conviction for criminal activities associated with money laundering involving the use of virtual assets.

Outcome/Contribution

Argentina's court convicted seven members of a transnational drug trafficking criminal organization (three Mexican citizens and four Argentine citizens) with punishments ranging from 5–15 years in prison for the crime of **AGGRAVATED ILLICIT STORAGE OF DRUGS**.

The broker involved in the exchange maneuvers was sentenced to five years in prison and was ordered to pay a fine eight times the amounts of the transactions for the crime of money laundering through virtual assets. It was estimated the amount laundered was at least (USD) 468,400.

As a result of a search ordered by the court, almost two tons of cocaine were seized, valued at (USD) 60 million. Cash and property—such as cars, tools and machinery—were also confiscated.

Indicators

- **Reporting entities** performed well in identifying suspicious activities.
- **Cooperation on domestic and international information exchanges**.
- **Rapid detection** and **seizure of assets**.
- **Use of intelligence reports** by the court.

CASE 7

Over (USD) 95.2 million laundered with the use of money mules and the involvement of a hotel —Hong Kong, S.A.R., China JFIU (Joint Financial Intelligence Unit)

Introduction

This case involves a complex investigation and cross-border operation initiated by the S.A.R.'s FIU Hong Kong, S.A.R., China (the Joint Financial Intelligence Unit, or JFIU), leading to a crackdown on a cross-border criminal syndicate using virtual banks and cryptocurrency trading as conduit to launder crime proceeds derived from fraud.

Investigation

As recognized in the Mutual Evaluation Report, published by the Financial Action Task Force (FATF), Hong Kong, China (HKC) has a comprehensive AML/CFT regime. It consists of a robust legal framework, effective law enforcement, rigorous preventive measures, international cooperation, public education and publicity. To ensure informed decisions on formulating AML/CFT policy, a risk assessment on money laundering and terrorist financing (ML/TF) is updated periodically. In the latest assessment, HKC indicated fraud-related crime continues to be one of the most significant ML threats to the jurisdiction.

Given its status as an international finance, trade and transportation centre, HKC continues to be exposed to both external and internal ML threats—in particular, transnational/cross- border ML syndicates. The accelerated use of technology in the financial system has potential benefits in improving the accessibility to—and efficiency of—the system and unlocking new business opportunities to users. But it also provides new and faster ML channels for criminals. In the latest risk assessment, exploitation of virtual banks and virtual assets (VAs) by criminals to launder crime proceeds was identified as an emerging challenge for HKC.

In the first quarter of 2021, a virtual bank in HKC discovered 43 accounts being intensively connected with an extremely high volume of transactions. Some of the accounts were found receiving crime proceeds. This triggered a real-time monitoring alert. A U-turn pattern was also frequently observed.

The case was urgently referred to the JFIU. It conducted initial analysis on STRs, and found a common set of IP addresses and device IDs shared among the suspicious accounts. Crime proceeds mixed with crypto trading were circularly laundered among these accounts. The JFIU then enquired with banks and crypto-trading platforms on the targeted set of suspicious IP addresses. As a result, over 80 local bank accounts surfaced that had laundered (HKD) 740 million—equivalent to (USD) 95.2 million—in criminal proceeds in connection to at least 40 fraud cases reported in HKC.

Most of the bank accounts were short lived as the extremely high volume of turnover triggered additional due diligence. In the JFIU's initial analysis, it was believed these accounts were opened by money mules under the control of an ML syndicate. Based on the initial analysis, the JFIU conducted extensive enquiries to identify the syndicate and their activities.

The JFIU discovered the syndicate accessing the bank accounts and crypto-trading platforms via a Virtual Private Network (VPN) server, masking the original IP addresses. While the syndicate could not be located with the VPN IP address, JFIU evaluated all sharing device IDs, which identified every individual smartphone. This determined a set of devices most likely to be reused to operate new accounts to continue the money laundering activities.

JFIU monitoring revealed the digital footprint of a router used by the syndicate. That led the JFIU to be able to locate the operating centre of the syndicate: a hotel in a neighboring jurisdiction of HKC (Jurisdiction A, a non-Egmont member), which was involved in a conspiracy to defraud and engage in money laundering.

On further review of the opening processes of the suspicious accounts, JFIU found a local male appeared frequently behind the account holders in their account-opening photos. Most of the accounts were briefly accessed by the IP address of the male's residence or via his smartphone. Judging from the overall circumstances, the local male was believed to be a core syndicate member responsible for recruiting local money mules handing over the accounts to the syndicate in Jurisdiction A.

FIU Action

In this case, the syndicate recruited a large number of money mules to process the crime proceeds and exploit the anonymity of crypto trading to circumvent detection. To locate the genuine criminals behind the money mules, JFIU looked beyond transactions and examined every digital footprint left by each online access of the accounts. The JFIU also applied advanced analysis processes, including (but not limited to) in-depth analysis against large, diverse data sets that featured semi-structured and unstructured raw data from different sources. Those sources included IP addresses, tracking of specific device IDs and digital footprint associated from the tracked devices—all of which helped uncover otherwise hidden correlations and other insights.

In addition to digital footprint tracking, traditional methods (e.g., reviewing photos captured during each account login) were also deployed by the JFIU.

Evaluation

The JFIU took the lead, requesting bank log records of suspicious accounts for in-depth analysis. Through analysis and mapping, it found a set of common IP addresses and device IDs among the suspicious accounts.

In addition to fund flow and digital footprint tracing, the JFIU also conducted extensive review of photos captured when reviewing e-banking transactions involving the accounts of the money mules. In addition to the abovementioned money mule recruiter, the JFIU also found the background of the account-opening photos of the money mules matched the decor of some hotel rooms in Jurisdiction A. This important piece of information led to the identification of the target hotel.

Outcome/Contribution

The case is currently under active investigation by the Hong Kong Police Force (HKPF).

In September 2021, HKPF and law enforcement in Jurisdiction A mounted a joint arrest operation to neutralize the cross-border syndicate. A total of 14 individuals—including the account recruiter and over 10 money mule account holders—were arrested in HKC. Law enforcement in Jurisdiction A also arrested eight core syndicate members inside the target hotel for **CONSPIRACY TO DEFRAUD** and **MONEY LAUNDERING**.

Indicators

- **Observing the emerging risk of abusing virtual banks to conduct money laundering activities**, the JFIU is now coordinating with the regulatory authority of banks in HKC to encourage banks provide digital footprints in their STR submission. This was key in ensuring prompt, effective detection in the case.
- **Prompt reporting of the virtual bank** reflected the close working relationship between the JFIU and reporting entities. This case demonstrated the importance of public-private collaboration in detecting ML activities.
- With the assistance of law enforcement in Jurisdiction A, **eight core syndicate members were found renting rooms in the target hotel** in that jurisdiction. They had been operating the Hong Kong money mule accounts for ML for over a year.
- This **case illustrated the importance and use of intelligence exchange between FIU, regulatory authorities and reporting entities** in combating the evolving ML activities. The combined use of traditional intelligence gathering, analyzing digital footprints and cross-border collaboration were indispensable to this case.

CASE 8

Establishment of common indicators of sexual exploitation of children —Philippines AMLC (Anti-Money Laundering Council)

Introduction

For years, many young Filipinos suffered a silent, secret pandemic: the Online Sexual Exploitation of Children (OSEC). This case demonstrates that successfully fighting against online sexual exploitation is achievable via multisector collaboration and cooperation through various mechanisms involving public and private sectors and the international community.

OSEC is an emerging, constantly evolving, significant threat: not just in the Philippines but worldwide. It is the most disturbing aspects of cybercrime, extending across borders and has a deep, long-term impact on victims and the communities where they live.

Investigation

In 2019, the Anti-Money Laundering Council (AMLC) conducted its first study on child pornography in the Philippines, entitled *Child Pornography in the Philippines: An Evaluation using STR data (STR data from 2015 to 2018)*. The study used data from suspicious transaction reports (STRs) collected from that period. It identified OSEC as a significant, emerging threat in the country—and that Filipino children were especially vulnerable. The study noted that OSEC operations in the country range from local, small-scale enterprises to large-scale international organized networks operating inside and outside the Philippines.

According to Filipino government officials tasked with combating the problem, the Philippine child pornography industry is one of the biggest in the world, exceeding (USD) 1 billion a year. Foreign nationals from known offender countries operate in the Philippines with the assistance of Filipino nationals, who exploit Filipino children for child pornography[2].

The study identified some of the common indicators that possibly associate a transaction to OSEC. It also identified top locations where beneficiaries claim the funds and countries of the senders of funds.

Using that study as point of comparison, the AMLC then conducted in 2020 a global threat assessment, entitled "*Online Sexual Exploitation of Children: A crime with a global impact and an evolving transnational threat.*"[3] It also conducted a post-2019 study, entitled "*Child Pornography in the Philippines: Post-2019 Study using STR Data (STR data from 2019 to the first semester of 2020).*"[4]

[2] *Child Pornography in the Philippines: An Evaluation using STR data (STR data from 2015 to 2018)*

[3] http://www.amlc.gov.ph/images/PDFs/2020%20AUG%20AMLC%20OSEC%20AN%20EMERGING%20RISK%20AMID%20THE%20COVID19%20PANDEMIC.pdf

[4] http://www.amlc.gov.ph/images/PDFs/2020%20DEC%20CHILD%20PORNOGRAPHY%20IN%20THE%20PHILIPPINES%20POST-2019%20STUDY%20USING%20STR%20DATA.pdf

VOLUME OF STR's ASSOCIATED WITH OSEC

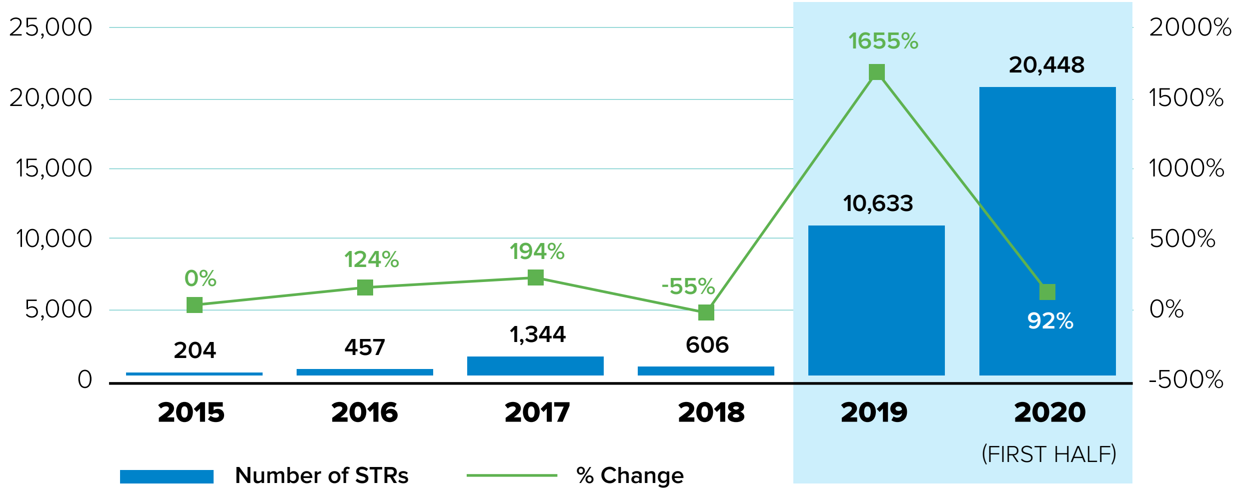


Figure: Yearly volume and increase of OSEC-related STRs received from 2015 to June 1, 2020 (as of run date, June 4, 2020).

Those two newer studies updated the findings in the first report and identified new trends in OSEC in the Philippines.

Major findings:

- A significant increase in the number of STRs from 2018 to 2019 until June 2020.
- Increase in suspicious transaction reporting can be attributed to the awareness of the Covered Persons (CPs)—the majority of which are money service businesses (MSBs), those that have become active in reporting suspicious transactions and attributed to the AMLC sharing its first study on OSEC.
- MSBs appear as the most preferred financial channel. This could be for two reasons: (1) stringent controls in the banking sector, particularly the know-your-customer (KYC) measures that deter criminals, and (2) accessibility of MSBs, which are visible in most areas, including remote rural locations. This allows easy access to facilitators and offenders to financial institutions.
- Awareness campaigns spearheaded by AMLC, other law enforcement agencies and private organizations, contributing to an increase in STR submissions.
- The use of electronic money issuers (EMIs) and virtual currency exchanges (VCEs) to channel funds, which could be an indicator of an emerging threat relating to the use of e-money and virtual assets as payment channels for child abuse content.
- A surge in the number of STRs observed during the start of the community pandemic quarantine (CQ) period in the Philippines. That can also be linked to the efforts of the AMLC, to other relevant agencies and to the private sector in spreading awareness about OSEC.

	YEAR					
Month	2015	2016	2017	2018	2019	2020
January	89	–	–	24	34	3,323
February	27	32	74	13	103	3,088
March	11	102	24	–	110	5,512
April	66	–	2	–	–	2,476
May	–	18	6	–	597	5,634
June	–	2	–	–	134	415*

- A significant increase in the amount of OSEC-related STRs during the CQ period. The average amount per transaction, however, is lower during the CQ period, compared with the same period in 2019. With those figures, the high volume of STRs during the CQ period can be associated with a high demand for OSEC materials (on the side of sex offenders), while on the side of OSEC facilitators, there appeared to be a need for money. That observation can be connected to factors brought about by the pandemic (e.g., travel restrictions due to lockdowns, giving more time for sex offenders to surf the web and prey on minors), the need for money due to work stoppages in which parents or older relatives of the victims found income online.

FIU Action

The AMLC recommended the following in regard to the Philippines' fight against OSEC:

- Continuous, increasing awareness and understanding on OSEC, particularly CPs.
- More information sharing among law enforcement and relevant offices, and close partnerships among the Financial Intelligence Units.
- Further strengthening and broadening the Public Private Partnership Program (PPPP), and information sharing platforms in the Philippines.
- Develop a collaborative multisector response by encouraging participation and involvement of law enforcement, professionals, private sector and civil society in conducting public awareness programs and campaigns.
- Create strong partnerships among law enforcement agencies, regulators and private-sector agencies.
- Observe timely information sharing, coordinated sharing of equipment for processing digital evidence, better preservation of evidence, avoiding duplicated efforts, reducing costs and ensuring bi-directional training of investigators.

To increase awareness about the threat posed by OSEC and the financial activities involved in these crimes, the AMLC studies, along with the list of Persons-of-Interest (POIs) were shared with the following groups:

- Domestic and foreign law enforcement investigating OSEC cases.
- Other relevant government agencies.
- FIUs of the countries identified to be sending remittances to the Philippines with consent to further share with their respective law enforcement agencies.
- The Bangko Sentral NG Pilipinas (BSP).
- CPs and other members of the AMLC PPPP.

The AMLC studies were also used and presented to various meetings and webinars with relevant stakeholders. A public version of the post-2019 study was posted in the AMLC website.

The AMLC's Financial Crimes Investigation Group (FCIG) also began an investigation on some of the POIs identified in the post-2019 study.

Evaluation

The first study paved the way to stronger collaboration among agencies, domestically and internationally and served as a benchmark for the second study.

The first study was as starting reference for the Egmont Information Exchange Working Group (IEWG) Project on Online Streaming of Child Sexual Abuse and Exploitation (CSAE), co-led by the AMLC, Australian Transaction Reports and Analysis Centre (AUSTRAC), and United Kingdom Financial Intelligence Unit (UKFIU). The project produced an amalgamated strategic intelligence picture related to online streaming of CSAE and a collation of financial indicators and keywords, disseminated to Egmont-member FIUs and to their respective law enforcement partner financial institutions[5].

The first study was used in the Trilateral Partnership Program (TPP) among the AMLC, AUSTRAC, and United Kingdom National Crime Agency (UKNCA). The collaboration among participating FIUs enabled the development of an operational list of Philippine facilitators and a snapshot of the identified offenders from Australia and United Kingdom[6].

The second study confirmed the involvement in OSEC of some POIs of a law enforcement agency. Cases were also referred to the AMLC[7]. Money laundering and/or child exploitation cases against these POIs have been filed before the Philippine Department of Justice (DOJ) and/or Regional Trial Court. Case information was also shared with the law enforcement and federal police of a foreign country.

Sharing the studies with various FIUs resulted in the expansion of the list of the study's POIs. It also helped generate leads to other potential POIs not identified in the study.

Outcome/Contribution

Sharing these studies domestically and internationally led to the expansion of the list of POIs, generating breakthrough leads that resulted in the arrest and prosecution of perpetrators. It also promoted awareness and raised public awareness about the evils of OSEC, prompting cooperation, including that of CPs.

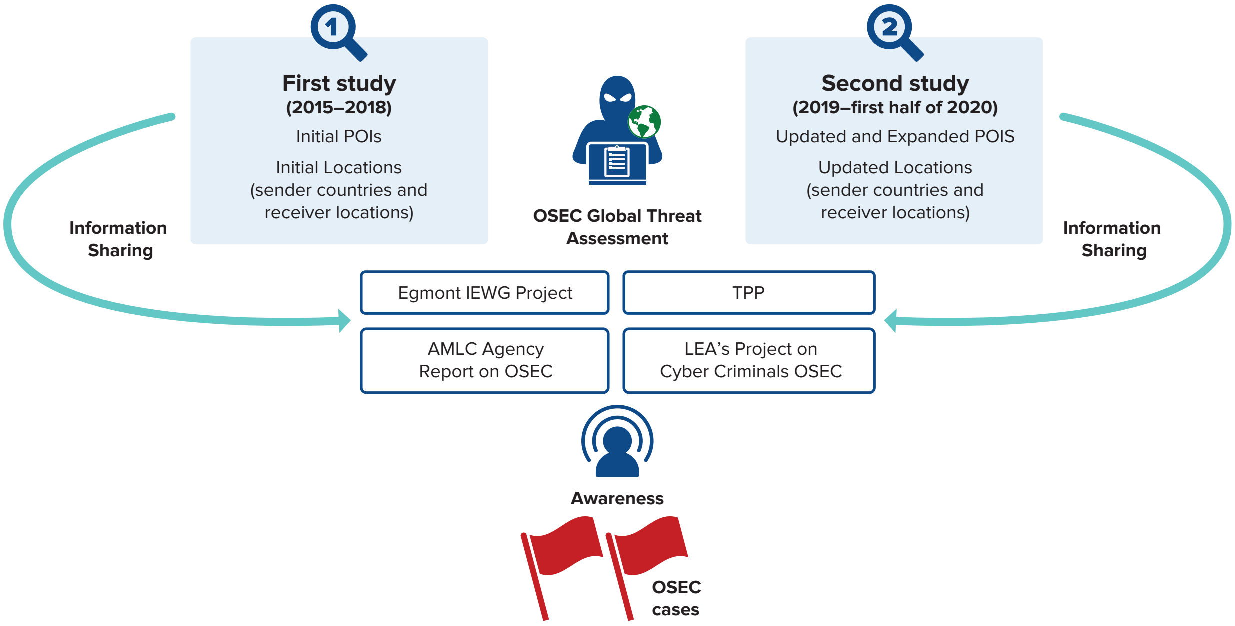
Among the significant outcomes of this sharing:

- Helped in the case build-up of an FIU and the arrest of one of the POIs identified in the report.
- An FIU filed a case to their Federal Prosecutor.
- Two FIUs used the post-2019 study and list of POIs for investigative and evidentiary purposes.
- The post-2019 study was part of the AMLC Agency report on OSEC submitted to DOJ Inter-Agency Council Against Trafficking (IACAT), used in the Cabinet Meeting with former President Rodrigo Duterte, which prompted the drafting of an Executive Order on strengthening efforts against OSEC via implementation of a multi-agency and coordinated approach.
- The post-2019 study caused the launch of a law enforcement agency in the Philippines aimed at intelligence and counterintelligence build-up, investigations and the subsequent arrest or neutralization of cyber criminals involved in child pornography cases nationwide.

[5] https://egmontgroup.org/wp-content/uploads/2021/09/2020_Public_Bulletin_Combatting_Online_Child_Sexual_Abuse_and_Exploitation_Through_Financial_Intelligence.pdf

[6] TPP Report on Live-Distance Child Abuse between Australia, United Kingdom and the Philippines.

[7] Three separate cases.



Indicators

Red-flag indicators related to child pornography identified in the AMLC studies include (but are not limited to) the following:

- Senders and beneficiaries of funds are usually **advanced in age, male foreigners from a western, Middle East country or high jurisdictions for child pornography**.
- **Individuals who send multiple remittances to different Filipino recipients** located in hotspots for child pornography in the Philippines (mostly in rural and economically depressed areas).
- **Senders who remit relatively low-value international or domestic remittances** to a large number of beneficiaries with unjustified purpose and relationship, (i.e., mostly non-familial).
- **Beneficiaries are usually unemployed or belonging to low-income class** and rely on remittances as a source of income.
- **Beneficiaries are usually either young adults or adults and are mostly females**.
- **Some beneficiaries were identified as minors or students.**
- **Beneficiaries related to each other as family members or relatives or who received remittances from same senders**.

Other indicators:

- The **amounts of the remittances are relatively low and below the reporting threshold.**
- **Remittances made usually through international and domestic MSBs**.
- **Beneficiaries claimed remittances from different branches of an MSB** within the same province or city.
- **Declared purposes** of the remittances are usually for daily costs, for example gifts, food, budget, salary, payment, allowances, miscellaneous fee, hospital bills, family support, allotment, store stocks/purchase of grocery, personal or household expenses, payments for bills, medicine, finances, maintenance, help, school payment, boarding house, transportation and travel.
- **Declared relationships** of the senders and beneficiaries (friend, boyfriend, fiancé, husband, brother, brother-in-law, boss, employer, uncle, cousin, sponsor or stepfather).
- **Swift or abrupt increase in the volume and number of transactions** over time by either the offenders or facilitators.
- Transactions of beneficiaries that **deviated during the global pandemic**.

3

Drug Smuggling & Gambling

Drug trafficking is a highly lucrative, illegal business practiced by criminal organizations including drug cartels. It generates billions of dollars in revenue annually, making it one of the most profitable criminal activities.

The United Nations Office on Drugs and Crime (UNODC) has observed a significant increase in drug use worldwide. In 2018, approximately 269 million drug users accounted for 5.3 percent of the global population between the ages of 15 and 64. By 2020, that number rose to an estimated 284 million, representing 5.9 percent of the population.

According to the Financial Action Task Force, drug trafficking yields substantial proceeds that must be handled discreetly. Criminals involved in drug trafficking employ various methods to control and conceal the funds, such as disguising their origins, altering their form, or transferring them to locations where they are less likely to attract attention.

Payment for drugs often involves large amounts of cash, which must be transported and eventually integrated into the legitimate financial system. This allows criminals to use the funds for personal expenses or to finance other illicit activities, while creating the appearance of legality.

Criminal groups are continuously adapting and innovating their distribution and payment methods. One notable trend is the growing industry of selling synthetic drugs online. The drug market has also become more diversified.

The UNODC's World Drug Report 2022 highlights the increasing complexity of drug markets, with the inclusion of numerous synthetic drugs that are not internationally regulated. Moreover, there has been a rapid increase in the non-medical use of pharmaceutical drugs.

Money launderers have many schemes to conceal the large amounts of money generated by illegal businesses. This section examines the connection between money laundering and activities such as smuggling and gambling.

Smuggling involves moving significant sums of money that need to be laundered. For instance, tobacco and cigarette smuggling presents a financial incentive to source products from cheaper markets and distribute them in markets where they can be sold at higher prices. This can involve both domestic and international movements, taking advantage of price differences within communities. Illicit tobacco trade encompasses various activities, with smuggling being driven by the desire to avoid excise taxes and circumvent regulations prohibiting the sale of such goods.

Gambling—particularly at casinos—offers another avenue for money laundering. Although casinos are not classified as financial institutions, the large number and frequency of transactions in this sector make it highly susceptible to money laundering. Casinos deal largely in cash, and their operations involve financial activities similar to those of traditional financial institutions, making them an attractive option for money launderers. Understanding the methods of money laundering in the gambling sector is crucial for policymakers and experts in combating financial crimes.

Implementing measures such as identifying warning signs and adopting a risk-based approach—and requiring employees to report any knowledge or suspicion of money laundering by customers, guests or colleagues—can help prevent money laundering within this industry.

Indicators of tobacco smuggling include the level of expertise displayed by individuals or groups involved in smuggling, and the ability to mitigate the risk of detection at various stages of the smuggling process, which directly impacts the profit margins of criminals.

In the casino sector, red flags for potential money laundering include clients providing false or counterfeit identification, using multiple names or aliases, or employing counterfeit bank-payment cards.

Through analysis of financial transaction data, Financial Intelligence Units (FIUs) have been able to trace the origin and destination of funds and establish connections between different criminal groups that were previously unknown to law enforcement agencies.

CASE 9

A global operation of illegal online gambling —Israel Money Laundering and Terror Financing Prohibition Authority (IMPA)

Introduction

This case involved a complex investigation where an in-depth strategic analysis conducted by the Israel's FIU (the Israel Money Laundering and Terror Financing Prohibition Authority, or IMPA) triggered the start of a joint investigation by a multi-agency task force against a global operation of illegal online gambling, which is a medium-high risk in Israel. The network made use of seemingly legitimate businesses, front men and virtual assets.

Contributing to the success of the case was strong domestic cooperation between agencies within a dedicated task force, the use of sophisticated IT tools and data mining abilities, and the international collaboration between IMPA and key counterpart FIUs, resulting in immediate freezing of assets abroad.

Investigation

Within the framework of a dedicated task force against illegal online gambling, IMPA conducted a thorough strategic analysis of financial intelligence to identify suspicious entities involved in online gambling activity. The analysis included keyword searches in Unusual Activity Reports (UARs), statistical analysis of Currency Transaction Reports (CTRs) and a review of open-source intelligence—all in conjunction with relevant data sources. Within the analysis, relevant typologies, indicators and activity patterns that characterize online gambling were considered.

IMPA's analysis resulted in detailed network analysis and fund-flow charts showing the money trail. This included details about transactions made within Israel and abroad between the parties involved. It also included transaction amounts and dates, bank accounts details and other available information. By using advanced IT tools during the investigation, IMPA was able to detect links to new suspects, as well as assets and businesses abroad. The links were further established through information received from counterpart FIUs within the framework of information requests.

IMPA disseminated a spontaneous disclosure based on the results of the strategic analysis to the Israeli National Police (INP) regarding an entity who had not previously been investigated. This disclosure led to the start of an investigation by the thematic Task Force comprising representatives from the INP, the Israeli Tax Authority (ITA), the State Attorney's Office (STO), and IMPA. Within the Task Force, IMPA's intelligence was shared and examined, along with information from all other participating agencies to compile the broadest and most comprehensive picture possible. The information disseminated by IMPA helped create a full understanding the criminal activity, the key entities involved, and the money laundering scheme used.

The investigation revealed a scheme involving a worldwide online gambling network operating in sophisticated, innovative ways to organize illegal gambling activities, collect and distribute funds and launder the proceeds. The network made use of seemingly legitimate businesses, front men and complex money-laundering methods, including the use of virtual assets. The criminal activity revealed a wide scope of offences, including money laundering, illegal online gambling, fraud and tax evasion.

As the investigation evolved, IMPA sent information requests to several FIUs in countries where the involved entities operated, either physically or through their financial activity. The FIUs replies consisted of new, valuable information and revealed newly involved entities. It also included financial transactions, information on business activity, bank account details and related assets. This information enhanced intelligence and deepened understanding of the involved entities' cross-border activities and helped substantiate the case against them. Following an urgent request via the Egmont Secure Web (ESW), the FIU of Ukraine and IMPA took coordinated, coherent actions carried out both via correspondence and telephone. This cooperation led to the immediate, successful freezing of the bank accounts of the main suspect and his spouse by Ukraine's FIU. This provided time needed to proceed with a formal request for mutual legal assistance.

Eventually all the gathered information was integrated for use by the STO to continue with the subsequent legal actions, including asset seizure and submission of indictments.

FIU Action

IMPA played a key role in initiating this investigation, by conducting a strategic analysis using sophisticated methods and IT tools to assess known red flags and typologies relevant to money-laundering of proceeds from online gambling. The analysis led to the identification of an individual whose financial activity raised a suspicion of involvement in illegal online gambling activity and the laundering of the illicit proceeds. IMPA's spontaneous disclosure to the Task Force led to initiation of the investigation. IMPA also contributed significantly to the development of the case by: mapping the natural entities and businesses involved, providing intelligence reports, confirming the suspicions about the offenses, and by giving a comprehensive financial intelligence picture about the way the funds were moved. Following the covert phase of the investigation, IMPA diligently pursued additional intelligence about both new and existing involved subjects, affiliated entities and their operations.

To investigate illegal activity abroad in this case, IMPA sent information requests to several foreign FIUs. The information received from those foreign FIUs and from local reporting entities enabled IMPA to detect cash transfers abroad and identify the methods used by the parties involved to collect the gamblers' funds, transfer them to related accounts and integrate the proceeds into the legitimate financial system.

Evaluation

This case exemplifies close domestic collaboration and joining forces internationally to investigate a complex scheme as part of the joint Illegal Online Gambling Task Force. IMPA used its unique financial information and sophisticated IT tools to compile the most comprehensive picture possible, which led to the exposure of a complex illegal international online gambling network. In this case, financial intelligence information played a crucial role at every stage of the investigation, demonstrating how successful results are achieved when the FIU forms an integral part of the investigation team throughout the covert, overt and pre-trial stages.

IMPA's cooperation with foreign counterpart FIUs was very significant. It revealed valuable information about new entities and led to investigation advancement and the immediate freezing of funds abroad by the counterpart FIU.

Outcome/Contribution

The total value of the offenses was estimated at (ILS) 29.2 million, and the value of the assets seized in Israel was (ILS) 3.4 million. When the investigation became public, seven suspects were arrested, and dozens of people were detained for questioning and for evidence collection. The State Attorney's Office submitted six Mutual Legal Assistance (MLA) requests to various jurisdictions.

The prosecution filed an indictment against four key persons operating the illegal network. The indictment includes four charges of **MANAGING AND ORGANIZING ILLEGAL GAMBLING** worth approximately (ILS) 3.0 million, **MONEY LAUNDERING**, **RECEIVING PROPERTY BY DECEPTION** and **SEVERE TAX EVASION**.

Indicators

Indicators alone may not always lead to suspicion of illegal online gambling, but they can be a very useful resource in triggering enhanced inspection and further monitoring.

Indicators in this case include:

- **Frequent, low-value money transfers sent to a bank account** without reasonable business explanation and frequently performed using different methods of payment. Micro transactions are a financial behaviour associated with gambling activity.
- **Business activity likely to be associated with video games or other types of online casino games**, such as poker. In this case, the suspects used an online store selling gaming tokens and coins as a platform to transfers the proceeds.
- **Rapid deposit and withdrawal cycles** in a bank account, resulting from dozens of players frequently depositing money for bets and the operators quickly withdrawing those funds to avoid noticeable accumulation in the account.
- An **account characterized by numerous sources of deposits** juxtaposed with significantly fewer beneficiary accounts.
- **Multiple deposits originating from different accounts** that do not appear to be related to one another or linked in any way.

CASE 10

Illicit drug trafficking —Ecuador UAFE (Unidad de Análisis Financiero y Económico)

Introduction

Ecuador's FIU (Unidad de Análisis Financiero y Económico, or UAFE) carried out a Report of Unusual and Unjustified Operations (ROII, or Reporte de Operaciones Inusuales, Injustificadas) for an alleged crime of money laundering in which several people were analyzed as part of a structure of illicit drug trafficking in narcotic and psychotropic drugs.

Investigation

The UAFE sent the ROII to the State Attorney General's Office, with which the investigation corresponding to the crime of money laundering could begin.

FIU Action

Ecuador's FIU proceeded to carry out a search of information due to an alert signal on Mr. Luargas García Wilson Wilfredo (Guatemalan citizen) and his spouse Mrs. Mejía Loor Aída Ximena (Ecuadorian citizen). A few days after his arrival in Ecuador in 2011, he received a transfer from the United States for (USD) 360,000, of which (USD) 258,000 was sent through transfers and cheques payable to Mr. Parrales Panchana Segundo Marcos.

In 2014, at the age of 18, Mrs. Mejía García Aída Ximena, with a single marital status, purchased a vehicle for (USD) 38,835, paid in several cash payments. In 2015, Mr. Luargas García Wilson Wilfredo, married Mrs. Mejía Loor Aída Ximena. Subsequently, in the same year, Mrs. Mejía and her spouse constituted a company in Panama, holding the positions of Director-Treasurer, and Attorney-President, respectively. The company was dissolved in March 2016.

It is important to mention that, in 2018, Mr. Luargas García Wilson Wilfredo was extradited from Guatemala to the United States for the crime of **DRUG TRAFFICKING**.

Evaluation

UAFE received a warning signal from which the analysis of information of the people under investigation began. Information was extracted from the UAFE database that appears in the System for the Prevention of Money Laundering and Financing of Terrorism (SISLAFT), through which the originators and beneficiaries of related transactions were identified with the people analyzed in the case of cash and cheque deposits, paid cheques that were cashed and transfers received and sent locally.

Once the banks where the analyzed subjects registered accounts were identified, account statements, legality of funds, images of cash and cheque deposits, paid cheques, SWIFT messages of transfers received and sent from abroad were requested.

Likewise, the notaries were required to provide the deeds of the procedures carried out by the analyzed subjects regarding the acquisition of goods.

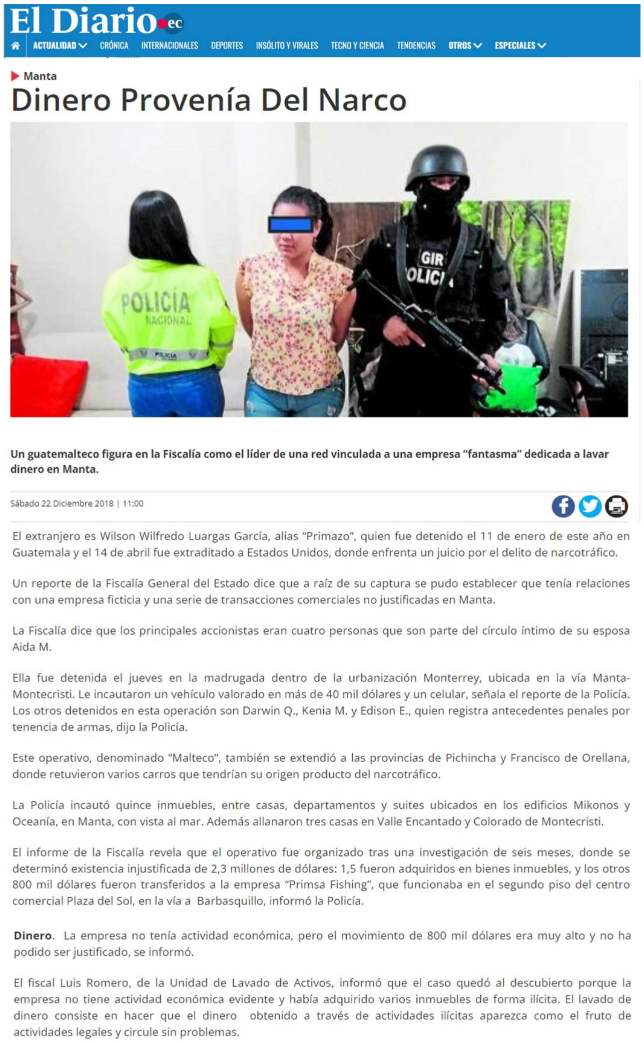
With the information described, the UAFE proceeded to analyze and prepare the Report of Unusual and Unjustified Operations, which was sent to the State Attorney General's Office in 2018.

Outcome/Contribution

The Ecuadorian state sentenced Mrs. Mejía Loor Aída Ximena, spouse of Mr. Luargas García Wilson Wilfredo, and two other people involved to 10 years (second instance sentence).

Indicators

- **Real estate purchased** for approximately (USD) 357,617.31.
- **Vehicles purchased** for approximately (USD) 223,217.00.
- The **vehicles were paid** for by different people through cash deposits.
- Company constitution in a **tax haven**.



Manta

Dinero Provenía Del Narco

Un guatemalteco figura en la Fiscalía como el líder de una red vinculada a una empresa "fantasma" dedicada a lavar dinero en Manta.

Sábado 22 Diciembre 2018 | 11:00

El extranjero es Wilson Wilfredo Luargas García, alias "Primazo", quien fue detenido el 11 de enero de este año en Guatemala y el 14 de abril fue extraditado a Estados Unidos, donde enfrenta un juicio por el delito de narcotráfico.

Un reporte de la Fiscalía General del Estado dice que a raíz de su captura se pudo establecer que tenía relaciones con una empresa ficticia y una serie de transacciones comerciales no justificadas en Manta.

La Fiscalía dice que los principales accionistas eran cuatro personas que son parte del círculo íntimo de su esposa Aida M.

Ella fue detenida el jueves en la madrugada dentro de la urbanización Monterrey, ubicada en la vía Manta-Montecristi. Le incautaron un vehículo valorado en más de 40 mil dólares y un celular, señala el reporte de la Policía. Los otros detenidos en esta operación son Darwin Q., Kenia M. y Edison E., quien registra antecedentes penales por tenencia de armas, dijo la Policía.

Este operativo, denominado "Malteco", también se extendió a las provincias de Pichincha y Francisco de Orellana, donde retuvieron varios carros que tendrían su origen producto del narcotráfico.

La Policía incautó quince inmuebles, entre casas, departamentos y suites ubicados en los edificios Mikonos y Oceanía, en Manta, con vista al mar. Además allanaron tres casas en Valle Encantado y Colorado de Montecristi.

El informe de la Fiscalía revela que el operativo fue organizado tras una investigación de seis meses, donde se determinó existencia injustificada de 2,3 millones de dólares: 1,5 fueron adquiridos en bienes inmuebles, y los otros 800 mil dólares fueron transferidos a la empresa "Primsa Fishing", que funcionaba en el segundo piso del centro comercial Plaza del Sol, en la vía a Barbasquillo, informó la Policía.

Dinero. La empresa no tenía actividad económica, pero el movimiento de 800 mil dólares era muy alto y no ha podido ser justificado, se informó.

El fiscal Luis Romero, de la Unidad de Lavado de Activos, informó que el caso quedó al descubierto porque la empresa no tiene actividad económica evidente y había adquirido varios inmuebles de forma ilícita. El lavado de dinero consiste en hacer que el dinero obtenido a través de actividades ilícitas aparezca como el fruto de actividades legales y circule sin problemas.

Source: www.eldiario.ec/noticias-manabi-ecuador/490599-dinero-provena-del-narco.

CASE 11

Drug trafficking by father and son —Fiji FIU

Introduction

A father and son, Tallat Rahman and Joshua Aziz Rahman, were involved in a joint criminal enterprise of importation, exportation and distribution of controlled drugs across multiple jurisdictions.

The complexity of the case involved law enforcement authorities from several jurisdictions conducting parallel investigations of a joint criminal enterprise that was importing methamphetamine and cocaine into New Zealand. The Fiji FIU received an information request from the Criminal Investigation Department of the Fiji Police Force for financial background information on Tallat Rahman, Joshua Aziz Rahman and their associates.

Investigation

The operation was initiated by the National Organized Crime Group of the New Zealand Police Force in establishing links of members of an organized crime group operating in New Zealand. The investigation also involved working with the Fiji Police Force and other law enforcement agencies in the region.

From late 2018 to early 2019, Tallat Rahman was identified as a target member of a criminal enterprise tasked with importing methamphetamine and cocaine and organizing its delivery into New Zealand.

Fiji FIU's preliminary findings identified the following sequence of operations by Tallat Rahman and Joshua Aziz Rahman:

- Tallat Rahman and a local individual shared business ownership with a registered Company D incorporated in 2012.
- Joshua Aziz Rahman sent approximately FJ 61,000 into a local law firm trust account from Canada in between 2014 to 2015. The funds were narrated as Tallat Rahman and Company D.
- Tallat Rahman was the sole owner of a registered Company A, incorporated on November 24, 2017.
- Tallat Rahman received (FJ) 200, 000 into a local law firm trust account from a company in Hong Kong on December 5, 2017. The funds were narrated as in trust for Tallat Rahman.
- Tallat Rahman transferred (FJ) 40,000 from the trust account into Company A on December 21, 2017. The funds were further transferred to an entity in Mexico.
- Company A received a shipment from the entity in Mexico, which contained various homeware items on January 18, 2018. The items were stored at the residential property leased to Tallat Rahman in Suva, where the drugs were discovered.

In December 2018, the father and son came under the radar of the New Zealand Police Force after they were seen delivering a bag of cash to a member of the joint enterprise for what seemed to be the sale of methamphetamine drugs.

On February 8, 2019, Tallat Rahman travelled to New Zealand and was arrested by the New Zealand Police, charged with importing methamphetamine drugs in relation to a consignment delivered to New Zealand from the USA on February 4, 2019.

The next day, Joshua Rahman came under the Fiji Police Joint Transnational Serious Organised Crime Taskforce radar, when he was seen with three targeted individuals who were allegedly involved in transnational drug shipments. This led to the execution of a search warrant for the residential address of Tallat Rahman and Joshua Rahman in Suva, Fiji on February 14, 2019. The Fiji Police Force discovered and seized 39.5 kg of cocaine (average purity of 81%), valued at approximately (FJ) 39.5 million, or equivalent to (USD) 18.3 million. Joshua Aziz Rahman was the sole occupant of the leased property when it was searched.

FIU Action

The Fiji FIU issued a temporary restriction notice on bank accounts associated with Tallat Rahman, Joshua Aziz Rahman and related entities on February 20, 2019.

On February 28, 2019, the Fiji FIU issued a formal information dissemination report to the Fiji Police Force on Tallat Rahman, Joshua Aziz Rahman and their associates. A day later, the Fiji FIU conducted a high-level presentation of their case findings to the Fiji Police Force.

On March 22, 2019, the Fiji FIU issued two follow-up spontaneous case dissemination reports to the Office of the Director of Public Prosecutions and the Fiji Police Force. On the same day, the Fiji FIU conducted a presentation to the Office of the Director of Public Prosecutions regarding the case.

On October 27, 2020, the Director of Public Prosecutions filed a restraining order on the remaining funds: (FJ) 75,101.99 held in the bank account of Tallat Rahman.

Evaluation

On receipt of the information request on February 14, 2019, the Fiji FIU began tactical analysis in tracing the proceeds of crime.

Initial intelligence findings were obtained from the Fiji FIU’s online database and other external databases that the Fiji FIU has access to through memoranda of understanding.

The Fiji FIU sent several information requests to foreign FIUs on Tallat Rahman, Joshua Aziz Rahman and other associated entities and individuals. Information from these FIUs provided key intelligence that helped the Fiji FIU to better understand the syndicate.

Of note:

- Sharing real-time Fiji FIU information to law enforcement agencies during the operation enabled the investigators and prosecutors to identify suspected proceeds of crime in Tallat Rahman’s account.
- The movement of funds into Tallat Rahman’s personal and business accounts in 2017 to 2018 from two major entities in Hong Kong and Mexico established transnational links.
- The restraining order was not sufficient to conclude that the remaining funds were part of the proceeds of crime. The initial funds received from the company in Hong Kong were spent. The financial institutions information established that Tallat Rahman received a cheque deposit of (FJ) 118,118.30 that was from the share of his father’s estate.

Outcome/Contribution

Multilateral investigations—including information sharing between New Zealand Police Force, Fiji Police Force and other local and foreign law enforcement agencies—contributed to the successful prosecution of Tallat Rahman and Joshua Aziz Rahman.

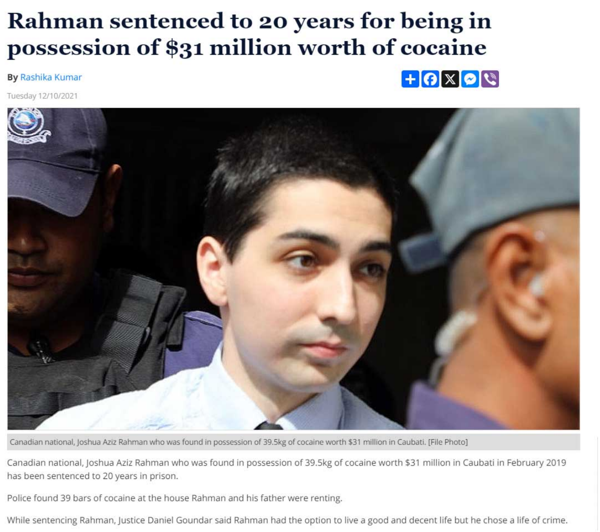
Tallat Rahman was tried before the New Zealand District Court in Auckland on July 6, 2020, and on the same day was sentenced to 16 years of imprisonment for the following offences:

- Importing a Class A controlled Drug contrary to section 6 (1) (a) & 6 (2) (a) of the *Misuse of Drugs Act (1975)*.
- Conspiracy to import a Class A controlled Drug contrary to section 6 (1) (a) & 6 (2A) of the *Misuse of Drugs Act (1975)*.
- Participating in an Organised Criminal Group contrary to section 98A of the *Crimes Act (1961)*.

On April 16, 2021, Joshua Aziz Rahman appeared before the Suva High Court Fiji and was found guilty of joint possession of an illicit drug with his father, Tallat Rahman. On October 12, 2021, he was sentenced to 20 years of imprisonment for unlawful possession of illicit drug contrary to section 5(a) of the *Illicit Drugs Control Act*.

Indicators

- The **creation of shell companies** without any significant operations or business presence but used as means to move funds and facilitate importation.
- The **use of trust accounts** to transfer funds from foreign individuals and entities into Fiji implies a vulnerable corporate arrangement between the client and the firm to legally “gatekeep” alleged proceeds of crime.
- The **transnational links of funds** from entities located in high-profile drug trafficking hub countries, such as Mexico and Canada.
- The **high value of remittance** and rapid movement of funds.



Rahman sentenced to 20 years for being in possession of $31 million worth of cocaine

By Rashika Kumar

Tuesday 12/10/2021

Canadian national, Joshua Aziz Rahman who was found in possession of 39.5kg of cocaine worth $31 million in Caubati. [File Photo]

Canadian national, Joshua Aziz Rahman who was found in possession of 39.5kg of cocaine worth $31 million in Caubati in February 2019 has been sentenced to 20 years in prison.

Police found 39 bars of cocaine at the house Rahman and his father were renting.

While sentencing Rahman, Justice Daniel Goundar said Rahman had the option to live a good and decent life but he chose a life of crime.

Source: Rahman sentenced to 20 years for being in possession of $31 million worth of cocaine (fijivillage.com)

CASE 12

Illicit Drug Trafficking —Peru FIU

Introduction

The FIU Peru's successful investigation of this case led to the dismantling of a criminal organization that had introduced illicit funds into the financial system for the purposes of laundering them. Peru's judiciary validated the freezing of funds prompted by the FIU Peru and ordered preventive detentions for those involved, as requested by the Public Prosecutor's Office.

This criminal organization allegedly dedicated to the sale of olive oil, through three front companies. In a short period of time (approximately 18 months), the company received several wire transfers and a significant amount of money from many countries without commercial reason. The FIU Peru detected that the bank accounts of these three companies were operated from abroad. Additionally, the beneficial owners were being investigated abroad for the crime of drug trafficking.

Investigation

The investigation was initiated following a warning issued by the United States Drug Enforcement Administration (DEA), which informed the FIU Peru of the detection of a criminal organization dedicated to the illicit drug trafficking. This organization operated through the incorporation of front companies—Company A, Company B and Company C—which received numerous wire transfers from abroad. Between April 2019 and December 2020, those companies received 1,317 wire transfers for a total amount of (USD) 100,641,076, and subsequently executed 1,157 wire transfers for a total amount of (USD) 98,256,398. Notably these companies did not engage in international trade activity and reported zero sales or income to the Tax Authority. They primarily conducted domestic transfers within the local financial system. This scheme aimed to evade detection by maintaining an incongruent balance between recorded income and tax information. Companies A, B and C did not engage in any foreign trade activity.

The Peruvian shareholders failed to provide information regarding leasing of offices in an exclusive financial sector of Lima, purportedly for the administration of the group of companies. Furthermore the FIU Peru identified other related companies sharing the same address and shareholders, including individuals from Peru, Colombia and Venezuela.

Individuals from Colombia and Venezuela made multiple entries to Peru on the same date as the wire transfers occurred, and to the countries involved in the inflow and outflow of funds.

The information gathered and analyzed helped in the preparation of a first Financial Intelligence Report, leading to the freezing of approximately (USD) 3,000,000 in funds.

Reporting Entities from the financial sector then submitted new Suspicious Transaction Reports (STRs). This additional information helped the FIU Peru to compile a complementary Financial Intelligence Report: identifying new alerts, new suspects involved, related companies as Company D and Company E, and tracing the entire money flow route.

FIU Action

The FIU Peru engaged in coordinated efforts with various stakeholders within the national money laundering prevention system, including:

- Swift, efficient collaboration with the Public Prosecutor's Office and the Judiciary—paramount in freezing the funds. This enabled the Judiciary to validate the freezing of the funds within 48 hours. Further coordination with the Public Prosecutor's Office helped in the provision of evidence when requested, particularly in cases involving the preventive detention of the individuals implicated in the criminal activities.
- The cooperation of the Reporting Entities (from the financial sector) played a crucial role. They provided information and documentary evidence of transactions, which helped validate suspicions promptly.

Evaluation

The investigation was initiated following a warning from the American DEA, notifying the FIU Peru of the detection of a criminal organization involved in illicit drug trafficking. This organization used front companies (i.e., Company A, Company B and Company C) to conduct numerous wire transfers primarily originating from Hong Kong, North American country 1, North American country 2, and directed abroad, mainly to South American country 1 and Central American country 1. Domestic transfers occurred between these companies within the local financial system. This scheme aimed to conceal the true balance between the recorded income and the tax information. Companies A, B and C did not engage in any foreign trade activities.

The Peruvian shareholders failed to provide economic information regarding the leasing of offices in an exclusive financial sector of Lima, purportedly for the administration of the group of companies. The FIU Peru identified other related companies sharing the same address and shareholders involving Peruvian, Colombian and Venezuelan citizens.

The individuals from Colombia and Venezuela made multiple entries into Peru on the same date as the wire transfers occurred, and to the countries involved in the inflow and outflow of funds.

The information gathered and analyzed enabled the preparation of a first Financial Intelligence Report leading to the freezing of approximately (USD) 3,000,000 in funds.

Subsequently, Reporting Entities from the financial sector submitted new STRs. This additional information allowed the FIU Peru to compile a complementary Financial Intelligence Report with new alerts, new suspects involved, and details of related companies, such as Company D and Company E, and to track the entire money flow route.

Outcome/Contribution

The allegedly illicit funds injected into the financial and economic system by the sponsoring lawyer revealed the utilization of various money laundering typologies:

- Receipt and remittance of transfers from overseas to companies unrelated to the legitimate commercial activity of the three companies.
- Use of accounts belonging to the same company across different financial institutions, which lay dormant for a period of time before suddenly exhibiting significant financial activity without any evident justification.
- Transfers of funds to and from abroad involving recently created companies with diverse economic activities, situated in countries deemed to be high-risk.
- Substantial movement of funds without corresponding declaration of sales and/or income to the tax authorities.
- Receipt and transmission of international transfers without registration of foreign trade activities with customs authorities.
- Overseas management of local accounts to administer funds of illicit origin.

Indicators

- Individuals **established multiple front companies** to inject illicit funds from abroad and from high-risk countries into the Peruvian financial system. These funds—believed to originate from illicit drug trafficking—were laundered within the Peruvian financial system before being sent abroad (primarily to Colombia and Panama) in pursuit of higher returns through investment companies located in those countries.
- **Judicial authorities froze their funds and seized their assets**, totaling (USD) 3,000,000, and ordered preventive detention for those involved. The ongoing judicial proceedings encompass money laundering charges and were expanded to include new individuals implicated in the crimes.
- The **case uncovered money laundering typologies** to conceal the true origin of the illicit funds upon their introduction into the financial system.
- **Companies** A, B, C, D and E (the final two obtained through the FIU's analysis) **failed to register economic information or capital increases** consistent with their operations recorded in the financial system. Their shareholders and/or representatives, often of foreign nationality, also failed to report economic information consistent with the companies' operations and primary business activities. Furthermore, the beneficiaries of the funds abroad in commercial activities were distinct from those of the local companies.
- The **local companies did not engage in any foreign trade activities**. Also, the ordering and beneficiary companies of the transfers had different commercial activities, offering no apparent justification for such transactions.

The restrictive measures taken by the Peruvian Judiciary against the alleged criminal organization (including freezing of funds and preventive detention) underscore the coordination and functioning of the Peruvian money-laundering prevention system. Reporting Entities within the financial system promptly reported suspicious transactions involving the individuals concerned. This helped the FIU Peru determine the destination of the illicit funds and compile a complementary second report.

Fraud & Embezzlement

Each year, individuals and organizations suffer from fraud, resulting in the loss of savings, jobs and investments, and subjecting them to financial and personal hardships. Embezzlement, which is closely associated with fraud, involves the illegal appropriation of public and private assets for personal gain.

This crime leads to an inefficient distribution of goods and services, including the misallocation of life-saving medical supplies, substandard public infrastructure, misused funds intended for those in need, and environmental deterioration. Unlike robberies that involve physical force, fraud is a deliberate act of deception or trickery aimed at acquiring wealth from individuals or companies.

Although it may not involve direct violence, fraud is a form of theft that causes much suffering. The consequences of fraud and embezzlement have resulted in the collapse of bridges and buildings, contaminated drinking water and air, and the unwitting consumption of harmful food and medicine. These crimes have the potential to victimize anyone. Fraud manifests itself in various forms, such as online sales scams, website manipulation, pyramid schemes and other types of schemes involving charities, employment and payroll, identity theft, credit-card and debt-elimination scams, as well as fraudulent contracts and procurement practices. All of these activities yield significant profits at the expense of innocent individuals and organizations.

The global pandemic created a fertile environment for an unprecedented surge in fraudulent activities. As governments worldwide urgently procured personal protective equipment, virus tests, vaccines, and provided financial relief to individuals and businesses, criminals sought to exploit the crisis.

Fraudsters collaborated with corrupt public- and private-sector officials to divert resources meant for pandemic response for their own personal gain. A substantial amount of this misappropriated money entered the global financial system, prompting Financial Intelligence Units (FIUs) worldwide to actively trace these funds and analyze new types of fraud and embezzlement typologies employed in these crimes.

The following examples highlight a range of fraud and embezzlement cases detected by FIUs over the past four years. These cases involve a range of fraud types, including: financial statement fraud, misappropriation of assets, cash skimming and larceny, misuse of company resources, theft of intellectual property and trade secrets, consumer fraud, as well as insurance and procurement fraud. Embezzlement crimes in these cases include the abuse of office for personal gain or the gain of a third party, misappropriation and diversion of public property, and trading in influence.

These cases illustrate the transnational nature of corruption and fraud. They show how criminals quickly transition from one illicit money-making scheme to another, concealing their illicit gains in multiple jurisdictions. Effective collaboration among law enforcement agencies, financial regulators and public-private partnerships is vital in identifying and combating these types of crimes.

By working together, the public and private sectors can assess risks more effectively, detect illicit activities and recover stolen assets—whether they're hidden domestically or abroad.

Indicators

- **Rapid and consecutive money transfers** to another account shortly after deposit.
- **Movement of funds to countries** recognized for opaque financial-sector regulations or high levels of perceived corruption without justification.
- **Difficulty in verifying customer identification details.**
- **Unnecessarily complex corporate ownership** structuring and concealed beneficial ownership.
- **Schemes that promise abnormally high investment returns.**
- **Multiple customers sending international fund transfers** to the same beneficiary abroad.
- **Several international fund transfers sent to the same beneficiary in a single day.**
- **International fund transfers involving substantial amounts of money.**
- **U-turn transactions**, involving the transfer of funds out of a country and then bringing some of those funds back into the same country.
- A series of **low-value international fund transfers**.
- **Transfer of funds to recipients** in countries where they lack a valid economic or financial reason for having a bank account.
- **Transfer of funds to companies** owned by relatives or associates of politically exposed individuals.

CASE 13

Cash withdrawals of approximately (EUR) 37 million in Italy from Hungarian shell companies for the purpose of tax evasion —Italy UIF (Unità di informazione finanziaria), and Hungary’s FIU

Introduction

This case involved repeated cash withdrawals carried out from Italian ATMs with payment cards held by Hungarian shell companies with Italian Business Owners (BOs). Money withdrawn was sent abroad by Italian shell companies, which received funds mostly by active Italian firms. The latter took fiscal advantages from this scheme through false invoices: generating deductible expenses and input VAT to reduce tax burden.

Collaboration between Italian and Hungarian FIUs improved the analysis of Money Laundering (ML) schemes of funds linked to fiscal and other types of crimes that were taking advantage of the misuse of foreign payment cards.

Investigation

This case involved a sophisticated fraudulent tax scheme. It confirmed the versatility of fiscal offences based on false invoicing, which are a particular social concern in Italy.

Expertise was assembled by Italy’s FIU (Unità di informazione finanziaria, or UIF) and Hungary’s FIU (or HFIU). It led to the discovery of a strategy aimed at tax avoidance and to repatriate in Italy those funds sent abroad without adequate taxation.

In the period 2019–2020, UIF received Suspicious Transactions Reports (STRs) concerning anomalous uses of foreign credit cards, involving systematic withdrawals below the threshold of (EUR) 1,000 from ATMs in Northern Italy.

Reporting entities (i.e., the owners of the ATMs) knew the card numbers (PAN) and details regarding the single operation (i.e., data, time, amount, location), but lacked access to information on cardholder identity. The recurrence of withdrawals made with the same cards was considered an element of risk, especially when significant amounts of cash were withdrawn.

Using this information, which was shared by Italian reporting entities, the UIF made an initial analysis of the ATM location used and the frequency of withdrawals. They identified concentrations of ATMs in an area or connections between different cards that were used at the same ATMs, in sequence within a few minutes. The amounts and occurrences of Italian ATM withdrawals, using foreign cards found to be issued by Hungarian financial intermediaries, made it possible to assume the phenomenon was probably linked to a large-scale laundering operation that was exploiting the Italian and Hungarian financial systems.

UIF contacted their Hungarian counterparts to gather more information about the origin of the funds withdrawn in cash, the holders of the payment cards and the related bank accounts. The large number of entities involved forced Italy's FIU to focus the analysis (in collaboration with Hungary's FIU) to a cluster of six Italian enterprises that sent funds to four Hungarian firms.

During the same period, FIU Hungary received a growing number of STRs, in which Hungarian companies were reported for receiving considerable funds from Italian remitters. HFIU shared with UIF many spontaneous communications regarding the described fraudulent scheme and decided to start a strategic analysis on the matter.

The cardholders turned out to be Italian citizens, using funds originated by newly established Hungarian companies, held by Italian beneficial owners and characterized by a very simple corporate governance structure, despite having huge financial turnover. The in-depth analysis performed on these Hungarian company accounts exhibited similar suspicious transaction patterns. These were exclusively credited with wire transfers sent by Italian firms (often connected to the Hungarian companies beneficial owners) from their Italian bank accounts. Hungarian companies did not seem to carry out any legit business activity: appearing to act as shell companies, solely to facilitate monetization of illicit Italian funds. The last part of UIF's analysis focused on the companies ordering the transfers to Hungary. After consulting Italian FIU archives, the analysis of the financial statements and banking operations of the Italian companies involved made it possible to verify cash withdrawals were functional in repatriating funds related to invoices for non-existent transactions.

UIF used network analysis techniques to detect other schemes characterized by the misuse of foreign payment cards. For example: frauds in the trade of Energy Efficiency Certificates, obtained by implementing energy efficiency projects actually never carried out.

Part of these funds were transferred through a system of false invoices to Hungarian bank accounts held by the Italian fraudsters. The funds were then returned to Italy using Italian ATM payment cards linked to the Hungarian bank accounts.

FIU Action

By exploiting new, operational and strategic analysis techniques—and resorting to structured exchanges of information and further bilateral initiatives—the UIF and HFIU identified the illicit scheme in this case.

On Italy's side of the investigation, the UIF identified Hungary as the home country of the financial intermediaries issuing the foreign cards. It did so by examining the first six digits of each card's PAN[1]. To identify the cardholders acting in Italy and the correlated accounts, UIF forwarded various requests to their Hungarian counterparts. The information provided by HFIU and contacting the cards issuers allowed the UIF to identify not only the information requested, but also the origin of the funds transferred (i.e., Italian companies) and the areas in Italy where the withdrawals were made—the highly industrialized Northern regions of the country.

On Hungary's side of the investigation, HFIU shared with UIF many spontaneous disseminations linked to the described fraudulent scheme. These reports disclosed a range of data-based facts, such as: amounts of banking transactions, holders of cards and subsidy accounts and origin of funds. Nevertheless, they did not indicate the PAN of the payment cards, so it was impossible to connect them with the STRs sent by Italian reporting entities. To maximize HFIU disclosures, they were followed by UIF requests for information regarding the PAN codes of all payment cards linked to the accounts spontaneously shared by HFIU. This extensive, bilateral exchange of information was essential to take full advantage of information at the disposal of both FIUs.

[1] The primary account number (PAN) is the card identifier found on payment cards. The card number prefix identifies the issuer of the card, and the digits that follow are used by the issuing entity to identify the cardholder as a customer, which is then associated by the issuing entity with the customer's designated bank accounts.

Evaluation

UIF estimated that in 2019-2020, Italian shell companies sent (EUR) 40 million to the Hungarian companies examined in the investigation. Withdrawals from Italian ATMs equaled (EUR) 37 million.

Strategic analysis conducted by HFIU for the same period highlighted wire transfers from Italian to Hungarian companies of approximately (EUR) 200 million and withdrawals exceeding (EUR) 230 million.

UIF shared with law enforcement the results of its analysis. In early March 2021, it resulted in positive feedback about ongoing penal proceedings against some subjects named in that analysis. Italian law enforcement sent a request to UIF for information to acquire from HFIU further details on certain subjects involved in the scheme.

Furthermore, Italian judicial authorities handed down a jail sentence to a beneficial owner of certain Italian and Hungarian companies. HFIU also shared its analysis with Hungarian law enforcement agencies, which triggered two criminal investigations on suspicion of ML.

Outcome/Contribution

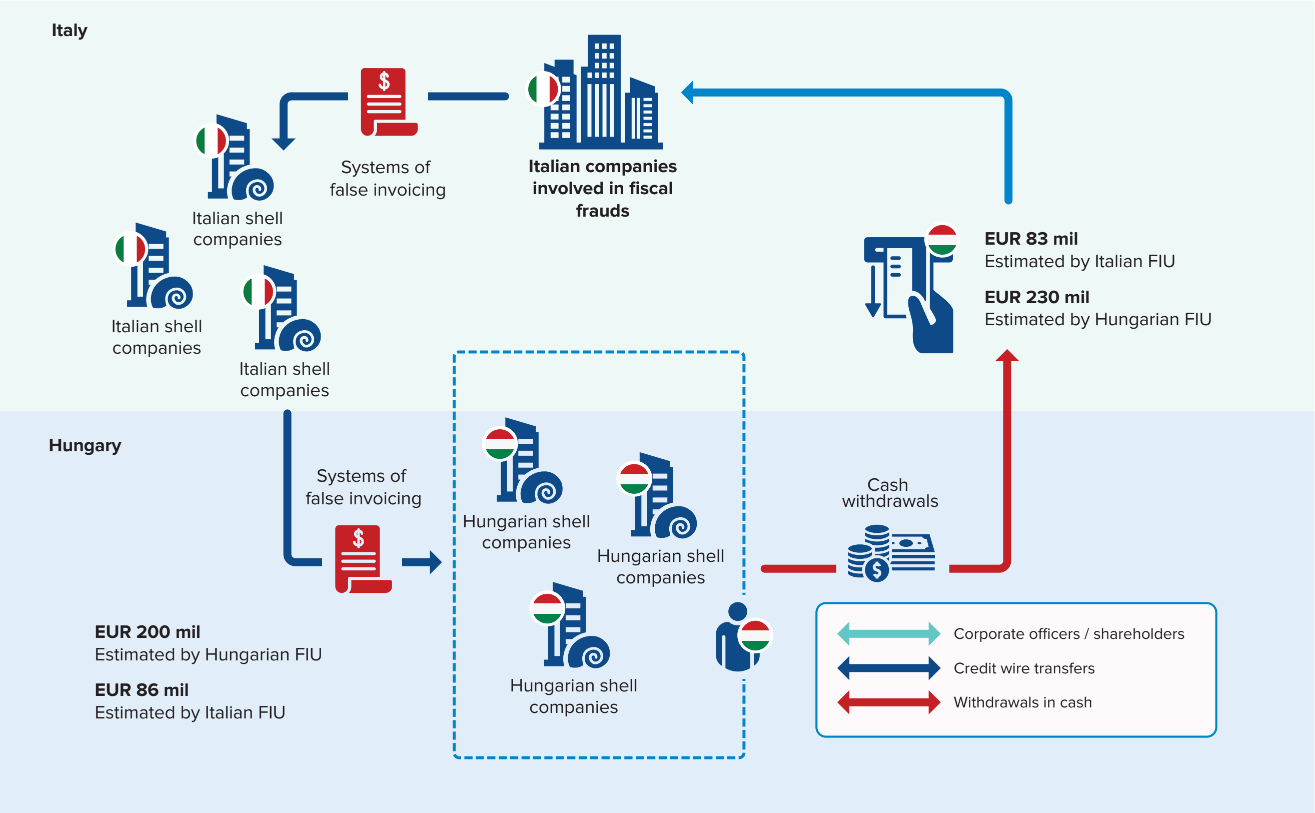
Several criminal cases remain open in both countries concerning tax crimes based on false invoicing and frauds in the energy efficiency certificates market in Italy, as well as money laundering in Hungary.

These types of analyses triggered a debate within both FIUs, leading them to encourage financial intermediaries to carefully monitor potential misuse of foreign payment cards. It also prompted them to further emphasize the importance of cooperation with bar associations responsible for AML (anti-money laundering), as well as supervision of attorneys and other professionals (e.g., accountants, notaries and labour consultants) who also could be involved in organizing illicit schemes.

Indicators

- **Repeated ATM cash withdrawals** for large amounts involving foreign payment cards is a trigger that assumes the presence of underlying illegal activity.
- The **bankcard numbers associated with the foreign bank accounts are vital pieces of information.** Mandatory cooperation is needed between the FIUs involved to identify the network of bank transactions and the active shell companies behind them.
- This case uncovered s**ome of the vulnerabilities in the international anti-money laundering regulatory framework**, especially with regarding the potential role played by the companies managing the payment networks, which possess complete information on the transactions made by cardholders.
- **National and foreign shell companies engaging in the following behaviour patterns**: having been recently established, simple corporate governance structures, lack of updated financial statements, many corporate changes to their offices, officers or shareholders, newly opened bank accounts with incoherent financial turnovers and little accounting data available—all of which is exploited exclusively to move funds unlawfully abroad.
- The **aforementioned techniques of network analysis and pattern recognition** can be exploited to identify suspicious money-laundering activities regarding other types of crimes, because cash withdrawals, shell companies and systems of false invoicing are all methods for disguising and covering-up funds originated by several illegal activities.

Scheme 1: Cash withdrawal scheme from Hungarian shell companies for the purpose of tax evasion.


Italy
Systems of false invoicing
Italian companies involved in fiscal frauds
Italian shell companies
Italian shell companies
Italian shell companies
EUR 83 mil
Estimated by Italian FIU
EUR 230 mil
Estimated by Hungarian FIU
Hungary
Systems of false invoicing
Hungarian shell companies
Hungarian shell companies
Hungarian shell companies
Cash withdrawals
EUR 200 mil
Estimated by Hungarian FIU
EUR 86 mil
Estimated by Italian FIU
Corporate officers / shareholders
Credit wire transfers
Withdrawals in cash

CASE 14

Fraud detected by the use of dummy banking accounts with the same username and password —Taiwan AMLD, Anti-Money Laundering Division

Introduction

Taiwan's FIU (Anti-Money Laundering Division, or AMLD) received Suspicious Transaction Reports (STRs) indicating same or similar red flags related to certain online banking accounts since the end of 2019. AMLD successfully linked these suspicious accounts with criminal activities, such as fraud and online gambling. After analyzing the pattern of the illegal trends, AMLD shared its report with authorities and detected illegal cases from a typology. With the cooperation between private and public sector, the information analyzed and disseminated by AMLD successfully assisted law enforcement in their criminal investigations.

Investigation

Initial Detection—AMLD analyzed STRs from January to December of 2019. The suspicious activity of these STRs is described as follows:

- The account owners set up the same username and password for their online banking service. They also designated the same transfer accounts.
- After completing their setup, a small amount of money was transferred in via an ATM or online banking service as a test to confirm the online banking service and ATM cards were functioning.
- These account owners are not related.

After studying the typology of these dummy accounts, AMLD completed a strategic report and sent it to all relevant authorities. This led to opening two cases.

In the strategic report, the following were indicators of dummy accounts:

- Nearly all owners (over 99%) of these dummy accounts were Taiwanese nationals.
- 60% of the account owners were between ages 21 and 30, and 25% of them were between ages 31 and 40. In the 21 to 30 age group, most had just graduated from school or were new to the employment market.
- Half of the account owners did not have criminal records. The other half had criminal records related to fraud, gambling, narcotics and violent crime.
- 68% of the account owners did not have any record of tax declaration, and 31% of the owners' annual income was under (NTD) 500,000 or approximately USD 33,000.

Usage indicators involving these dummy accounts:

- 62% of these accounts remained dormant, and 38% were active. Once an account was activated, it had a very short life span (between one to six months). During the active period, there would be frequent transactions.
- All active accounts had frequent log-in and transaction activities, and their IP address indicated these activities originated from different geographic locations.
- 80% of the active dummy accounts transferred funds with third-party payment processors.
- Based on the account activity, the potential predicate offense related to these active dummy accounts might include telecom fraud, online gambling, underground banking system and illegal fundraising.

Online Tele Fraud—Mr. C, the director of Company X, used social networking and communications apps to purchase dummy accounts. The account owners followed Company X's instructions to apply for online banking service, and then set up the same username and designated the specific transfer accounts. Mr. C and Company X were involved in a telecom fraud case at the same time. They lured victims to transfer money to these dummy accounts. Company X then withdrew cash from ATMs or transferred it to other accounts held by Company X via online banking services.

Online Gambling—Mr. J established Company W for online gambling. Another subsidiary company provided hardware maintenance, client services, database management to support Company W. Most of the gamblers transferred funds into the dummy accounts held by Company W. From 2016 to 2020, Company W received approximately (NTD) 59.5 billion, approximately (USD) 20 billion in profits. To launder the illegal proceeds, Mr. J established an investment, Company D, to purchase the stocks of public companies worth of (NTD) 700 million. Mr. J also invested in real estate in other countries. According to the law, the seized cash in several accounts had a total value of approximately (NTD) 3 billion. Mr. J and his companies were prosecuted for gambling and money laundering in October 2020. In these two cases, the subjects systematically collected dummy accounts and then used these accounts for themselves or provided them to others to conduct criminal activities.

There are two key elements to success in these cases. First, the financial institutes filed STRs to the FIU immediately when irregularities were detected. Second, there was domestic cooperation with the relevant authorities, including the supervisor of financial institutes and local law enforcement. The FIU—as intermediary between the private and public sectors—would connect the early warning from financial institutes and criminal investigation by law enforcement agencies. That helped all sectors to combat criminal activities more efficiently. AMLD shared its financial intelligence with law enforcement agencies and resulted in detecting these cases.

FIU Action

AMLD found connection among some of the reported dummy accounts, beneficiaries and criminal cases. Those cases were being detected by the law enforcement during the same period, such as illegal online gambling, cyber fraud and underground banking.

AMLD reviewed all STRs with the similar suspicious activity (i.e., different financial accounts with the same username and password for online banking services). There were more than 1,000 dummy accounts and more than 50 designated transfer accounts involved in this analysis.

According to account owners' statements, some saw online advertisement for business opportunity or for recruiting. Some sold their bank accounts to unknown criminal groups or gangs via social media or other communication apps. They all followed instructions issued by unspecific persons: to apply for activating an online banking service and to reset the username and password of the account. Then they handed out their accounts, including the account book and ATM card, to certain individuals. These circumstances indicated certain persons or groups collected dummy accounts intentionally.

After tracing the flow of funds in these dummy accounts—combined with background analysis including criminal history, career, tax records and CTR—AMLD discovered some of these dummy accounts were highly relevant to criminal activities. They pertained to engaging in online gambling, fraud and the underground banking system—all under investigation by local law enforcement in Taiwan. It seemed that these crime syndicates used these accounts to conceal, convert and transfer their illegal proceeds.

Recognizing that the dummy accounts could compromise Taiwan's financial stability, AMLD shared its findings in December 2019 with the country's Financial Supervisory Commission (FSC). The FSC forwarded the information to all financial institutes immediately and also demanded all financial institutes to pay attention to the suspicious activities and take commensurate measures to mitigate ML/TF risks. After receiving these notifications, the financial institutes fully reviewed their customer data and reported any suspicious activity to AMLD immediately. Enhanced due diligence procedure was performed on clients with high ML risks. Some accounts were subsequently closed.

Evaluation

Starting from noting unusual accounts (which were revealed as dummy accounts) and gathering STRs to analyze the criminal pattern, AMLD uncovered a series of red flags. These were shared in their report to relevant authorities, who then detected several illegal transactions. After disseminating their information to law enforcement, the related STRs were analyzed by AMLD. These findings were disseminated to law enforcement. With the early warning of the symbols and the help of private and public sectors, law enforcement agencies solved the case and seized the illegal proceeds.

Outcome/Contribution

Online banking services provide low-cost convenience, privacy and fast responses. They are also accompanied by ML risks and uncertainty. These advantages can prevent criminals from being detected by law enforcement, leading to new types of crime. AMLD recognized these threats and vulnerabilities and shared its analysis results with relevant authorities. As a result, this early warning captured law enforcement's attention, detecting tele fraud and online gambling, involving a sum of more than (USD) 20 billion. It is also a good example of cooperation within banking entities, FIU and supervisory agencies.

Indicators

- **Analyzing and detecting New Trends and Types of illegal crimes,** which lead to major cases from STRs.
- **FIU shared information and strategy reports** with relevant authorities.
- **Cooperation between private sector** (e.g., bank, law enforcement and supervisors), leading to an efficient criminal-investigation environment.

CASE 15

Criminals used shared construction companies to steal money from victim —Bahrain Financial Intelligence Department (FID)

Introduction

In 2022, Bahrain's FIU (Financial Intelligence Department or FID) discovered a case that would launch a full parallel investigation alongside public prosecution and law enforcement in that country. The case involved three parties: Person A (Victim), Person B (Perpetrator 1) and Person C (Perpetrator 2). The case highlights the lengths that the perpetrators were willing to go to in engaging in fraud and in their subsequent attempts to launder their illicit profits.

Evaluation

In 2019, Person A held a meeting with Person B to discuss opening a new construction company. Both parties agreed to pursue the matter. The following day, both individuals went to the Ministry of Industry, Commerce and Tourism to open up a new commercial registration and establish their new project (i.e., the previously agreed upon construction company). They signed documents stating that Person A owned 50% of the shares and Person B owned the other 50% of the shares, with a capital amount of (BD) 250,000. Next, these individuals went to the bank to open a bank account for the company and deposited the capital amount to start their project. Person A deposited a total amount of (BD) 200,000. Person B deposited the amount of (BD) 50,000, and borrowed (BD) 75,000 BD from Person A, which was deposited into the account with his capital amount.

Person B then proposed running the company while Person A would receive his profits annually. Person A would agree to this idea verbally without signing any documents to reflect this agreement. Person B went on running the company until the whole capital amount was transferred into Person B's account, and Person A became a victim of Fraud. Person B was charged with fraud and sentenced to five years in prison. Acknowledging he committed a crime, Person B evaded local authorities to avoid arrest as he laundered and circulated the entire capital amount into many different bank accounts to hide its source and attempt to legitimize it.

Person B (Perpetrator 1) was charged with fraud and ordered by the court to return the amount back to Person A (the Victim). At this point, it became apparent that cited amount was no longer in Person B's bank account and had been laundered. These events led to Bahrain's FID to launch a parallel investigation with public prosecution and law enforcement.

The FID began legal proceedings: to obtain a warrant to gain access to all information concerning the assets of the perpetrators. Permission was granted by authorities for the FID to access and place a freeze order on all assets and bank accounts. After analyzing all the information at hand, it was clear Person B had transferred the whole amount of the stolen capital—(BD) 250,000—to his personal account and was transferred to a then-unknown individual's account.

Through gathering additional intelligence, careful analysis and filing subpoenas to uncover identities, the unknown individual in question was revealed to be a friend of Person B. They became a suspect in the case, and labelled as Person C (Perpetrator 2). It was then clear that Person C was an accomplice of Person B, and that money laundering had taken place.

After completing and examining the analysis report, it became clear there was actually an amount of (BD) 250,000 in Person C's account. It was transferred from Person B's account. Person C opened up a document-clearing office and used this amount as the capital amount for his new company. That company would work in the clerical field of clearing documents and help new investors in opening new commercial registrations. Person C would then launder and legitimize that money by using it to open new commercial registrations and loaning people an amount of (BD) 50,000 as the capital amount for their new company. This allowed them to deposit it in their company's account to ease the process of opening up a new commercial registration.

When the commercial registration was opened successfully, the amount was then debited and transferred back to Person C's office account. Person C continued circulating the amount in this particular field many times: loaning new investors the capital amount of (BD) 50,000. When the amount was returned to Person C's office account, it would be transferred back to Person B's account. Person C would also charge (BD) 300 for every commercial registration clearance service and then transfer the amount in different segments to Person B until he managed to receive the whole amount back in a seemingly legitimate way. Person C took his profit during the circulation process by being an accomplice.

After looking into the report, the case became clear. Bahrain FID contacted Person C's clients, whom Person C helped in opening up new commercial registrations.

After all the clients reported to the FID, it showed that Person C knew these individuals were looking to open up new business, so he went on offering them the capital amount: returning it once the Commercial Registration was opened and completed and only paying Person C (BD) 300 for his services (based on given statements). All of the gathered intelligence was then sent to the public prosecution to provide the FID with an arrest warrant for both Person B and Person C.

Three days after the warrant was issued, Person C was the first person arrested. While asking him about Person B, he informed that Person B was hiding at a farm, far from their location. Authorities went to that location and found Person B, who was subsequently arrested and charged with fraud and is now suspected of having engaged in money laundering.

Outcome/Contribution

As a result of the investigation's findings, the perpetrators were arrested referred to Public Prosecution to complete all legal procedures before referring the case to court.

The investigation accentuated the need for a heightened awareness campaign (subsequently implemented) on the dangers of fraud and that precautions should be taken to prevent more of these kinds of incidents from occurring.

CASE 16 Money stolen with the use of shell companies —South Africa Financial Intelligence Centre (FIC)

Introduction

Swift, effective work between the South Africa's FIU (Financial Intelligence Centre, or FIC) and domestic/ foreign law enforcement helped track and trace public funds stolen from the Kingdom of Lesotho and repatriated to South Africa. Most of the proceeds were returned. Nine accused, including seven officials, that face charges of fraud and money laundering.

Investigation

Rooted in Lesotho and branching out into South Africa, this case highlights the effectiveness and responsiveness of domestic and foreign authorities working collaboratively and persistently in fighting money laundering.

The crime originated in Lesotho, where government officials diverted public funds intended for suppliers into bank accounts of shell companies registered in South Africa.

An investigation by the Lesotho Mounted Police Service and the Lesotho Directorate of Corruption and Economic Offences (DCEO) uncovered a scheme by government officials to defraud the Lesotho government. The investigation revealed that government officials had siphoned about (ZAR) 50 million from state coffers.

The Lesotho Mounted Police Service investigation revealed fraudulent payment instructions had been approved by the Lesotho government and effected by the Lesotho Central Bank, believing the instruction to move the money was legitimate.

More than (ZAR) 38 million of the (ZAR) 50 million had been transferred to South African bank accounts held in the names of shell companies registered in Lesotho's neighbouring country.

The FIC South Africa, Lesotho's FIU, the Lesotho Mounted Police Service and its Directorate of Corruption and Economic Offences, as well as South Africa's Asset Forfeiture Unit (AFU) all demonstrated exceptional cooperation, collaboration and responsiveness in working on this case to address theft, fraud and money laundering.

Despite its complexity, collaboration between these agencies led to a remarkable recovery rate of the proceeds of crime. It demonstrated that the South African team of the FIC and law enforcement were capable and effective, even under extreme duress. Overall, prompt action by law enforcement, the FIC, Lesotho's FIU and the banks involved in this case resulted in the successful recovery of funds.

The first tranche of funds was preserved less than a month after the FIC received a transnational request for information from its counterpart, the Lesotho FIU.

The FIC issued directives on bank accounts temporarily securing material positive balances. Responsiveness of the banks to enquiries and requests from the FIC assisted with the recovery of material positive balances in numerous bank accounts. This helped ensure the funds were not dispersed while the AFU was following legal proceedings to preserve the funds.

Lesotho authorities arrested and charged nine suspects—including seven government officials—for theft, fraud and money laundering. Amounts of (ZAR) 23.7 million and a fixed property purchased for (ZAR) 2.34 million were preserved. Eleven motor vehicles were also confiscated.

FIU Action

The FIC compiled a financial flow analysis, revealing that the suspects had transferred more than (ZAR) 38 million from the Lesotho government to three South African bank accounts held in the names of shell companies registered in the country. This was the outcome of a request from Lesotho FIU.

The FIC's analysts used open- and closed-source searches to profile the suspects and examined data on transfers of funds internationally.

Analysis of the shell companies and related transactional activities revealed that little financial activity had taken place in these bank accounts prior to the deposit of the proceeds. The FIC subsequently issued enquiries to the banks, to obtain as much detail as possible on the related accounts: including bank account information, account balances, copies of bank statements and know-your-client (KYC) documentation.

The FIC followed up with directives to freeze the accounts. According to FIC regulations, accounts may be frozen for ten business days. This allowed time for the FIC to prepare and submit an urgent ex-parte preservation application, which ensures funds are not dissipated during the preparation process of preservation applications.

A financial flow chart was created to help visualize and identify links between subjects and other bank accounts.

The FIC received requests for information from the AFU and Lesotho FIU, and initiated its analysis with a focus on the subjects and bank account numbers provided in the requests for information.

A search was conducted on the FIC's registration and reporting system to verify whether any regulatory reports had been submitted in the past, containing these bank account numbers. Had this been found, the next step would have been to obtain statements from the relevant banks via regulations in the *FIC Act*. However, as no regulatory reports were found regarding these bank accounts, the FIC issued queries to the banks to obtain as much information as possible on the account holders, such as bank account information, account balances, copies of bank statements and KYC documentation.

Queries to the banks and the FIC's further analysis determined the shell companies were newly registered and that the bank accounts were also new. The bank accounts related to the shell companies had been dormant before the large money transfers via Lesotho. Furthermore, the identified banks had not filed any regulatory reports on the accounts with the FIC.

The FIC issued 51 enquiries to the identified banks after receiving affidavits from the AFU in South Africa and the Lesotho government. All the banks responded within one to two business days, providing account balances, KYC documents, bank statements and contra account details.

Through analysis, the FIC ascertained the positive balances in the bank accounts were the proceeds of the crime under investigation. During analysis, due consideration was given to possible co-mingling of funds, as well as the balance of the account before the proceeds of crime were received.

The funds were traced further, establishing to whom the funds were transferred, by analyzing contra account details. Transaction descriptions were considered, and analysis confirmed the payment with contra account details. For example, a transaction description could include the make and model of a motor vehicle.

However, it was not assumed that a motor vehicle was purchased, but that was confirmed with contra account details. Again, the financial flow chart assisted in visualizing and identifying links between subjects and other bank accounts and transactions.

Analysis revealed that various properties were purchased. The AFU obtained affidavits from the relevant conveyancers. Funds were received into their trust accounts for the purchase of properties. The funds were transferred to third-party administration accounts specifically opened for the purpose of facilitating the purchase of the properties. Registration for some of the properties was incomplete and the balances in accounts could be secured without affecting the businesses of the conveyancers. The FIC secured the interest of the proceeds of crime generated in the third-party administration accounts.

Directives were issued to the relevant banks to secure funds in accounts with material balances. The funds were temporarily secured for ten business days. The AFU was able to prepare and submit an ex-parte preservation application during the period. Time was of the essence to trace as much of the funds as possible in a short period for inclusion in the preservation application, while ensuring the directives did not lapse before the preservation order was obtained.

Timely reports were disseminated to the AFU and the Lesotho FIU on funds secured via FIC directives and other implicated accounts.

The FIC filed affidavits in support of a successful AFU preservation order application in terms of the *Prevention of Organised Crime Act* brought before the Free State High Court in South Africa. The process will be repeated, should further material positive bank account balances be identified.

During the analysis process, the FIC ensured regular contact was maintained and exchanged with:

- The **investigating officer**, to ensure an exchange of information on the progress of the investigation and the financial analysis.
- The **banks**, ensuring correct information and/or documents were completed and received in a timely manner.
- **Conveyancers**, in which analysis indicated that subjects purchased immovable properties. It was established that the conveyancers were not subjects (i.e., assisting with money laundering) and could be approached as accountable institutions.

The case developed as the FIC conducted transactional analysis, revealing the flow of funds. The findings of the FIC's analysis were provided to the AFU and the Lesotho FIU as the information became available. The AFU and the Lesotho FIU then acted on the findings to ensure the funds were preserved or traced further.

The FIC further contributed by:

- Identifying involved persons and entities (subjects).
- Profiling subjects.
- Tracing funds and assets.
- Transactional analysis revealing the flow of funds.
- Identifying suspects benefiting from the stolen funds.
- Identifying entities and bank accounts used to launder the funds.
- Identifying movable and immovable assets.

Regulations in the *FIC Act* allow the FIC to freeze the proceeds of crime for ten business days. This period allowed time for the AFU to prepare and submit an urgent ex-parte preservation application. This ensured the funds were not dispersed by the suspects during the preparation process of the preservation application.

Evaluation

The Lesotho government detected fraudulent payment instructions during their bank statement reconciliation processes. Officials from the Lesotho treasury allegedly forged payment instructions to the Central Bank of Lesotho. The Lesotho FIU subsequently submitted requests for information to the FIC once it was discovered the funds had been transferred to bank accounts of front companies registered in South Africa.

Outcome/Contribution

Lesotho authorities arrested and charged nine suspects, including seven government officials, for **THEFT**, **FRAUD** and **MONEY LAUNDERING**. Eight of the nine suspects were granted bail. One of the eight died after being released. The main suspects are still under arrest and have not yet been convicted.

Amounts of (ZAR) 23.7 million and a fixed property purchased for (ZAR) 2.34 million were preserved, and 11 motor vehicles were confiscated. More that (ZAR) 38 million was laundered from Lesotho to South Africa. The AFU is awaiting conclusion of the forfeiture process.

Through further analysis of bank statements, the FIC established the flow of proceeds of crime from Lesotho to South African banks. Furthermore, it traced other assets. The FIC's ability to secure funds for a period of ten business days contributed extensively to the successful preservation of more than (ZAR) 23 million in proceeds of crime.

5

Trade-Based & Third-Party Money Laundering

Trade-based and third-party Money Laundering (ML) involves disguising proceeds of criminal activities as payments for imports/exports or other transactions to facilitate the illegal transfer of illicit funds. It is the most common type of money laundering globally. Schemes are often carried out by professional money launders with specialized knowledge, using a variety of methods to mitigate risk.

Due to their complicated, interconnected nature, supply chains around the world are used by organized crime, professional money launderers and terrorism financing (TF) networks to engage in a range of activities, including: laundering proceeds of criminal activities (e.g., drug trafficking), financing terrorism and circumventing sanctions. Many customs, law enforcement, financial intelligence units (FIUs), tax and other authorities find it more difficult to detect and fight trade-related money laundering compared to other activities. Even the most knowledgeable authorities are hindered by the complexity and ever-changing techniques used in this area.

FIUs are responsible for strategic analysis of their databases to detect ML/TF typology and emerging trends, as well as ongoing independent operative analyses to track suspicious targets. FIUs notify authorities of illicit activities detected by their analyses. The cases presented in this section illustrate techniques used by a range of individuals involved directly or indirectly in trade-based and third-party money laundering activities.

CASE 17

Cleaning out the laundromat: breaking the biggest structural money laundering mechanism —Latvia FID (Finanšu izlūkošanas Dienests)

Introduction

This case involved the investigative efforts of Latvia's FIU (Finanšu izlūkošanas Dienests, or FID). In early 2018, Country A published a notice of proposed rulemaking against Bank A, based on findings that it was a bank suspected of engaging in money laundering. Later that year, Bank A initiated voluntary liquidation procedures. Its license was soon revoked. At that time, (EUR) 2.4 billion were still to be paid out to the bank's creditors.

The Latvian authority, Latvijas Banka, approved the liquidation, requiring a thorough assessment of each creditor and their source of funds. As the Latvian FIU began assessing the bank's transactions and clients, it became evident that Bank A systematically engaged in money laundering offenses, and laundered millions of Euros through the Latvian financial system.

This case showcased the successful handling of a professional money laundering case so complex it required the establishment of unprecedented domestic and international financial intelligence exchange mechanisms, involving FIUs from 25 jurisdictions. The outcomes of this case elevated the Latvian FIU into a leadership role among this project.

Investigation

Between 2013 to 2018, over (EUR) 300 billion were transferred through Bank A. These funds went to dozens of different jurisdictions linked to money laundering schemes facilitated by Bank A. Latvia's FIU received access to all transactions made by Bank A customers from that period, as well as a list of IP addresses of transaction parties, and KYC ("know your customer") data. Through international and domestic cooperation, Latvia's FIU processed and analyzed the largest amount of financial intelligence data ever connected to a single case.

Initial analysis of creditors revealed a variety of money laundering typologies (see Scheme 2 and Scheme 3):

- Large sums of funds received in Bank A originated from foreign accounts held by non-resident legal entities, which were part of laundering schemes.
- Transactions made between the bank's non-resident customers showed signs of transit operations having no economic purpose.
- A large number of the bank's customers were considered to be shell companies with declared non-resident Ultimate Beneficial Owners (UBOs).

The case created a significant public-private partnership: the Cooperation Coordination Group (CCG). This was a new framework for exchanging financial intelligence in operational and strategic matters with law enforcement, private partners and other stakeholders in an ad-hoc format. Over 100 meetings were held.

A novel multilateral cooperation forum was also established as a result of this case: the International Financial Intelligence Taskforce (IFIT). It consisted of FIUs from 25 jurisdictions working together to exchange financial intelligence related to Bank A. The support received from the foreign partners was essential for FIU Latvia to assess and freeze funds and to advance the case with local law enforcement. Within the IFIT, participants developed a shared understanding of the issues related to Bank A, bolstering coordinated action across borders. The IFIT was a safe forum for FIUs to share concerns and increase awareness of operational and strategic analysis being done. It was also used to exchange priorities, typologies and methodologies.

FIU Action

- FIU Latvia requested and received access to Bank A's database, consisting of all transactions from January 2013 to June 2018. To collect, structure and analyze this information, a data room was created using customized software (i.e., new tools created to process large data sets in a structured, searchable format). The data room contained details on every historical transaction that the bank's customers made during the five-year review period.
- FIU Latvia obtained consolidated KYC information on every customer. This consisted of main attributes relevant to identifying customers (e.g., identity information, residence/legal address, account information, information on declared UBOs). The IP address list of every transaction made during this five-year period was also included.
- FIU Latvia began disseminating and exchanging financial intelligence with the other jurisdictionally involved FIUs to gather operational information and to complete their analysis on suspicious transactions and Bank A customers.
- FIU Latvia organized meetings with members of the Latvian State Police and Prosecution Office to discuss draft analysis on the most complicated ML schemes in Bank A. This was soon formalized with the unprecedented formation of IFIT and the CCG. Regular meetings were organized with liquidators of Bank A, creating a shared plan for analyzing the clients, exchanging information and sharing large data sets of client information, thus reducing the time and resources needed for information exchange on an analytical level.
- Experts were involved from different backgrounds and institutions in an early phase of the investigation, helping set goals for future actions.
- Legal entities were identified that were being used by the employees of Bank A to process the fees related to a legalization scheme (i.e., disguised as payments for legal service or donations to charity by Bank A). These profits were then moved from the legalization scheme over to other entities, obscuring the connections between Bank A, its employees and its customers.
- International cooperation on institutional and analytical levels involved exchanging information on large data sets, as well as in individual cases by using the Electronic Single Window (ESW) channels. This helped form a wider perspective on Bank A clients and their role in these legalization schemes.
- A new information exchange method was established. It was used when cooperating with Latvian law enforcement (i.e., information on transactions was processed and compiled). Thus, law enforcement carried out faster procedural actions, thanks to documentation that permitted its use in court.
- FIU Latvia continued to support the investigation even after sending the case to law enforcement. It did so by providing analytical support to police as well as the Prosecution's Office.

Evaluation

Initial detection of crimes in this case was announced by Country A. It indicated the involvement of Bank A in facilitating ML schemes, obstructing regulatory enforcement, and in conducting activity linked to North Korea. Within ten days of the announcement, the European Central Bank (ECB) announced that the bank and its subsidiaries were failing—or were likely to. The Latvian financial supervisory authority allowed Bank A to undergo self-liquidation, with the ECB removing its license. To ensure strict oversight of the bank's self-liquidation, FIU Latvia evaluated and contributed to developing the methodology for the liquidation procedure in line with anti-money laundering (AML) rules.

The liquidation methodology required each creditor to be assessed for their source of funds. To ensure FIU Latvia's capacity to conduct the investigation into creditors during the liquidation, it requested—and was provided—full access to all historical transactions made by Bank A customers from 2013 to 2018, as well as a list of transaction party IP addresses and full KYC data.

Initial analysis of creditors revealed a variety of ML typologies. Large sums of funds received in Bank A originated from foreign accounts held by non-resident legal entities, which were considered to be part of publicly known worldwide laundromat schemes (e.g., the "Russian Laundromat" or "Azerbaijani Laundromat"). Transactions made between the bank's non-resident customers showed signs of transit operations with no economic purpose. A large number of the bank's customers were considered to be shell companies with declared non-resident UBOs. These were but a few of the red flags that quickly led to the conclusion Bank A was involved in institutionalized ML.

During the initial analysis, the complexity of the Bank A case became apparent. The typologies discovered were significantly beyond the usual ones seen in such cases. The role of Bank A in this case entailed long-term, systematic behaviour.

Two different working groups were created, whose preliminary analysis indicated:

- Bank A had failed to comply with requirements of the Latvian AML law by providing financial services to high-risk clients with signs of being shell companies. These were generally used to transfer funds from Commonwealth of Independent States (CIS) to credit institutions in other countries, disguising their true source.
- The services offered by Bank A to their clients allegedly included the establishment of shell companies, thus placing Bank A under suspicion of being a willful participant in legalization schemes.

Analysis of historical Bank A customer transaction data produced many important insights. FIU Latvia traced almost 30 jurisdictions that had significant transactions with Bank A from 2013 to 2018. FIUs of those jurisdictions were invited to participate in a specialized taskforce within the framework of the Bank A case: an ad hoc IFIT, which served as a practical platform for financial intelligence sharing. A total of 25 FIUs from around the globe participated in the IFIT, led by FIU Latvia. Its purpose was to jointly analyze money flows to and from Bank A, and to examine the former customers of the bank so as to prevent pay-outs of illegitimate funds to the bank's creditors, as well as to detect perpetrators and movement of criminal funds abroad.

Outcome/Contribution

There is an ongoing criminal process against Bank A for suspicion of professional money laundering.

Thanks to close cooperation among 25 FIUs under the leadership of the Latvian FIU between 2018 and 2023:

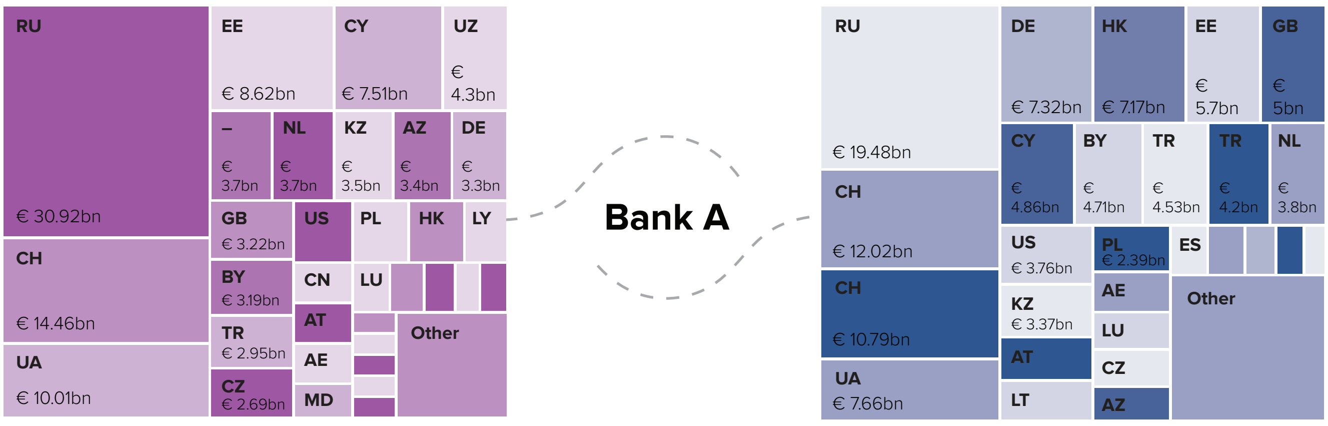
- Dissemination of 1021 reports to law enforcement agencies.
- Freezing of at least (EUR) 1.18 billion in funds.
- Initiation of over 581 criminal proceedings in Latvia, and 316 reports added to already-initiated criminal proceedings.
- Confiscation of at least (EUR) 179 million in funds.
- Seizure of at least (EUR) 1.16 billion in funds (without real estate, financial instruments or other assets).

The case triggered significant reforms of Latvia's financial sector. The country became the first to comply fully with all the standards set by the Financial Action Task Force (FATF) on Money Laundering. Across IFIT members, changes included: amendments to the national AML/CFT legislation, increased analytical staff and expanded access to databases, improved guidelines and training for reporting entities to better identify suspicious transaction patterns, creation of novel IFIT and PPP cooperation frameworks, and closer international and local collaborations.

Indicators

- **A large number of the bank's customers were considered to be shell companies** with declared non-resident UBOs.
- **Large sums of funds received** in Bank A originated from foreign accounts held by non-resident legal entities, which were part of laundromat schemes.
- **Both incoming and outgoing payments** within Bank A **contained generic references to contracts**, invoices and acquisition of various types of goods often not within the stated business purpose of entities moving the funds.
- **Transactions made between** the bank's non-resident customers showed signs of transit operations with no economic purpose.
- **Money was used for acquisition of assets** (e.g., properties, yachts, jewellery, art) and lifestyle payments (e.g., school fees, holidays, legal fees).

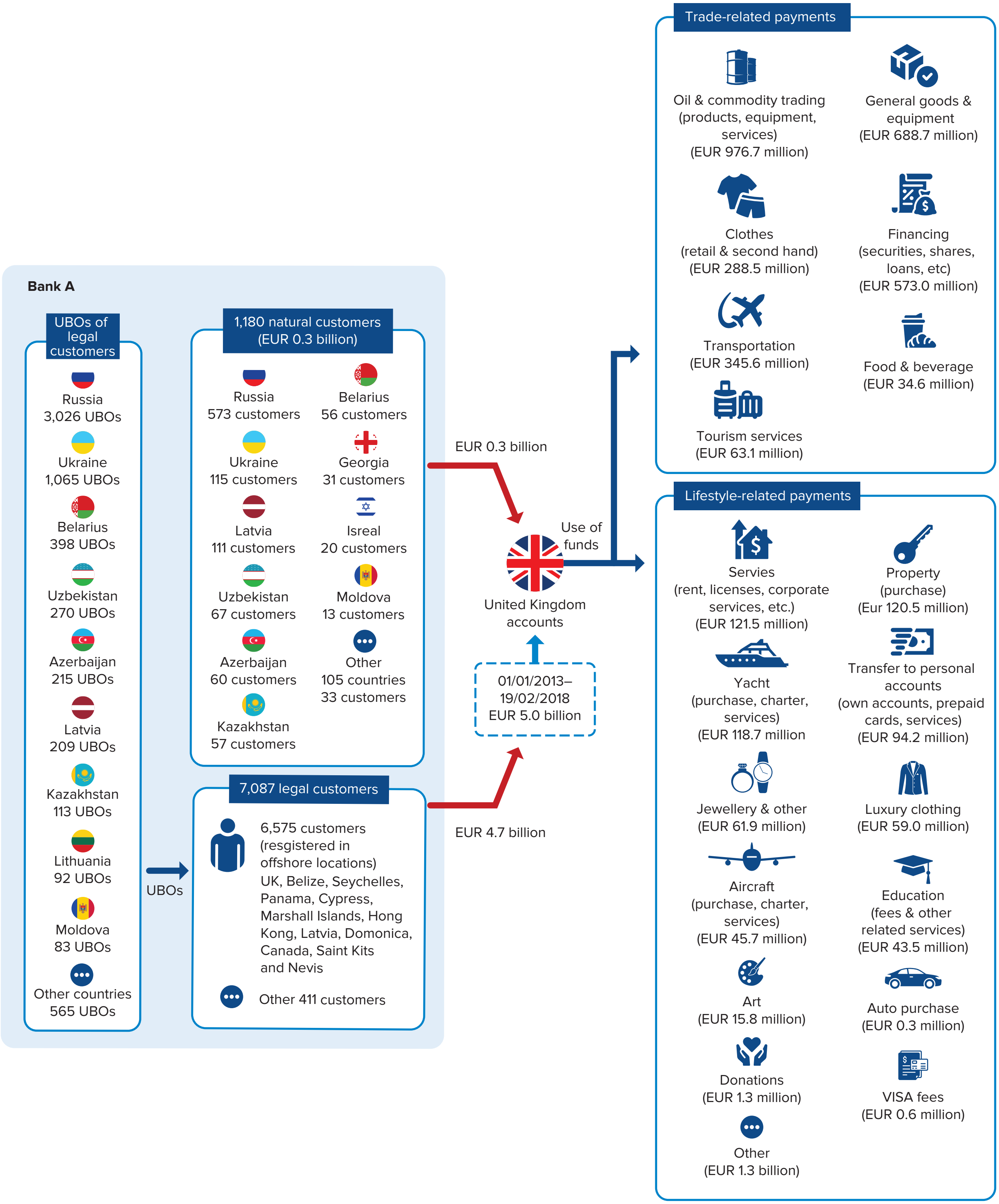
Scheme 1: Transactional data analysis of Bank A as a conduit (2013–2018).



INCOMING – (EUR) 161.5 BILLION

OUTGOING – (EUR) 160.2 BILLION

Scheme 2: Complex layering using the accounts of Bank A.



Bank A

UBOs of legal customers

Russia
3,026 UBOs

Ukraine
1,065 UBOs

Belarius
398 UBOs

Uzbekistan
270 UBOs

Azerbaijan
215 UBOs

Latvia
209 UBOs

Kazakhstan
113 UBOs

Lithuania
92 UBOs

Moldova
83 UBOs

Other countries
565 UBOs

UBOs

1,180 natural customers
(EUR 0.3 billion)

Russia
573 customers

Belarius
56 customers

Ukraine
115 customers

Georgia
31 customers

Latvia
111 customers

Isreal
20 customers

Uzbekistan
67 customers

Moldova
13 customers

Azerbaijan
60 customers

Other
105 countries
33 customers

Kazakhstan
57 customers

7,087 legal customers

6,575 customers
(resgistered in
offshore locations)
UK, Belize, Seychelles,
Panama, Cypress,
Marshall Islands, Hong
Kong, Latvia, Domonica,
Canada, Saint Kits
and Nevis

Other 411 customers

EUR 0.3 billion

EUR 4.7 billion

United Kingdom
accounts

01/01/2013–
19/02/2018
EUR 5.0 billion

Use of
funds

Trade-related payments

Oil & commodity trading
(products, equipment,
services)
(EUR 976.7 million)

General goods &
equipment
(EUR 688.7 million)

Clothes
(retail & second hand)
(EUR 288.5 million)

Financing
(securities, shares,
loans, etc)
(EUR 573.0 million)

Transportation
(EUR 345.6 million)

Food & beverage
(EUR 34.6 million)

Tourism services
(EUR 63.1 million)

Lifestyle-related payments

Servies
(rent, licenses, corporate
services, etc.)
(EUR 121.5 million)

Property
(purchase)
(Eur 120.5 million)

Yacht
(purchase, charter,
services)
(EUR 118.7 million

Transfer to personal
accounts
(own accounts, prepaid
cards, services)
(EUR 94.2 million)

Jewellery & other
(EUR 61.9 million)

Luxury clothing
(EUR 59.0 million)

Aircraft
(purchase, charter,
services)
(EUR 45.7 million)

Education
(fees & other
related services)
(EUR 43.5 million)

Art
(EUR 15.8 million)

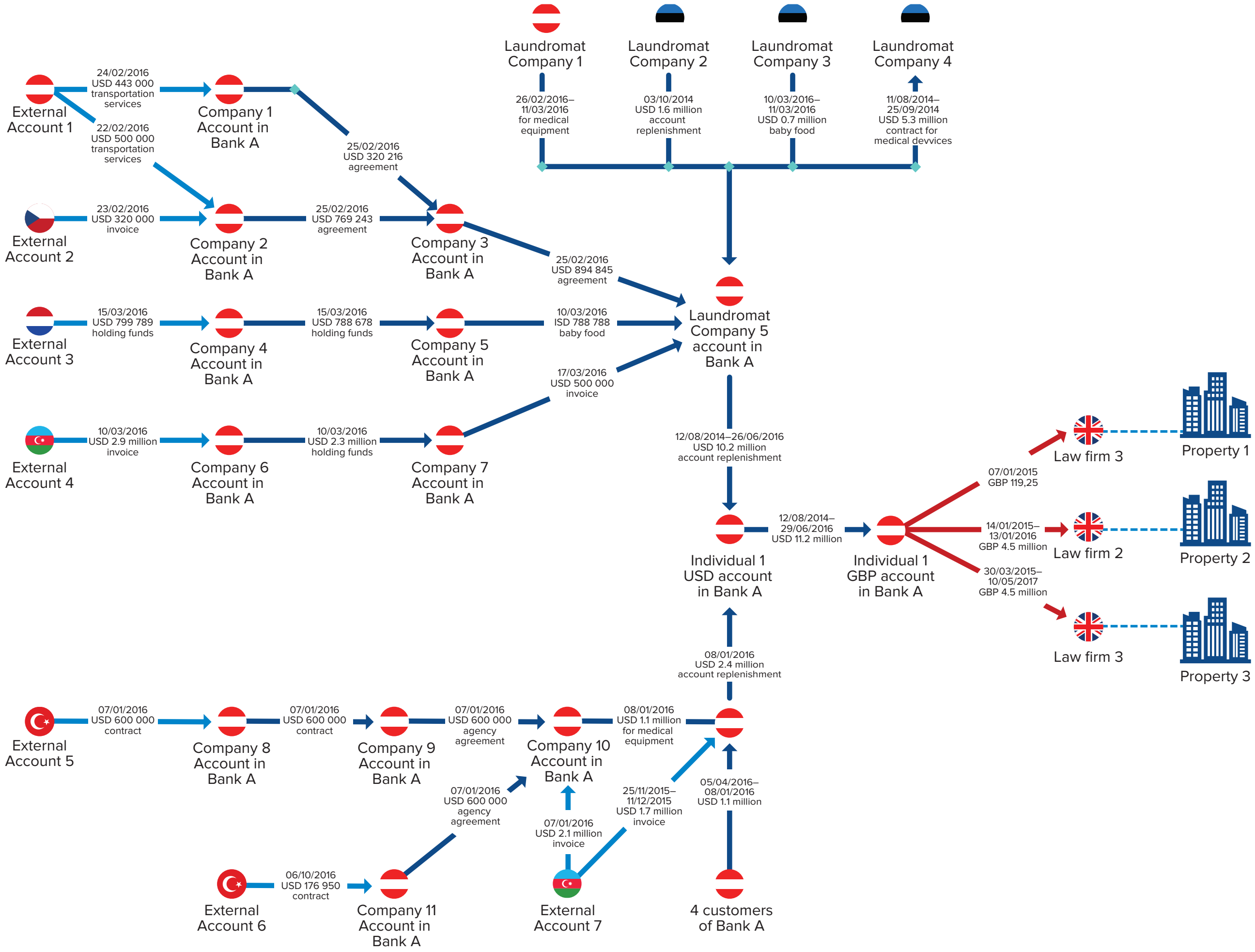
Auto purchase
(EUR 0.3 million)

Donations
(EUR 1.3 million)

VISA fees
(EUR 0.6 million)

Other
(EUR 1.3 billion)

Scheme 3: Bank A as a channel to integration countries.



CASE 18

Stolen car, Stolen money —Senegal CENTIF (Cellule nationale de Traitement des Informations financières)

Introduction

This case involved OMEGA, an individual who owned a car dealership specializing in importing used vehicles. An investigation by Senegal's FIU (Cellule nationale de Traitement des Informations financières, or CENTIF) and law enforcement—prompted initially by newspaper reports—revealed that this individual, along with other Senegalese nationals residing in Europe, were facilitating the trafficking of stolen vehicles and motorcycles across Europe.

Investigation

In 2021, the Senegalese FIU received information concerning an individual identified as OMEGA, who owned a car dealership specializing in importing used vehicles. The individual held two separate company accounts with Bank 1 and Bank 2. These operated smoothly without any incidents or anomalies.

However, newspapers reports alleged OMEGA's involvement in an international trafficking operation of stolen vehicles and motorcycles across Europe. His subsequent arrest by authorities prompted both Bank 1 and 2 to submit Suspicious Transaction Reports (STRs) to Senegal's CENTIF.

A police investigation provided substantial evidence against OMEGA, implicating him in a criminal association, international trafficking of stolen vehicles, money laundering through his shell company, and the injection of illicit funds into the financial system. OMEGA allegedly benefited from the collaboration of other nationals residing in Europe, facilitating the trafficking network.

After analyzing the case—including STRs, information provided by police and other data collected by the FIU—it became evident the transactions in the two bank accounts did not align with legitimate activities of OMEGA's company. Personal and professional expenses were mingled within these accounts, which also received proceeds from the trafficking of stolen vehicles. This commingling of funds complicated cash flow management and tax accounting. Notably, both bank accounts saw significant cash deposits from OMEGA, often followed by cheque withdrawals.

Given the consistent indications of money laundering stemming from international trafficking in stolen vehicles, the FIU forwarded information to the Public Prosecutor's Office for potential prosecution on charges of money laundering.

FIU Action

The FIU conducted an asset investigation that enabled the detection of several key findings, including identifying all movable and immovable assets owned by OMEGA and associated parties, and discovering OMEGA's financial assets held within local banks. International cooperation, including collaboration with counterparts such as France's Tracfin, resulted in gathering additional information corroborating allegations against OMEGA.

Evaluation

The investigation into the case spanned two years. Various methods were employed, including collection, compilation and analysis of information sourced from banks, governmental organizations and foreign financial intelligence units, such as Tracfin.

Highlights:

- Financial analysis proved instrumental in establishing allegations of criminal conspiracy, international trafficking in stolen vehicles, receipt of stolen goods, use of shell companies for laundering illicit funds, and the integration of illicit funds into the financial system.
- Investigators successfully identified luxury vehicles and motorcycles believed to have been stolen overseas.
- OMEGA's accomplices were identified in Europe.
- The illicitly obtained vehicles were either sold in Senegal for cash via cheque transactions or exchanged for undeveloped land.
- The transactions conducted through the two bank accounts deviated from the legitimate operations of the company. Personal and business expenses were commingled, complicating cash management and account oversight.

Outcome/Contribution

At the end of the FIU and police investigations, appeared serious and consistent indications of money laundering involving the sale of stolen vehicles and motorcycles through OMEGA's company. The case was transferred to the Senegalese Public Prosecutor and OMEGA was detained. The case has yet to complete its judicial process.

Indicators

Money laundering red flags were as follows:

- **Amalgamation of funds.**
- **Strong manipulation of cash.**
- **Suspect implication in international trafficking of stolen vehicles.**
- **Criminal association.**
- **Recycling funds of illicit origin in real estate.**

CASE 19

Politically-exposed person attempts to hide illegal funds —Burkina Faso CENTIF-BF (Cellule Nationale de Traitement des Informations Financières)

Introduction

This case is about a politically-exposed person who attempted to hide (USD) four million in funds by layering it in many banks accounts across several jurisdictions, and then setting up shell companies via the complicity of a legal professional.

Investigation

This case began with a comprehensive submission made to Burkina Faso's FIU (Cellule Nationale de Traitement des Informations Financières, or CENTIF-BF) in August 2018, by local financial institution ECOBANK-BURKINA. It involved an individual from Saudi Arabia (referred to as Mr. X), his wife (Ms. X), and their associated companies, including one registered in the British Virgin Islands (as of April 2018), and another (Company Y), incorporated in Burkina Faso (as of August 2018).

Company Y was wholly owned by Company Z. Both were owned by Mr. X, born in Riyadh and residing in the United States. Mr. X claimed to have sought to engage in real estate activities in Burkina Faso, including land and property transactions, renovations, constructions and sales.

In May 2018, Mr. X initiated the opening of a corporate account in Burkina Faso for Company Y, which was still in the setup phase. However, even before the completion of the incorporation process or the opening of the corporate account, his bank in Burkina Faso received two wire transfers of (USD) two million each on June 21, 2018.

Upon inquiry by the bank regarding the purpose of these transfers, Mr. X stated the funds were contributions from Company Z for the establishment of its Company Y affiliate in Burkina Faso. The transfers originated from Mr. X's personal account at a bank in Ivory Coast (UBA). He explained the funds stemmed from the 2017 sale of a family property in Riyadh, totaling (USD) seven million: wired from Bank of America, transited through his personal account in Ivory Coast, and deposited in his account in Burkina Faso for financing Company Y's activities.

As evidence, Mr. X provided a property title written in Arabic, for which the bank requested a translated version. That was never received. Instead, he furnished other banking documents detailing the transfer process from his wife's account at BANK ALJAZIRA in Riyadh to his accounts at Bank of America, Merrill Lynch, United Bank for Africa in Ivory Coast, and ultimately to his account with ECOBANK in Burkina Faso.

According to Mr. X, the property sale was settled by a cheque in his wife's name, without proof of their marital relationship. His wife deposited the money into her account at BANK ALJAZIRA, then transferred it to Bank of America and subsequently to his savings account. From there, the funds moved between his various accounts before reaching Company Y's account in Burkina Faso.

In September 2018, Mr. X requested the transfer of the entire sum back to his Bank of America account, citing his inability to continue investing in Burkina Faso's real estate market due to misinformation provided by local real estate agencies.

FIU Action

The report from ECOBANK-BURKINA prompted analysis by CENTIF-BF in October 2018. The case was not only significant due to the substantial amounts involved—totaling (USD) four million—but also due to the intricate pattern of transfers across multiple banks and jurisdictions. Complicating matters further, Mr. X—a politically-exposed person—posed an elevated risk of potential involvement in corruption.

In response, a committee meeting of CENTIF-BF convened on October 10, 2018, to urgently address the case. The committee swiftly decided on emergency action, issuing a letter of objection to Mr. X's transfer request on the same date to prevent the funds from being returned to him.

The committee initiated two information requests: one to FinCEN (USA) and another to the Saudi Arabia Financial Investigation Unit (SAFIU) on October 26, 2018. CENTIF-BF also filed the case with the Public Prosecutor at the Regional Court of Ouagadougou on October 12, 2018.

The information sought from SAFIU aimed to ascertain the presence of Mr. X and Ms. X in their database and to authenticate a cheque suspected of being falsified, containing uncommon land block information. SAFIU's response on December 11, 2018, confirmed Ms. X's relation to Mr. X, but found no trace of Mr. X in their database. However, they authenticated the cheque, confirming its legitimacy and closing the case.

FinCEN responded on March 22, 2019, providing valuable new information, which CENTIF-BF obtained authorization to share with the Public Prosecutor. However, FinCEN was unable to furnish details on the subject's economic and social environment.

Following inquiries, FinCEN informed CENTIF-BF that law enforcement queries on Mr. X, Ms. X and the two entities yielded negative results. However, financial database research revealed four filings, including two Suspicious Activity Reports (SARs) and two Currency Transaction Reports (CTRs), totaling (USD) 21,700.

One SAR identified Mr. X in suspicious wire transfers involving foreign high-risk jurisdictions, while the other implicated both Mr. X and Ms. X in suspicious transactions across multiple locations and accounts, including transfers to Ouagadougou. These transactions indicated potential layering tactics and structuring to evade reporting requirements.

The SAR also disclosed Ms. X's ties to the Royal Saudi Family, along with her involvement in the suspicious financial activity noted in this report. Further raising concerns were the subsequent cash withdrawals, which were structured to avoid reporting limits.

On receiving authorization, CENTIF-BF forwarded the information from FinCEN to the Public Prosecutor to bolster their case.

Evaluation

The case remains unresolved in court, but significant strides have been made in the investigative process in Burkina Faso. On October 12, 2018, the court issued an Order of Seizure, following CENTIF-BF's directive to ECOBANK-BURKINA on October 10, 2018, to refrain from executing the transaction, as stipulated by Article 68 of Burkina Faso's *AML/CFT Act*. Furthermore, on January 30, 2019, a request for mutual legal assistance was dispatched to the judicial authority of the Kingdom of Saudi Arabia.

The objectives of this request included:

- Verification of the true identities of Mr. X and Ms. X.
- Investigation into whether Mr. X transferred real estate assets to Ms. X as gifts.
- Confirmation of the sale of any land by Mr. X, including the selling price and payment details.

- Inquiry into whether Mr. X and Ms. X were subjects of suspicion for financial crimes, such as embezzlement, money laundering or related offenses by Saudi Arabian law enforcement and judicial bodies.

Outcome/Contribution

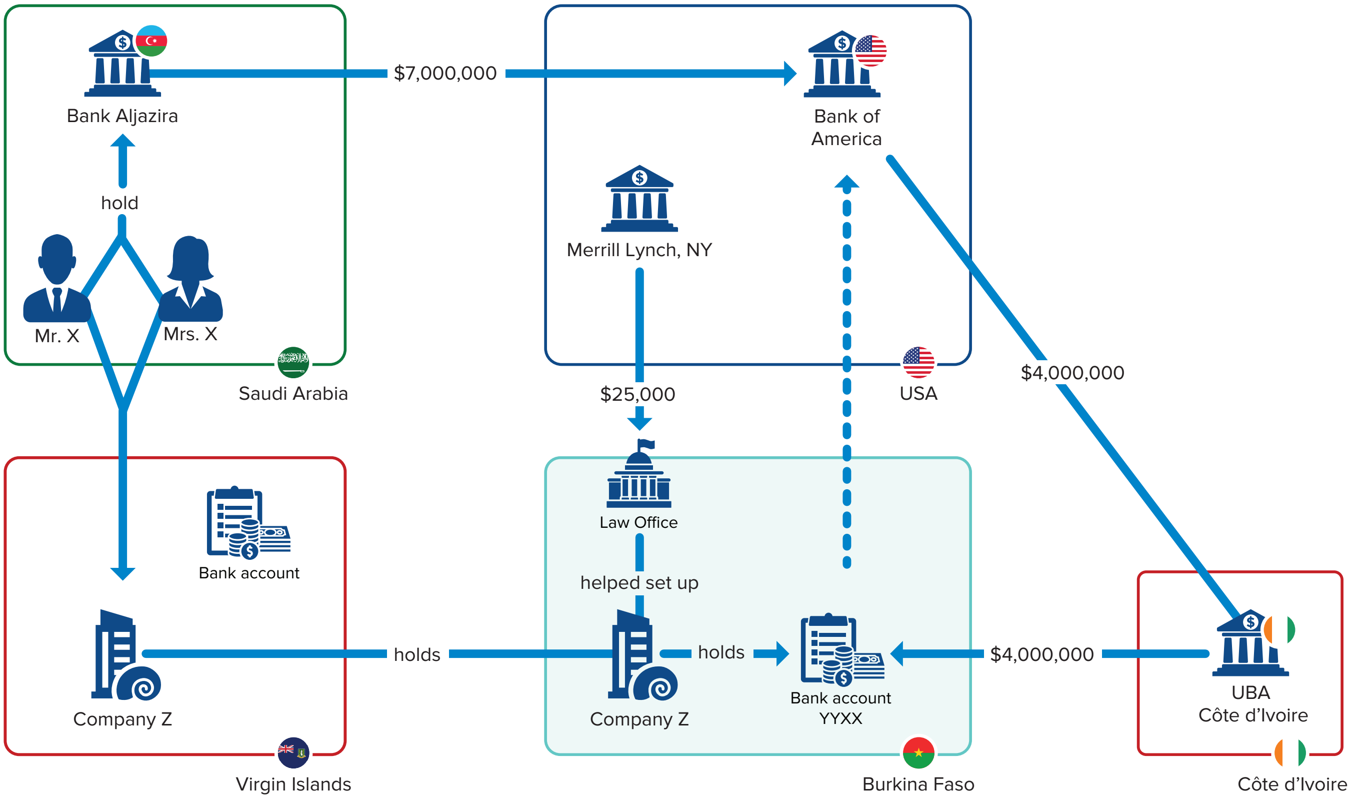
From this case, several best practices and insightful lessons emerged.

Among them: the commendable approach taken by CENTIF-BF upon identifying red flags in the SAR. Recognizing the urgency of the situation, they quickly took necessary actions to gather crucial information, laying the groundwork for potential prosecution.

The use of international cooperation channels stands out as another best practice. By leveraging these channels, CENTIF-BF was able to access valuable information from counterparts in other jurisdictions, enhancing the depth of their investigation.

In terms of lessons learned, there remains significant room for improvement in fostering effective international cooperation among FIUs, law enforcement and judicial authorities. Despite the majority of countries having ratified pertinent conventions for mutual assistance and in addressing money laundering and terrorism financing, there are still challenges to overcome in realizing seamless collaboration across borders.

Scheme 1: Politically-exposed person attempts to hide illegal funds.



CASE 20

Forex and Fraud —Tunisia CTAF (Commission Tunisienne des Analyses Financières)

Introduction

The Tunisian FIU (Commission Tunisienne des Analyses Financières, or CTAF) received a report from a regulation authority regarding a company suspected of committing foreign exchange offences according to Tunisian foreign exchange regulations and start their research.

Investigation

This is a case of trade-based money laundering, fraud, exploitation and misuse of advantages granted by the Tunisian state, as well as money smuggling.

YIN, a Tunisian car dealership company created in the 1990s, was the exclusive importer of a certain world-renowned car brand and was its legal representative in the country. YIN was thus allocated by the Tunisian Commerce Ministry an annual quota to settle its imports invoices from foreign suppliers in foreign currencies. This is because of Tunisia Foreign Exchange Regulations, which stipulate the conditions under which the Tunisian Dinar can be converted into foreign currencies. In addition, YIN benefited from a Flat-Rate Tax System.

An individual identified as “Mr. Ahmed” was the CEO of YIN.

The company’s car parts supplier, YANG (located in Country A) opted for a Cost and Freight rule for the goods transported to the Port of Rades (Tunisia).

OCEANA was a sea carrier connected to a large multinational company located in Country B, operating through several subsidiaries around the world).

The transport costs negotiated between YIN and OCEANA increased by 50% and were incorporated in the invoices established by YANG. Once the imports were settled and the transport costs paid, OCEANA transferred the increased amount of the invoice to an account number XYZ, which was opened in Country C and managed by VERA (a company that provided quality management, trustee and consultancy services, as well as incorporation and domiciliation of companies, and is located in Country D: one of the favourite tax havens of criminals around the world).

Several credit notes issued from OCEANA for the benefit of YIN but were addressed to a person named “Mrs. Helene.”

FIU Action

During the investigation, Tunisian CTAF carried out the following:

- Several requests were sent to the FIUs of Countries A, B, C & D.
- Requested information from the FIU of Country D, information on VERA and any economic or financial connection between YIN, Mr. Ahmed and VERA.
- Requested information from the FIU of Country D: The total volume of transactions between OCEANA and YIN.
- Requested information from the FIU of Country C.
- Information on the account XYZ, including the origin and destination of funds recorded on this account.
- Information on YIN and Mr. Ahmed.

Financial analysis was conducted on accounts opened abroad. This included accessing the Tunisia Trade Network database, and entailed domestic cooperation with the General Directory of the Foreign Exchange Operations within the Central Bank of Tunisia and OSINT (Open Source Intelligence).

Investigation

This investigation revealed that YIN, YANG and OCEANA were instigators and key actors of an illicit financial and legal arrangement. YANG issued import invoices to YIN, including costs plus 150 percent freight. Proceeds were sent. The goods (car parts) to YIN in Tunisia, and then transported by OCEANA. In exchange, YIN transferred the amount (allocated in foreign currencies by the Tunisian government) cited in each to YANG in Country A. After YANG collected its costs, OCEANA issued an invoice to YANG, which included 150 percent freight (negotiated between YIN and OCEANA). YANG then transferred that money to OCEANA. Regardless of that amount, YIN paid custom duties on a fixed fee basis (allocated to YIN as the exclusive importer of a certain world-renowned car brand) as soon as the goods arrived in port. Once OCEANA collected its 100 percent freight, it transferred the 50% smuggled from Tunisia and increased in the invoices. It did so by seemingly issuing credit notes to the benefit of Mrs. Helene. But in fact, the 50% was transferred to FIDUCIA into the account XYZ in Country C.

In 2016, that 50% sum represented no less than (EUR) three million.

That money was then transferred to Mr. Ahmed's personal account in Country C in the form of dividends.

Between 2017 and 2019, that account received (EUR) nine million as dividends. The beneficial owner of this financial and legal arrangement was Mr. Ahmed.

Role of the world-renowned financial institution and VERA	A world-renowned financial institution created a trust for Mr. Ahmed, and was used to receive the leaked money from Tunisia. VERA managed this trust FIDUCIA and its financial flows by disguising the scheme in such a way as to give it a seemingly valid economic and legal appearance.
Role of MARC (lawyer)	Marc's role was to prepare the financial statements of FIDUCIA and to incorporate the leaked flows from Tunisia to Country C as commissions as the result of an agreement between FIDUCIA and OCEANA. FIDUCIA negotiated with OCEANA the best freight rates on behalf of its sister YIN. It was also mentioned the amount of money that to be transferred to Mr. Ahmed as his dividend as shareholder of FIDUCIA.
Role of Mrs. Helene	The credit notes issued to her served to camouflage. The increased 50 percent fees were issued to the benefit of Mrs. Helene, but according to some emails exchanged between her and the bank of OCEANA in Country C, she personally asked the bank to send the money to FIDUCIA's account in Country C. All parties involved did receive their commissions for their valuable participation in this financial arrangement (the exact amounts of these commissions are unknown).

Evaluation

Analysis conducted by the CTAF confirmed the suspicions of the Tunisian Regulation Authority.
The possibly committed crimes in this case:

- Trade-based money laundering via over-invoicing.
- Fraud by establishing and presenting fake invoices.
- Exploitation and misuse of tax and customs advantages granted by the Tunisian government.
- Money smuggling (from Tunisia to Country C).
- Constitution of assets abroad in violation of the Tunisian foreign exchange regulations.
- Money laundering.

The case was disseminated to the Public Prosecutor's Office, which considered the evidence well founded. It ordered a judicial inquiry, which was undertaken by Tunisian Customs and Anti-Tax Evasion Department.

Over the past 30 years, an estimated (EUR) 90 million was leaked to Country C.

Outcome/Contribution

This case demonstrated why it was necessary for authorities to review existing policies and make improvements regarding involvement of nonfinancial businesses (e.g., lawyers, trusts and company service providers) in money laundering cases. The investigation also found a lack of instances of non-compliance by banks. The FIU didn't receive any STRs from the banking sector in Tunisia. The FIU salutes the regulation authority for having reported on this matter. International cooperation between FIUs via Egmont Secure Web proved to be an effective method of obtaining valuable information abroad. Without that, the FIU could not have found the missing pieces of this complex puzzle.

Indicators

- The **name mentioned in the credit notes** was **different** from the beneficiary of the funds.
- **Movement of funds through multiple jurisdictions.**
- **Misuse of legal arrangement.**

6

Terrorism, Human Trafficking and Organized Crime

Terrorism is commonly defined as violent acts committed against civilians in pursuit of political or ideological objectives. Terrorist organizations may have legitimate businesses that serve as a source of funding. However, terrorism can also be funded through illegal activities, making it similar to other criminal organizations. Identifying trends, methods and indicators related to terrorism financing is crucial preventing and responding to terrorist attacks.

Indicators

- **Large purchases of foreign currency.**
- **Opening accounts** in the name of legal entities or organizations with suspicious fund movements.
- **Small-sized wire transfers** to avoid detection.
- **Use of nonprofits** to generate or transfer funds.

The primary goal of **organized crime** is financial gain. Globalization and advancements in technology have contributed to the growth and internationalization of organized crime. Law enforcement agencies have observed a connection between organized crime and terrorist financing, as both activities try to capitalize on the opportunities presented by the other. While it is challenging to estimate the income generated by organized crime, it is believed that around (USD) two trillion is laundered annually.

Indicators

- **Use of foreign bank**s and currency.
- **Employing nominees**, fronts or other methods to conceal ownership of assets or accounts.
- **Known criminal associations.**
- **Deposits followed** by immediate transfers to concerning countries.
- **Large-sized cash deposits or withdrawals.**
- **Third-party payment of air tickets.**
- **Interconnection of seemingly independent businesses.**
- **Use of "ghost" employees.**
- **Presence of silent partners.**
- **Ownership of hidden assets.**

Organized crime groups often engage in various crimes that deprive individuals of their freedom, including **human trafficking**. This heinous activity violates fundamental human rights and has become a significant source of income for criminal organizations, rivaling traditional funding sources like drug trafficking. Experts in anti-money laundering and counter-terrorism funding explore ways to leverage the anti-money laundering system to detect, deter, disrupt and investigate human trafficking.

Indicators

- **Establishing companies** purporting to offer tourism or employment services in foreign countries.
- **International money transfers** using remittance services from high-risk countries.
- **Disproportionate number of remittance** senders compared to recipients.
- **Splitting of remittances** among related accounts.
- **Quick withdrawal** of funds received through remittances or transfers.
- **Inconsistent economic activities** of remittance senders.
- **Receipt of funds** from unrelated senders.
- **Funds received** by telecom or internet service providers through undisclosed or vaguely described services.
- **Acquiring legitimate offshore companies** to open bank accounts in different countries.
- **Use of online credit card systems** to transfer money to offshore companies or credit card accounts.

The importance of focusing on the detection, disruption and prevention of terrorism, organized crime and human trafficking cannot be overstated. Information exchange and international cooperation are key in the fight against money laundering and the protection of victims from horrendous fates. Financial Intelligence Units (FIUs) play a crucial role in this area, with many successful cases involving human trafficking. The examples presented here underline the gravity of the issue.

CASE 21

Terrorist group generated resources from an Australian-based NPO —Indonesia PPATK (Pusat Pelaporan dan Analisis Transaksi Keuangan)

Introduction

This case explores how a terrorist group in Indonesia, Mujahidin Indonesia Timur (MIT), generated its source of funds from an Australian-based NPO, The One Banner Project Incorporated (TOBPI). It also demonstrates the effective cooperation of PPATK with domestic partners and other FIUs as international partners in disclosing the case.

Investigation

On June 30, 2021, the Special Detachment of the Indonesian National Police (INP) arrested three suspected terrorists on suspicion of them having shipped packages of weapons from Bangka Belitung to Jakarta. The investigation found that the packages of weapons were intended to be smuggled to Poso, Central Sulawesi: a known location of operations for MIT. This revealed St Rugaya Umar as a funding facilitator. MIT was designated by the UN Security Council under the Al-Qaeda Sanctions Committee in September 2015. The Indonesian government (through the Domestic Targeted Financial Sanctions list) and the US Department of State have designated MIT as a terrorist organisation. MIT pledged its allegiance to Islamic State/ISIS/ISIL in 2014.

To deepen the investigation, the Special Detachment 88 Anti-Terror of INP met with PPATK for a coordination meeting regarding financial information assistances on July 27, 2021. As a quick response, PPATK revealed that St Rugaya Umar was one of the beneficiaries in Indonesia who actively received fund transfers from Australian-based TOBPI. This NPO has been under PPATK monitoring since 2020. On July 29, 2021, St Rugaya Umar was arrested in Makassar, South Sulawesi.

The results of PPATK's analysis showed that TOBPI and Amin Kobaitri (TOBPI's main controller) actively sent funds to St Rugaya Umar since December 2019. The total amounts sent by TOBPI and Amin Kobaitri to St Rugaya Umar were (IDR) 133.2 million and (IDR) 13.7 million respectively.

Later, in accordance with Amin Kobaitri's directive and approval, St Rugaya Umar sent (IDR) 4 million to a BNI account in the name of Muhamad Faizal and (IDR) 11 million to a BRI account in the name of RQ Al Ikhlas, which was under Faisal's control. Muhamad Faizal was known as an MIT facilitator who collected and distributed funds to support MIT's operational needs. The funds from St Rugaya Umar were used to buy a variety of equipment to support MIT in carrying out its operations.

Based on West Jakarta District Court Decision No. 330/Pid.Sus/2022/PN Jkt.Brt, St Rugaya Umar was found guilty of financing terrorism for the MIT terrorist group, and sentenced to three years imprisonment plus an (IDR) 50,000,000 fine with subsidiary of three months' imprisonment. In an effort to disrupt the flow of funds, DTTOT (List of Suspected Terrorists and Terrorist Organizations) Task Force has added TOBPI and Amin Kobaitri into the Domestic Targeted Financial Sanctions through Central Jakarta District Court Decision No. 05/Pen.Pid/2023/PN Jkt.Pst dated April 5, 2023.

Evaluation

A. INITIAL DETECTION

The June 30, 2021, arrest of the terrorist suspects in Bangka Belitung was preceded by coordination between PPATK and the Special Detachment 88 Anti-Terror of Indonesian National Police (INP). From April to May 2020, PPATK and AUSTRAC (Australia's FIU) were involved in bilateral cooperation within the framework of a joint analysis (Analyst Exchange Program/AEP) into alleged terrorism financing of the collection and distribution of donations carried out by several Non-Profit Organizations (NPOs) in Indonesia and Australia. The One Banner Project Incorporated (TOBPI), registered with the Australian Charities and Not-for-profits Commission[1], was one of the NPOs identified as having committed wire transfers worth a total of (AUD) 375,915.47 to the Philippines, Uganda, Indonesia, United Arab Emirates and Turkey.

IFTI Destination Country	Report Count	Total (AUD)
Philippines	173	299,361.09
Uganda	31	37,882.03
Indonesia	27	22,878.04
United Arab Emirates	3	13,574.04
Turkey	1	2,220.27
TOTAL	235	375,915.47

B. ROLE OF FIU AND ANALYSIS

PPATK played a role in tracking and analyzing the flow of funds from TOBPI and Amin Kobaitri to beneficiary parties in Indonesia, who were then allegedly using the funds to support the MIT. In the analysis process, PPATK used both open and closed sources to gather information.

IFTI reports contained instructions (provided by banks and other financial services) of transfers to and from abroad. The mechanism had been implemented since 2014 under the Indonesian law. There is no threshold of transaction amounts in this report. With IFTI database, PPATK was able to identify immediately fund transfers from Australia conducted by TOBPI and Amin Kobaitri to Indonesia with St Rugaya Umar as beneficiary. It was also identified that TOBPI sent funds to two other beneficiaries: an NPO named SBK (a subsidiary of TOBPI in Indonesia) and NH (founder of SBK). Details of the flow of funds from Australia to Indonesia are as follows:

Sender	Beneficiary	Total Amount (Idr)	Period
TOBPI (ANZ Banking Ltd, Melbourne and Commonwealth Bank of Australia)	St Rugaya Umar (Bank Mandiri 480010309790)	133,213,091.15	Dec 2019 to Jun 2021
Amin Kobaitri	St Rugaya Umar	13,710,540.27	May 2020
TOBPI (ANZ Banking Ltd, Melbourne)	SBK (BNI 2500011770)	71,665,605.00	Jul to Aug 2021
TOBPI (ANZ Banking Ltd, Melbourne)	NH (BCA 2832373541)	76,743,325.48	Jun to Jul 2021

[1] https://www.acnc.gov.au/charity/charities/35d2819f-0fd2-ea11-a813-000d3ad1f497/profile

The Integrated Customer Information System (SIPESAT) is an integrated database that contains information related to individuals and entities ownership of financial facilities. The tracing process on this platform is more effective and efficient, resulting in shorter times and lower costs. PPATK used the SIPESAT database to identify bank accounts and other financial facilities owned by St Rugaya Umar, SBK and NH.

The citizenship database contains identity number, date and place of birth and other relevant individual information. In this case, the citizenship database was used to verify that the parties under analysis and the recipients of fund transfers from TOBPI were the same.

The registration of legal entity and foundation database contains information of information on registration, establishment, type of business and structure of legal entities and foundations. With this database, PPATK was able to identify an NPO founded by St Rugaya Umar, named Ummaht Almal Alkhayrah. It was also identified the organizational structure of SBK which includes NH as the founder and as the President Director.

Information request to banks to collect supporting data and account's statements of suspects and related parties. The findings:

- Based on account statement #1480010309790 (Bank Mandiri) of St Rugaya Umar, the majority of funds received from TOBPI and Amin Kobaitri were withdrawn in cash and transferred to account #381201018169531 (BRI) of St Rugaya Umar. An outgoing transfer of (IDR) four million to the Muhamad Faizal account at BNI was also identified in this account. In St Rugaya Umar BRI's account, an outgoing transfer of (IDR) 11 million to account #007201011508533 (BRI) of RQ Al Ikhlas was traced.
- Based on account statement # 2500011770 (BNI) of SBK, the majority of funds received from TOBPI and Amin Kobaitri were withdrawn in cash (IDR) 56.2 million and transferred to account #2832373541 (BCA) of NH.
- Based on account statement #2832373541 (BCA) of NH, the majority of funds received from TOBPI and Amin Kobaitri were transferred to many parties, including SBK.

Open-source information for initial profiling of TOBPI. Based on Australian Charity and Non-for-profit Commission (ACNC) official website, TOBPI is a charity registered with ACNC and has complied with its annual reporting requirements.

Social media was used to explore the activities of the suspects on social media. TOBPI used its official website and social media accounts (Facebook and Instagram) to campaign for donation and post about their activities overseas. SBK's first collaboration project with TOBPI was noted in a March 2020 Facebook post on TOBPI's official page. On SBK's Facebook account, it was found that several campaigns for donations collaborated with TOBPI, and several posts contained Ummaht Almal Alkhayrah activities.

Passenger Risk Management (PRM) Data from Directorate General of Customs and Excise. PPATK has worked closely with the Directorate General of Customs and Excise (DGCE) in exchanging information. On February 11, 2022, the DGCE submitted data on Passenger Risk Management that confirmed Amin Kobaitri made two trips to Indonesia between September 30-October 4, 2019, and again within the period of February 12–25, 2020.

Vessel	Direction	Departure	Arrival	Movement Date	Itinerary
GA 0713	INBOUND	SYD	CGK	30/09/2019 16:45	SYD - CGK | CGK – KUL
GA 0820	OUTBOUND	CGK	KUL	04/10/2019 08:30	SYD - CGK | CGK – KUL
GA 0713	INBOUND	SYD	CGK	12/02/2020 14:55	SYD - CGK | CGK - UPG | UPG - CGK | CGK – SYD
GA 0712	OUTBOUND	CGK	SYD	25/02/2020 22:25	SYD - CGK | CGK – UPG UPG - CGK | CGK – SYD

Information exchange with other FIU (AUSTRAC and AMLC) through ESW. On September 30, 2021, PPATK initiated the implementation of a trilateral joint analysis with AUSTRAC and AMLC Philippines for the development of the analysis. According to the Philippine AMLC, TOBPI was allegedly connected to several NPOs of interest in the Philippines that are being monitored by the Philippines authorities on suspicion of terrorism financing. AUSTRAC confirmed that the Australian authorities, led by the New South Wales Police Force, are currently investigating Amin Kobaitri for possible terrorism financing. The three FIUs also submitted a request to the FIU Uganda to obtain information regarding donors in Uganda as well as possible indications of involvement with terrorist groups in Uganda. FIU Uganda has responded by providing additional information related to the NPO of interest in Uganda. FIU Uganda would continue to monitor its activities, particularly in terms of its possible connection with terrorist groups in Uganda and in the neighbouring countries.

C. DOMESTIC/INTERNATIONAL COOPERATION

To disclose this case, cooperation among related agencies is needed, both domestically and internationally. The cooperation and collaboration is explained as follows:

Domestic cooperation:

- PPATK and the Special Detachment 88 of Anti-Terror (Densus 88 AT) of Indonesian National Police have continuously coordinated in initial detection, information exchange, and the progress of investigations. Exchange of information was carried out through SIPENDAR (Sistem Informasi Pendanaan Terorisme/Information System of Terrorist Financing Suspects), an integrated platform to exchange intelligence related to terrorism financing between PPATK, Law Enforcement Agencies, and other agencies related to terrorism and terrorism financing, as well as reporting parties. This platform allows LEAs/other related agencies to submit their requests for financial transaction analysis assistance to PPATK as well as PPATK disseminate the intelligence reports to LEAs/other related agencies. SIPENDAR has a feature called Watchlist (updated every three months) which lists suspected individuals and entities involved in terrorism financing. This Watchlist is published to the reporting parties for information enrichment. PPATK and LEAs/other related agencies can utilize this for monitoring, analysis and investigation. PPATK has listed St Rugaya Umar, TOBPI, Amin Kobaitri, NH, and SBK into the Watchlist.
- PPATK has worked hand in hand with Directorate General of Customs and Excise (DGCE) in exchanging Amin Kobaitri's travel record. The travel record was utilized to confirm that Amin Kobaitri visited Indonesia in 2019 and 2020. Furthermore, this information was forwarded to Densus 88 Anti-Terror of INP to support their investigative process.
- PPATK as a member of DTTOT (List of Suspected Terrorists/Terrorist Organizations) Task Force worked closely in exchanging information with other members such as Densus 88 AT of INP, Indonesian State Intelligence Agency, The National Counter Terrorism Agency, Directorate General of Customs and Excise (DGCE) and Directorate General of Immigration to propose TOBPI and Amin Kobaitri into the Domestic Targeted Financial Sanctions List in accordance with the UNSCR 1373. Their inclusion on the Domestic Targeted Financial Sanctions List was established by Central Jakarta District Court Decision No. 05/Pen.Pid/2023/PN Jkt.Pst dated 05th April 2023. Under PPATK's monitoring, it is known that as of January 2023, the flow of funds from TOBPI to SBK is still ongoing: posing terrorist financing/terrorism threats to Indonesia. Therefore, financial disruption against TOBPI is needed immediately.

International cooperation:

- Exchanging information with other FIUs (AUSTRAC of Australia and AMLC of the Philippines) through Egmont Secure Web (ESW) concerning the flow of funds involving individuals and entities in other jurisdictions.

- Trilateral joint analysis between PPATK, AUSTRAC and AMLC from September 2021 to Mid-2022. Through this regional collaboration, a full picture of cases involving the three countries can be obtained. This program was covered in bi-weekly meeting between three FIUs. There was a session where each FIU coming with the investigators to get an update on investigation process. Three countries agree to consider measures to disrupt TOBPI and its key personnels, according to each country's approach to TF (such as prosecutions, designations and intercepting travel).

D. DISCLOSURE TO LAW ENFORCEMENT OR INVESTIGATION ARREST

Quick response and effective collaboration in exchanging information (as well as disseminating intelligence reports) between PPATK, Densus 88 Anti-Terror of INP and other related agencies/FIUs led to successful terrorism financing investigation with St Rugaya Umar as the main suspect. Based on the investigation, some findings were obtained as follows:

1. St Rugaya Umar's first interaction with Amin Kobaitri was in 2019 through Facebook. Since then, both of them actively communicated regarding the distribution of donations.
2. Ummaht Almal Alkhayrat was founded by St Rugaya Umar based on instruction from Amin Kobaitri as a subsidiary of TOBPI in Indonesia. This NPO was prepared to receive funds from TOBPI and distribute the funds for several programs.
3. In early April 2021, St Rugaya Umar traveled to Poso (Central Sulawesi) to meet Ustad Suaib and distribute the donations. In Poso, she was assisted by Ustad Suaib and Muhamad Faizal in distributing the donations to Rumah Quran (RQ) Al Ikhlas and wives of mujahideen (MIT members) who died while fighting with Indonesian forces. She was in Poso for four days.
4. Before her return to Makassar, St Rugaya Umar was informed by Muhamad Faizal that MIT lacked the funds to maintain their operation in Poso.
5. On mid-April 2021, St Rugaya Umar texted Amin Kobaitri through Whatsapp, asking for funds to support MIT, and Amin Kobaitri agreed to provide. By Amin Kobaitri's instruction, St Rugaya Umar made a fund transfer of (IDR) 11 million to RQ Al Ikhlas's account. That account was controlled by Muhamad Faizal. The funds were divided into two purposes: (IDR) one million as support for RQ Al Ikhlas while the rest of (IDR) 10 million as support for MIT. Part of the funds was used to buy two smartphones Samsung J2 Prime and two backup batteries.

St Rugaya Umar	:	"Ustad need help for the money"
Amin Kobaitri	:	"How much they need?"
St Rugaya Umar	:	"Up to you"
Amin Kobaitri	:	"Give them ten million"

In May 2021, St Rugaya Umar transferred once again (IDR) four million in funds to Muhamad Faizal's BNI account to support MIT. The funds were used to buy GPS tracking devices.

Outcome/contribution

Densus 88 Anti-Terror of INP submitted the case file to the Attorney General's Office of the Republic of Indonesia for prosecution process. St Rugaya Umar was charged with terrorism financing and terrorism. She was found guilty by the District Court of West Jakarta on August 18, 2022, of terrorism financing. She was sentenced to three years imprisonment and (IDR) 50,000,000 fine with subsidiary of three months' imprisonment (West Jakarta District Court Decision No. 330/Pid.Sus/2022/PN.Jkt.Brt).

In this case, the court seized 67 evidence items, including smartphones, backup batteries and GPS tracking device.

In the same year, Muhamad Faizal was found guilty of terrorism and sentenced to six years and six months imprisonment, and (IDR) 50,000,000 fine with subsidiary of six months imprisonment (West Jakarta District Court Decision No. 261/Pid.Sus/2022/PN.Jkt.Brt).

Terrorism financing evolves dynamically. NPOs can be misused as a source of funding for terrorist groups. In addition, sources of funding do not only come from within the country but also from abroad.

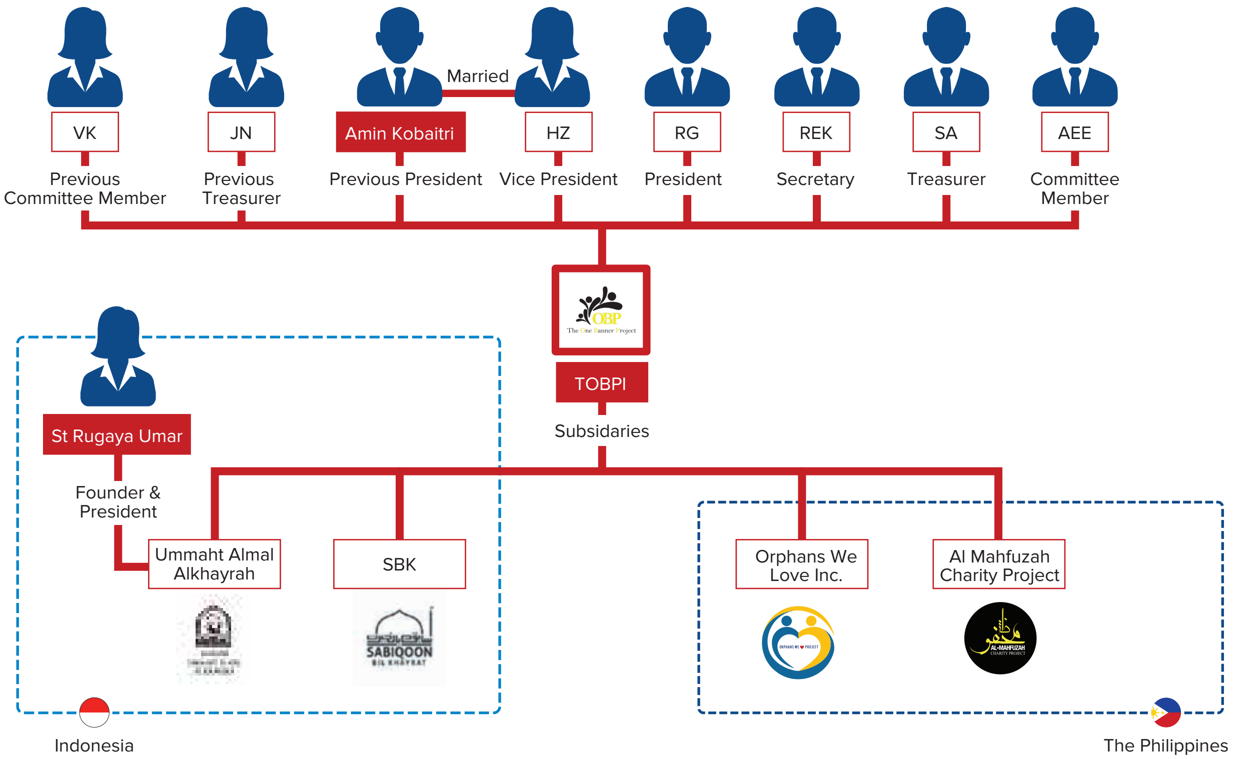
In this case, FIU plays pivotal role in detecting and tracing the flow of funds related to terrorism financing, including cross-border transactions, as an effort to support investigations conducted by LEA. FIU should continue to develop its systems in detecting and monitoring transactions related to terrorism financing. PPATK has used SIPENDAR (launched in 2021) as a new breakthrough in exchanging information related to terrorism financing between stakeholders in Indonesia. It has the feature of Watchlist that can be used in monitoring the persons and entities of interest and mitigating the terrorism financing risk.

Quick response and effective collaboration among domestic stakeholders have an important role in case disclosure. One of the keys in disclosing terrorism cases is "time". It may save thousands of lives.

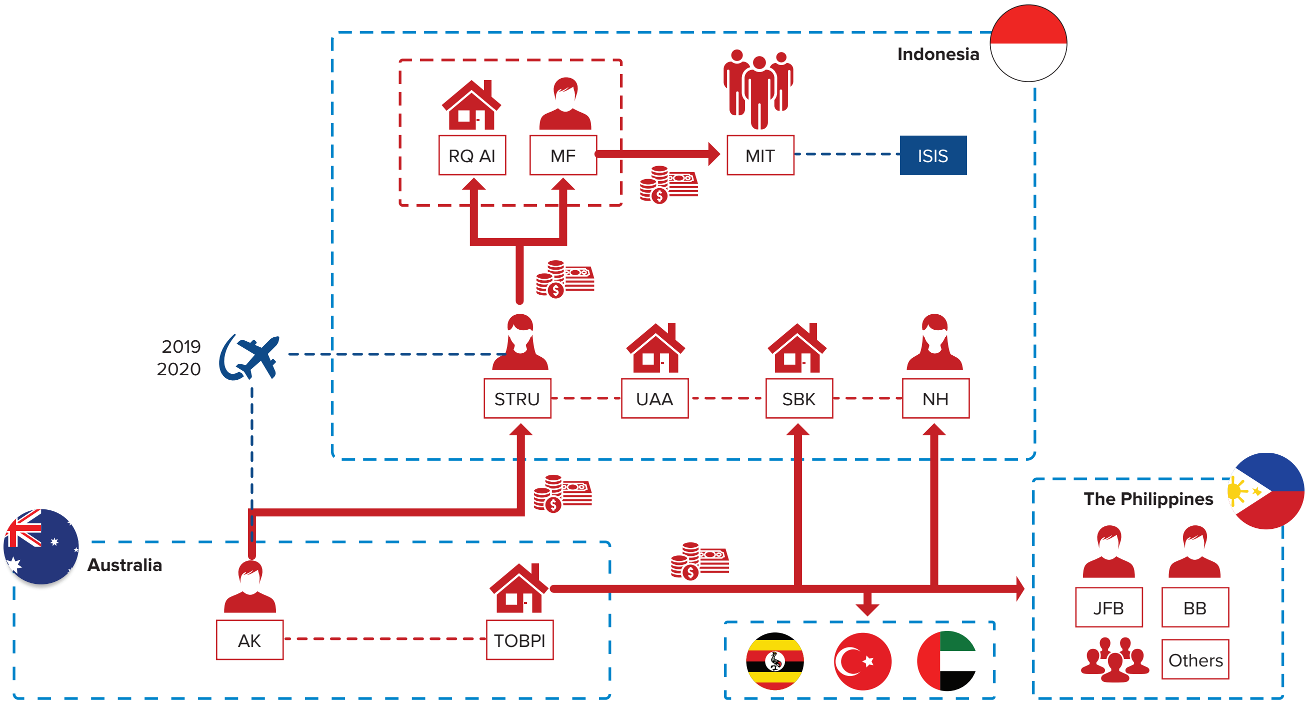
Terrorism financing is a transnational crime, so cross-border cooperation is very much needed in efforts to disrupt acts of and financing of terrorism. Collaboration between FIUs, such as joint analysis (in this case, collaboration between three FIUs), can be carried out to support investigation processes undertaken by the competent authorities in the respective jurisdictions.

Domestic Targeted Financial Sanctions List can be used as a mitigation approach to disrupt flow of funds related to terrorism financing.

Appendix A: TOBPI Structure and Office Holders



Appendix B: Funding Scheme



CASE 22

Web of frauds —Japan JAFIC (Japan Financial Intelligence Center)

Introduction

The Japan Financial Intelligence Center (JAFIC) significantly contributed to a Japanese police investigation that led to identifying and arresting money laundering group members. Informed by FIU-Nepal, JAFIC learned that fraudulent fund transfer from overseas bank accounts had arrived in Japanese ones. The origin of these funds was money stolen by hacking the SWIFT interbank messaging service of a bank in Nepal. Furthermore, extensive analysis conducted by JAFIC led to unveiling the large-scale money flows that had originated from multiple fraud cases. Six suspects were arrested, involving eight money laundering cases. Overseas organizations' assistance also contributed considerably to the operation.

Investigation

In 2017, JAFIC received notification from the FIU-Nepal stating that the SWIFT interbank messaging service of a bank in Nepal had been compromised followed by fraudulent fund transfer of stolen money to multiple accounts in jurisdictions outside Nepal. Eight transactions of approximately (JPY) 197 million or equivalent (USD) 1.7 million were requested to be transferred to bank accounts of Japanese banks and eventually two out of those attempted transactions of approximately (JPY) 18 million or (USD) 155,000 were completed. The police gained assistance via the ICPO and central authority routes and was able to identify the predicate offences as fraud.

Analysis

STR analysis conducted by JAFIC identified each account beneficiaries of two fraudulent fund transfer destinations and then learned transferred money had been withdrawn immediately after transactions. The fact also raised suspicions that the suspects had refused to return their money by claiming the transfers were for the purpose of legitimate dealings.

JAFIC also learned that the STRs on the other declined cases showed there had been suspicions of fraud involving money transfers of a substantial amount.

In the course of JAFIC's analysis of the money flows, JAFIC learned the FBI Tokyo requested Japanese National Police Agency for cooperation concerning other fraudulent money transfer cases where one of the two above-mentioned beneficiaries (hereinafter "A") was involved in. Based on the shared information by the FBI Tokyo, JAFIC found out that a Japanese company's bank account was a destination of a fraudulent money transfer from the Unites States. The money was transferred from the company's bank account to A's one, followed by retransfer from A's account to another person (hereinafter "B")'s bank account. Moreover, JAFIC's analysis showed the company's bank account was also a destination of other fraudulent fund transfers. These findings by JAFIC significantly contributed to Japanese police investigation.

FIU Action

JAFIC is an administrative-type FIU, which has been established within the National Police Agency. For assisting domestic prefectural police, which has authority to arrest suspects, JAFIC analyzed STRs and related information provided by overseas organizations. The FIU action started with JAFIC receiving input from the FIU-Nepal, followed by analysis of domestic STRs. JAFIC also reached out to FBI Tokyo for related information. JAFIC shared its findings with Japanese prefectural police that fraudulent money transfers from bank accounts in Nepal and United States to B's account by way of A's one and the money was highly possibly concealed in Japan.

Evaluation

JAFIC was able to provide with domestic prefectural police intelligence of the whole picture of its money laundering scheme. By using the intelligence, the prefectural police successfully identified the transferred defrauded money from foreign banks piled up in B's bank account. Six suspects including A and B were arrested in charge of "Concealment of Proceeds of Crime," predicate offenses of which were concerning eight fraud cases. The total amount: (JPY) 200 million or (USD) 1.3 million, proven by evidence including some gained through international mutual investigation assistance.

Outcome/contribution

JAFIC successfully correlated a case under analysis with fraud cases in the U.S. This was a direct result of JAFIC having reached out to the FBI Tokyo for relevant information. Learning the shared information from the FBI Tokyo right after the initiation of investigation, the prefectural police was able to form a complete picture of the money laundering scheme and correlations with the predicate offenses.

Indicators

- **Immediate withdrawal of received money.**
- **Unsubstantiated source of funds.**
- **Inconsistency with a customer profile**: a large amount of money was transferred from multiple foreign jurisdictions to a bank account in a short time span.

CASE 23

Human trafficking network recruited women to work as models or teachers only to be sexually exploited —Mexico FIU

Introduction

In 2019, an investigation was carried out on a transnational human trafficking network, in which recruited women mainly from Venezuela, were brought to Mexico under the pretense of being hired as models or teachers but were later exploited sexually. It also involved Money Laundering (ML) through five shell companies.

Some of the individuals involved in this crime had been investigated before, and even arrest warrants had been issued for the crimes of human trafficking and sexual exploitation.

The investigation led to the arrest of the organization's leader.

Investigation

SARs and information sent by an obligated subject (OS) of DNFBP (Designated non-financial Businesses and Professions) were detected through the FIU-MX risk model, in which the leader and founder (Subject A) of a criminal organization (OC) dedicated to Human Trafficking and Sexual Exploitation was identified.

The OC leaders (Subject A, Subject B) were spouses. They contacted women abroad mainly in South America, inviting them to Mexico with a deceptive offer that they would be hired as models or teachers. On arrival, their passports were taken and told they would be returned upon settlement of a debt accrued from travel, lodging, food and other expenses. This debt would be repaid with sexual services.

The OC used a website with a catalog of the victims (the photographs were modified to prevent family members from recognizing them), with which they offered services for their sexual exploitation. Company A was the owner of the website, and its shareholders were Subjects A and C (arrested on charges of Human Trafficking and Sexual Exploitation).

Clients contracted the services through the website, they agreed on the profile, date, time, location and payment method. The members of the network communicated the details to the victim and regarding the payment, it was indicated that the amount was used to reduce their debt and the payment of fees for advertising it on the website.

The money resulting from the crimes of Human Trafficking and Sexual Exploitation was placed in the Financial System (FS) through cash deposits and transfers (SPEI's) in shell companies, created to hide the origin of the resources and stratify them among the members of the OC via the payment of salaries, as if they were workers. Finally, Subject A integrated the resources through the acquisition of real estate and virtual assets.

It was also identified that a portion of the payments derived from the sexual exploitation were used by the OC to cover operational expenses (e.g., salaries to drivers and/or escorts in charge of ensuring the victims didn't escape), as well as the victims' expenses.

The rest of the money resulting from the Human Trafficking and Sexual Exploitation was laundered by the OC with the leaders as final beneficiaries (Subjects A and B) through shell companies that simulated the payment of salaries. Such payments were identified through the collection of tax information. With this information, it was possible to identify the amounts that the companies paid to the leader, simulating the legal appearance of the resources resulting from the crimes of human trafficking and sexual exploitation.

With this case, the FIU-MX identified the ML network used by an OC dedicated to the crime of human trafficking for sexual exploitation. Based on the financial analysis of the leader and inter-institutional collaboration, the location and arrest of the leader was achieved. In addition, partners, names, companies used to launder money were identified, as well as the main assets they acquired.

Additionally, an operation was identified sent by the DNFBP's of the leader of the OC (Subject A) related to the real estate sector, for the acquisition of real estate in the period from 2016 to 2018 for a value of (USD) $121,588.82, the OS sent an alert, because upon identifying its client it realized that according to information from open sources he had arrest warrants for the crimes of Human Trafficking and Sexual Exploitation. With the information sent by the SO and the inter-institutional collaboration with the data, location and arrest of the leader, who had been on the run for two years, was achieved.

FIU Action

The FIU-MX credits the 2014 incorporation of the DNFBP's into Mexican legislation in the Federal Law for the Prevention and Identification of Operations with Resources of Illicit Origin (LFPIORPI), with the obligation to report to the FIU the transactions that they carry out with their clients. It is a tool that has made it possible to identify and develop more complete cases with better results.

Compliance with the LFPIORPI by the DNFBP's OS by correctly identifying its client and sending the operation information to the FIU-MX, this with inter-institutional collaboration allowed the location and arrest of (Subject A) who had been a fugitive for two years. It also allowed the analysis and development of a case in which the OC's ML network was identified. Consequently, we collaborated in the criminal investigations with financial information and independent investigations were initiated for ML, with the predicate crime being Human Trafficking and Sexual Exploitation, so this case has been a starting point for other cases.

In addition, the FIU-MX has implemented actions to obtain additional information, therefore, it has signed multiple memorandums of understanding (MOU) with other Mexican agencies with which additional information is obtained. In that case, the tax information allowed the identification of companies that laundered the OC's money, that is, they hid the illicit origin of the money, placing it in cash in the companies and stratifying it through the payment of salaries to Subject "A".

In short, the information obtained from DNFBP's and the data from tax sources allowed the criminal investigations to be nourished and an independent case to be identified and developed against a ML network with the predicate crime of Human Trafficking and Sexual Exploitation.

A police report was filed with the Attorney General's Office FGR for ML, with the predicate crime being Human Trafficking and Sexual Exploitation against 18 individuals and legal entities.

The UIF-MX incorporated 18 natural and legal persons to the List of Blocked Persons (LPB), which implies the immediate suspension of the performance of acts, operations and services with the clients or users designated in the LPB, making it impossible for both to open accounts and cancel current ones, as well as prevent the disposition of resources they contain, either in one's own name or through mandates or commissions, that is, owner, co-owner, signatory and/or authorized, trustor, legal representative and /or representative and beneficiary.

The UIF-MX shared information to support criminal investigations related to the crimes of Human Trafficking and Sexual Exploitation, with inter-institutional collaboration allowing to locate and detain (Subject A) who had been a fugitive for two years.

Evaluation

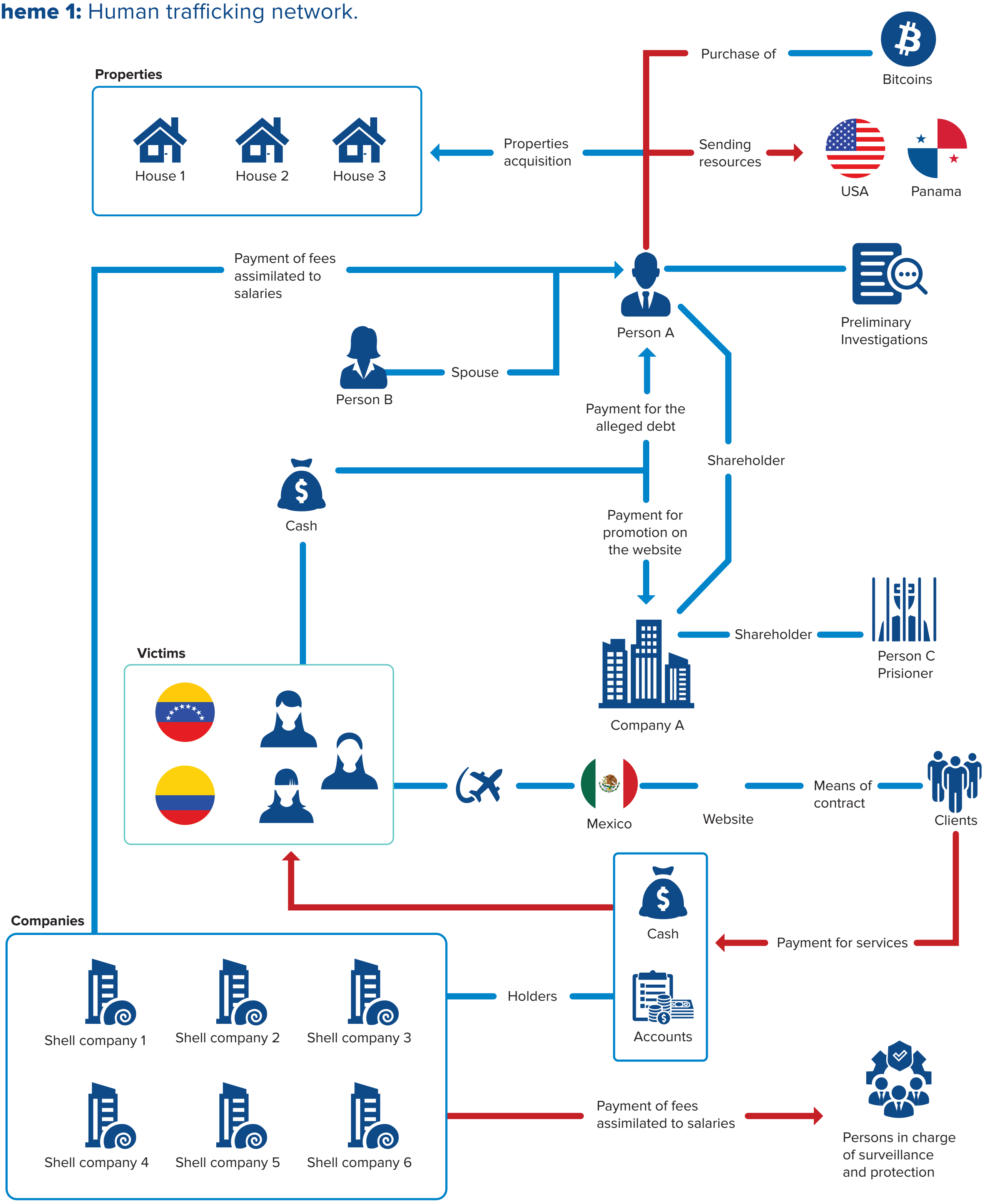
The information from DNFBP's made it possible to inform criminal investigations related to the crimes of **HUMAN TRAFFICKING AND SEXUAL EXPLOITATION**, coupled with the inter-institutional collaboration that made it possible to locate and detain (Subject A) who had been a fugitive for two years.

The data from tax sources added to the Open Source information from FS and DNFBP's were key to identifying partners and companies linked to the ML Network. Consequently, the identified subjects were reported to the FGR and designated to the LPB with the purpose of dismantling the OC by preventing them from using the Mexican FS.

Indicators

- **Obtain information** from an OS of a DNFBP's according to LFPIORPI, which was a key piece both in the development of the ML case and in the arrest of the OC leader who had been on the run for two years.
- **Taking advantage of tax information** as an additional source to the data held by the UIF-MX made it possible to identify, through payments reported to the treasury, the existence of five shell companies charged with concealing the illicit origin of resources.
- **The analysis of the information obtained** from various sources allowed the identification of the members of an ML network and its operation scheme.
- **The legal powers that the UIF-MX has allowed** it to begin a criminal investigation with an independent case against an ML network with the predicate crime of Human Trafficking and Sexual Exploitation and to include them in the LPB with the purpose of dismantling to the OC preventing it from using the Mexican FS.

Scheme 1: Human trafficking network.



CASE 24

The Third-Party Cash Deposit Project —Australia AUSTRAC

Introduction

This case study concerns criminal use of Intelligent Deposit Machines (IDMs), a type of automatic teller machine that offers high-speed, large-capacity cash deposits into a bank account, sometimes without needing identification or a bank card (for third-parties). IDMs provided anonymity, speed, efficiency and 24/7 access for criminals laundering funds.

The investigation started in 2019, when the Western Australia Police Force (WAPF) partnered with AUSTRAC and its industry partners to investigate a Perth-based organized crime syndicate using IDMs to launder proceeds of crime. It evolved in several stages through the creation of the Third-Party Cash Deposit Project.

Investigation

The investigation began in 2019, when the WAPF partnered with AUSTRAC to investigate an organized crime syndicate using IDMs to launder the proceeds of crime. AUSTRAC focused on identifying the characteristics displayed by depositors rather than the account holder, using innovative analysis techniques. This revealed that over a six-week period, depositors made 1,879 cash deposits via IDMs into 167 different bank accounts linked to the syndicate, totaling approximately (AUD) 5.4 million. This intelligence led to WAPF to arrest five members of the organized crime syndicate. While the arrests disrupted money laundering for a short time, AUSTRAC identified common money laundering techniques used in other Australian cities.

AUSTRAC expanded the use of the indicators to target the broader money laundering risk through a cross-agency project called the Third-Party Cash Deposit Project. The aim was to respond to the money laundering risks the analytical methodology identified and provide value-added intelligence to law enforcement investigations.

As part of this project, AUSTRAC and its public and private sector partners identified a money laundering syndicate controlled from Europe, directing the proceeds of crime from Australia to a country in Southeast Asia. This led to multiple arrests, both in Australia and internationally.

Strategic and tactical decisions maximized the Third-Party Cash Deposit Project's efficiency. AUSTRAC established co-located operational hubs to ensure the timely and secure exchange of information and operational analysis during the project. Security-vetted financial industry members worked with AUSTRAC analysts in these hubs on classified matters to identify financial patterns and predict where and when organized crime syndicates would target IDMs.

AUSTRAC used its powers under Australia's AML/CTF legislation to issue notices to private sector entities requesting 12 months' worth of data equating to over 7.8 million transactions conducted through IDMs. AUSTRAC engaged industry to help draft the notices to ensure the information requested was relevant and could be produced in a timely manner to assist law enforcement efforts. This information assisted AUSTRAC and its partners to better understand the size and nature of third-party cash deposits through IDMs.

AUSTRAC delivered significant operational and strategic outcomes from the project, including the development of a new risk assessment to understand the risk third-party cash deposits through IDMs presented. In response to this assessment, Australia's four largest banks conducted a review of their processes and tightened controls around third-party cash deposit rules involving IDMs. This helped mitigate IDM vulnerabilities. AUSTRAC shared this risk assessment with law enforcement and industry partners as a reference tool to understand the money laundering typologies and behavioral patterns.

The project also resulted in the seizure of cash and illicit goods, and disruption of one of Australia's largest money laundering syndicates.

FIU Action

AUSTRAC worked with industry partners to develop new and innovative techniques to analyze information, including an analytical technique called clustering, and leveraged trusted partnerships to get a holistic picture of this money laundering risk in Australia.

AUSTRAC developed a methodology to identify deposits displaying characteristics of a professional money laundering organization based on the time between deposits, number of deposits and total value. This analytical technique was referred to as clustered deposits or clusters. AUSTRAC analyzed the transactional data to identify patterns of deposits that matched the typologies in the risk assessment. These analytical methods identified patterns in the approximately 7.8 million transactions third parties made at IDMs, valued at (AUD) 4.8 billion.

AUSTRAC also introduced a secure information sharing platform with video conferencing, instant messaging and document management functionality. This was useful during different jurisdictional lockdowns during the COVID-19 pandemic, enabling analysts to continue to liaise with investigators despite not being in the office.

Joint efforts with law enforcement agencies leveraged Fintel Alliance, the AUSTRAC-led public private partnership (PPP), and resulted in the establishment of a PPP project on the topic. Joint project members shared information and resources to deepen understanding of IDM vulnerabilities and identify deposit patterns consistent with money laundering typologies. AUSTRAC shared these learnings with law enforcement partners to assist investigators with identifying, analyzing and handling financial information in support of prosecutions.

AUSTRAC created a catalogue of IDM cash deposits using a specific bank card or mobile phone number. This proved critical for physical law enforcement surveillance, helping to establish a pattern of deposit activity and to identify previously unknown accounts of interest.

Where AUSTRAC suspected an organized crime syndicate was controlling multiple accounts, AUSTRAC analyzed internet banking login information to determine whether the same person was controlling the accounts.

Evaluation

Following the identification of the IDM money laundering risk in 2019, AUSTRAC led and coordinated the Third-Party Cash Deposit Project through Fintel Alliance and in conjunction with law enforcement agencies and industry partners.

This project allowed for further development of the indicators and findings from the initial investigation, which were transferrable to a wider cohort of entities. AUSTRAC could harness the wider Fintel Alliance and the benefits of co-located operational hubs where security-vetted financial industry members worked alongside AUSTRAC analysts on classified matters.

The project allowed for easier dissemination of analyzed information, and shared insights and feedback between different partners. This included linking law enforcement agencies with government and industry partners on operational matters. These opportunities enhanced suspicious matter reporting and prioritized responses to law enforcement requests for information.

The broader project outcome was hardening the environment to money laundering. Australia's four largest banks conducted a review and tightened controls around third-party cash deposit rules involving IDMs, mitigating the resulting risks.

Outcome/contribution

Since resolution, law enforcement agencies seized:

- (AUD) 4 million in cash.
- 270kg of illicit tobacco.
- Illicit drugs, including cocaine, MDMA, methamphetamine and cannabis.
- Firearms and ammunition.
- Encrypted communication devices.
- Luxury vehicles.

The project saw thirteen people arrested and charged with multiple money laundering offences. It also allowed the development and exchange of actionable intelligence products including:

- A risk assessment.
- A methodology report.
- Two information reports for industry partners.
- Spontaneous information disclosures to other FIUs.
- 14 notices to private sector entities.
- 28 tactical intelligence reports.
- 114 information disclosures.
- Triage of 568 Suspicious Matter Reports.

Indicators

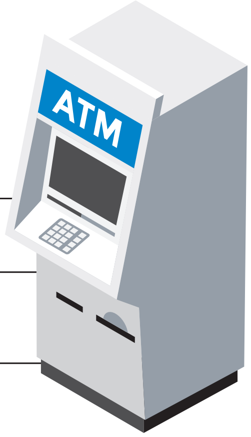
The initial indicator was **large amounts of cash being deposited at IDMs in quick succession.**

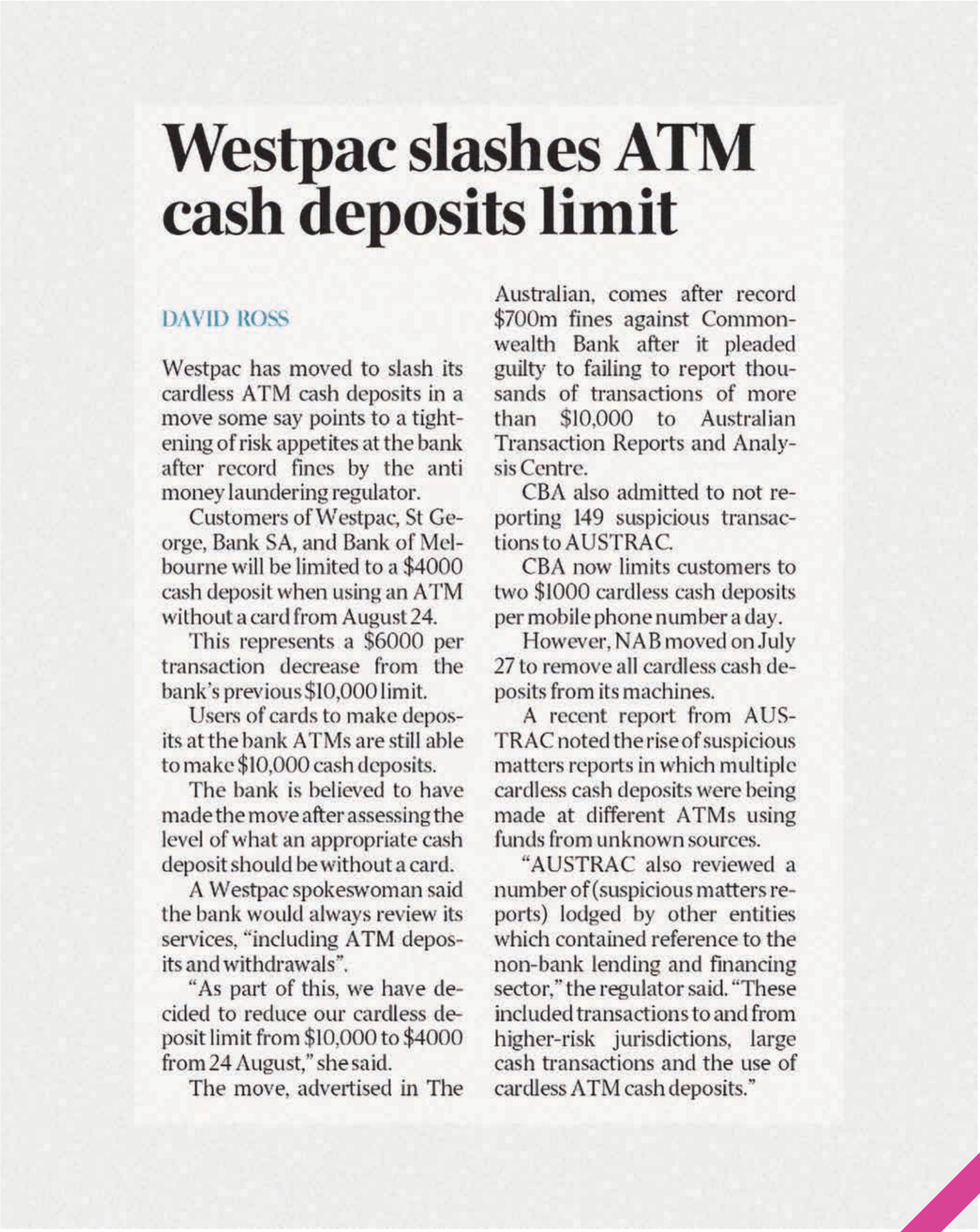
The deposits often occurred around midnight, when IDM or account deposit thresholds reset, allowing for greater volumes of cash deposited in a single session.

- **An indicator was that anonymous third parties** were transferring funds in quick succession to accounts to which they had no clear relationship.
- **Another identified indicator was that deposits at IDMs into accounts** were often undertaken in brief windows of time with successive identical deposit amounts. This pattern allowed for the creation of an analytic technique focusing on these clustered deposits or clusters. AUSTRAC analyzed the transactional data to identify patterns of deposits that matched the typologies in the risk assessment.

Deposit Clustering Algorithm

$2500	>	$2500	>	$1000	>	$2000	>>	**Total deposited >$7000**
(Account A)	>	(Account A)	>	(Account B)	>	(Account B)	>>	**More than 1 beneficiary account**
11:00am	— — —	11:03am	— — —	11:07am	— — —	11:12am		**At least 4 consecutive transactions**
	TIME BETWEEN EACH DEPOSIT < 5 MINUTES							





Westpac slashes ATM cash deposits limit

DAVID ROSS

Westpac has moved to slash its cardless ATM cash deposits in a move some say points to a tightening of risk appetites at the bank after record fines by the anti money laundering regulator.

Customers of Westpac, St George, Bank SA, and Bank of Melbourne will be limited to a $4000 cash deposit when using an ATM without a card from August 24.

This represents a $6000 per transaction decrease from the bank's previous $10,000 limit.

Users of cards to make deposits at the bank ATMs are still able to make $10,000 cash deposits.

The bank is believed to have made the move after assessing the level of what an appropriate cash deposit should be without a card.

A Westpac spokeswoman said the bank would always review its services, "including ATM deposits and withdrawals".

"As part of this, we have decided to reduce our cardless deposit limit from $10,000 to $4000 from 24 August," she said.

The move, advertised in The Australian, comes after record $700m fines against Commonwealth Bank after it pleaded guilty to failing to report thousands of transactions of more than $10,000 to Australian Transaction Reports and Analysis Centre.

CBA also admitted to not reporting 149 suspicious transactions to AUSTRAC.

CBA now limits customers to two $1000 cardless cash deposits per mobile phone number a day.

However, NAB moved on July 27 to remove all cardless cash deposits from its machines.

A recent report from AUSTRAC noted the rise of suspicious matters reports in which multiple cardless cash deposits were being made at different ATMs using funds from unknown sources.

"AUSTRAC also reviewed a number of (suspicious matters reports) lodged by other entities which contained reference to the non-bank lending and financing sector," the regulator said. "These included transactions to and from higher-risk jurisdictions, large cash transactions and the use of cardless ATM cash deposits."

WHAT MAKES **A GOOD CASE**

The Best Egmont Case Awards (BECA) competition is a highly anticipated event in the annual activities of the Egmont Group. It serves as a platform for members to showcase exceptional work.

A panel of judges evaluates a wide range of cases based on established criteria that defines what makes each one interesting and educational. The evaluation process considers the complexity and outcomes of each case. While the cases under consideration span the past four years, some are still ongoing at the time of publication due to lengthy judicial procedures. A few cases began before evaluation and were recently concluded.

Those cases still before the courts are adjusted to avoid compromising ongoing investigations. The complexity of each case is assessed based on intelligence-gathering methods, challenges faced, the use of open-source criteria, as well as on the collection of intelligence from both domestic entities and foreign jurisdictions through the Egmont Secure Web.

Selected cases showcase the exceptional skills of Financial Intelligence Unit analysts who use their knowledge to gather information from various sources, including public and private entities. Through their analytical expertise, they untangle intricate financial, legal and corporate obfuscation.

In each case, the FIU plays a pivotal role in uncovering criminal schemes, bringing the perpetrators to justice, and in confiscating illicit assets through judicial procedures. As criminals continuously devise new methods to evade financial regulators and law enforcement, FIU analysts consistently demonstrate their importance in analyzing complex data and connecting the pieces of the puzzle that often confound criminal investigators.

Given the unique position of FIU analysts, they can collaborate with financial institutions, domestic law enforcement agencies and foreign FIUs to discover novel schemes that would otherwise go unnoticed. The success of these cases is measured by effectively sanctioning criminals and recovering their hidden stolen assets.

The FIU has closely collaborated with law enforcement to identify financial and non-financial instruments involved in these cases. This entails coordinating activities with police, prosecutors, judges, taxation and customs authorities, as well as other relevant entities to paint a comprehensive picture of complex Money Laundering (ML) schemes.

The FIU frequently provides advice and support to prosecutors and police in building strong cases to withstand judicial review. Financial crimes continue to be perpetrated internationally in many instances. Thus, the FIU plays a crucial role in gathering information and intelligence from other Egmont members. It is then used for mutual legal assistance requests: ultimately to freeze criminal assets hidden abroad.

Although often operating behind-the-scenes, these cases vividly illustrate how FIUs centralize effective domestic and international coordination, leading to the arrest, conviction and sentencing of criminals and the recovery of stolen assets.

Many of these cases highlight the successful collaboration between FIUs and the private sector through public-private partnerships. Banks and other financial and non-financial institutions demonstrate a willingness to assist in these cases by gathering information (guided by the FIU) on their suspicious clients, and by actively sharing valuable information that may indicate potential criminal activity.

These public-private partnerships exemplify how both sectors can join forces to enhance the financial system's integrity, eliminate illicit actors and ensure a level playing field for all.

Criteria for BECA Case Selection

An example of an effective case:

1. It must have concluded within the last five years.
2. It should provide significant, informative value to Egmont member FIUs.
3. It should highlight new or sophisticated ML schemes, innovative techniques and methods, the involvement of multiple agencies and jurisdictions and cite the amount of funds involved.

Focus on FIU Work and Analysis

Cases should elaborate on the work of the FIU and its pivotal role in case development, including initiating the case, developing intelligence and leveraging international connections that may otherwise be inaccessible.

In addition, cases should demonstrate the value added by FIU analysis.

Identification of Domestic and International Cooperation

Cases should provide examples of effective international and/or domestic collaboration that contributed to a more successful outcome.

Cases may indicate the involvement of other jurisdictions and how they exemplified effective international cooperation.

Clear Demonstration of the Evolution of the Case

Each case should illustrate how it evolved and how feedback enhanced its development, ultimately leading to a positive outcome.

Challenges faced in identifying the ML scheme should be described and any new ML techniques or trends should be identified.

Successful outcome of each case should be demonstrated.

Other Results

Cases should show how they influenced changes to domestic legislation, policies and procedures of the FIU, as well as those of domestic and international partners.

In addition, cases should support the conclusions of national risk assessments.

BEST EGMONT CASES

Financial Analysis
Cases **2021–2023**

EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

Egmont Group
of Financial
Intelligence Units

THE EGMONT GROUP SECRETARIAT

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