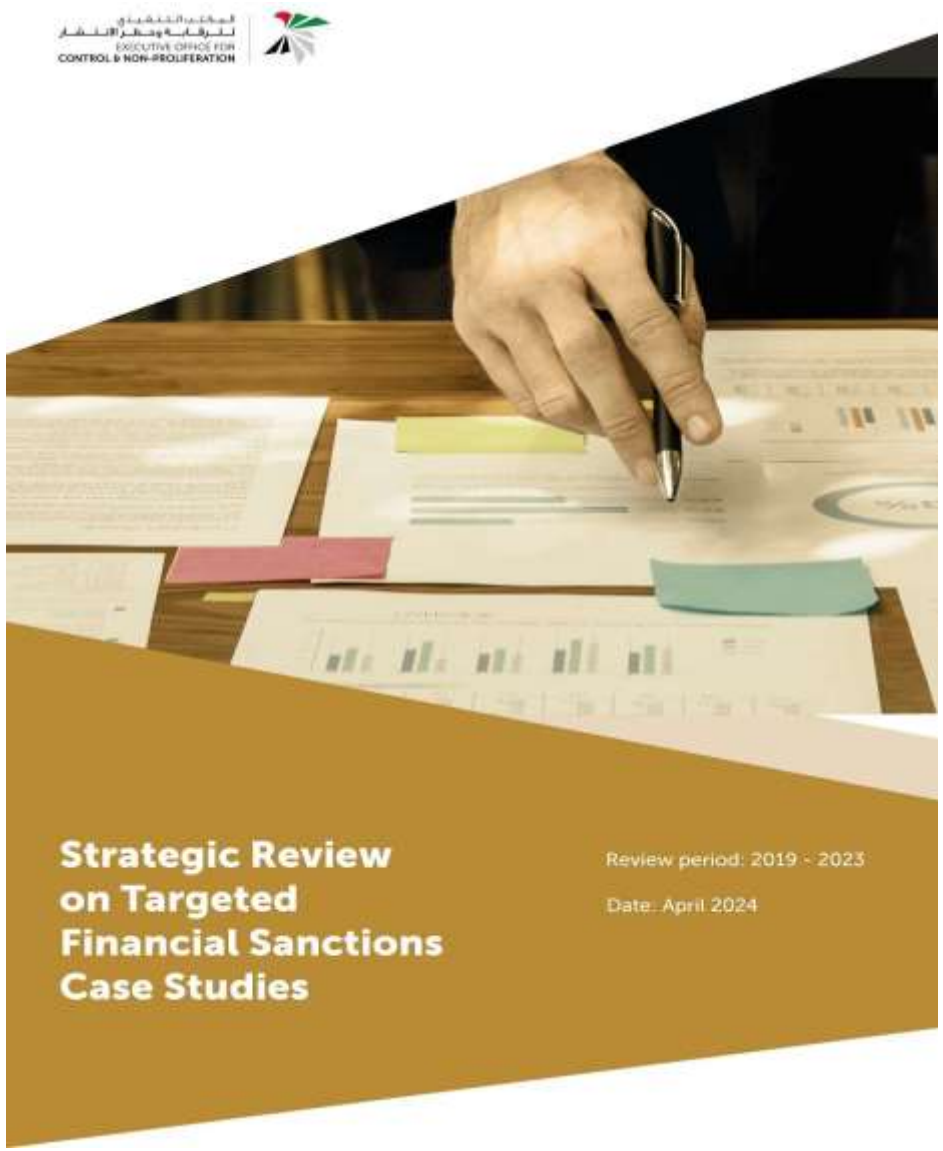
Targeted Financial Sanctions (TFS) Case Studies and Typologies



Introduction and Purpose

1. The United Arab Emirates (UAE), is a member of the UN – and is mandated to assist in suppression and countering Terrorist Financing, Proliferation Financing and Weapons of Mass Destruction (WMD).

2. To document how Financial Institutions (FIs), Designated Non-Financial Businesses Professions (DNFBPs) and Virtual Assets Service Providers (VASPs) can be abused by bad actors.

3. The Executive Office for Control and Non-Proliferation (EOCN) collaborates with the government and private sector to raise awareness about the main typologies and emerging TF/PF risks and sanction evasion.

4. The purpose of this document is to review past TF and PF cases and allow in understanding most common trends in cases related to TFS, in addition to studying changes in patterns and typologies across the years.

Methodology

The original document presents a total of 33 TF&PF cases collected from Law Enforcement Authorities across the UAE for a period from 2019 – 2023.

Respectively the periods were split into two - firstly 2019 to 2021 consisting of 23 case studies (18 TF and 5 PF) and secondly 2022 to 2023 consisting of 10 case studies (7 TF and 3 PF).

Ultimately upon analysis, the EOCN has classified cases based on the below 4 elements:

- Source of Information (Where is the suspicion coming from?)
- Type of Suspicion (Why is that suspicious?)
- Tools or Instrument Used (How did the perpetrators try to misuse the system?)
- TF & PF Patterns and Typologies (What transpired?)

Methodology

1. Terrorist Financing: This refers to the provision of funds or support to terrorist organizations or individuals to carry out terrorist activities. It involves the transfer of money or other assets for the purpose of facilitating terrorist acts.

2. Proliferation Financing: This involves providing financial support or resources to entities or individuals involved in the proliferation of weapons of mass destruction. It includes activities that help in the development, acquisition, or transfer of WMD-related materials, technology, or expertise.

3. WMD (Weapons of Mass Destruction): WMDs are weapons that can cause significant harm to many people or cause extensive damage to infrastructure and the environment. They include nuclear, chemical, and biological weapons designed to inflict mass casualties or destruction.

Chapter 1: Classification of TFS Cases for the Period (2019 – 2021)

Based on Source of Information

In this review, the sources of information vary across different entities such as local competent authorities, FIs and DNFBPs. The table below lists the 5 main sources of information of which cases are built upon. It is evident that the greatest source of information is from Intelligence information and International cooperations that leads to identify TF / PF activities or sanction evasion from UN sanction list or local terrorist list, followed by banks through Suspicious Transactions Reporting (STR) to the UAE Financial Intelligence Unit (FIU) on transactions that occur on the mainland or free zones, which assisted the LEAs to trace and freeze funds related to TF / PF activities.

Source of Information	*Number*
Intelligence Information and International Cooperation	12
Bank	7
Export Control Entities	2
Legal Entity	1
Brokerage	1

Based on Suspicion Identified

In many cases, the reason of suspicion on an activity/transaction involved is what triggers local authorities, FIs and DNFBPs reporting to competent authorities to conduct further investigations. The table below lists the 8 types of suspicions of which the cases were based on and it demonstrates that the highest type of suspicion for reporting methods used by criminals to conceal or disguise their intent to support TF/PF through using front or shell companies and shipments of dual-use items.

Type of Suspicion	*Number*
Front companies to support TF group (s)/ PF program	7
Shipment of Dual-Use items	6
Send/Receive Funds to designated NPO	3
Smuggling of Goods (Gold, Petrochemicals, etc.)	2
High volume transfer to / from high-risk jurisdictions	2
Account Belong to Designated Persons	1
Purchase stock by designated person	1
Remittance in small amounts	1

Based on Tools and Instruments Used

Criminals involved in TF/PF activities may use different financial and non-financial tools and instruments to facilitate placement and movement of funds to support their illicit activities, the table below lists the 9 tools used by criminals and clarifies that the most common tools or instruments to exploit the financial and non-financial system to assist TF activities or PF programs through using forged documents and bills, and bank wire transfers.

Type of Tool or Instrument	*Number*
Forge Documents and Bills	8
Bank wire transfer	6
Hawaladar	2
Transfer Via Exchange House	2
Purchase Stocks	1
Bank Deposit	1
Cash Cross Borders	1
Investments (Real Estate, Companies, etc.)	1
Bank Cheque	1

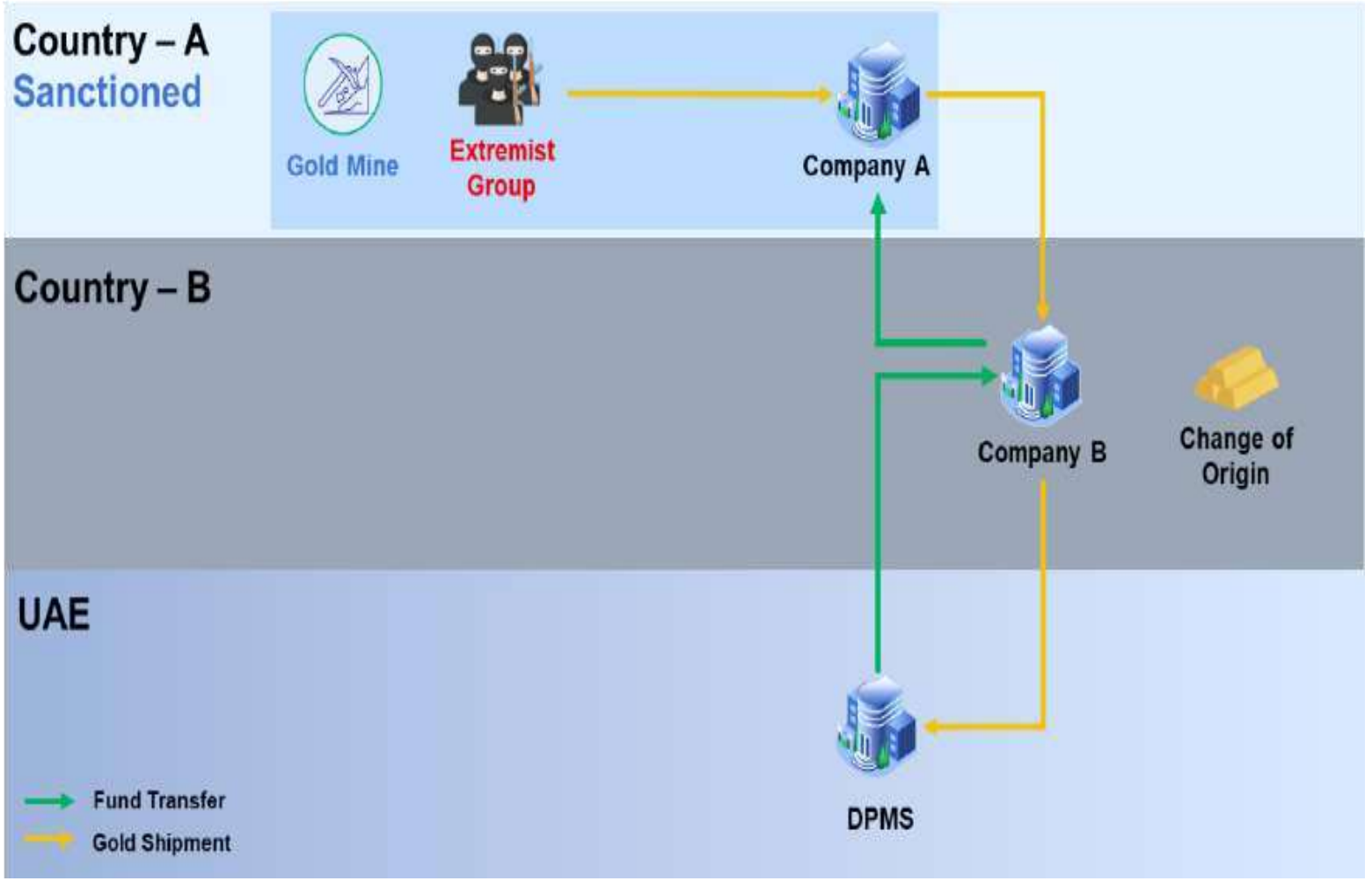
Targeted Financial Sanctions
Terrorist Financing Patterns & Typologies

First Pattern / Typology: Smuggling of Gold

This case study was triggered based on international cooperation through information received from foreign counterparts to local customs on a shipment headed to the UAE.

Gold extracted by extremist group located in sanctioned country A is smuggled to company B, located in country B, with the purpose of changing the origin of the gold to avoid any links with sanctioned country A.

DPMS in the UAE purchased the gold from company B (legitimately) and transferred the funds to company B which then remits the funds back to company A.

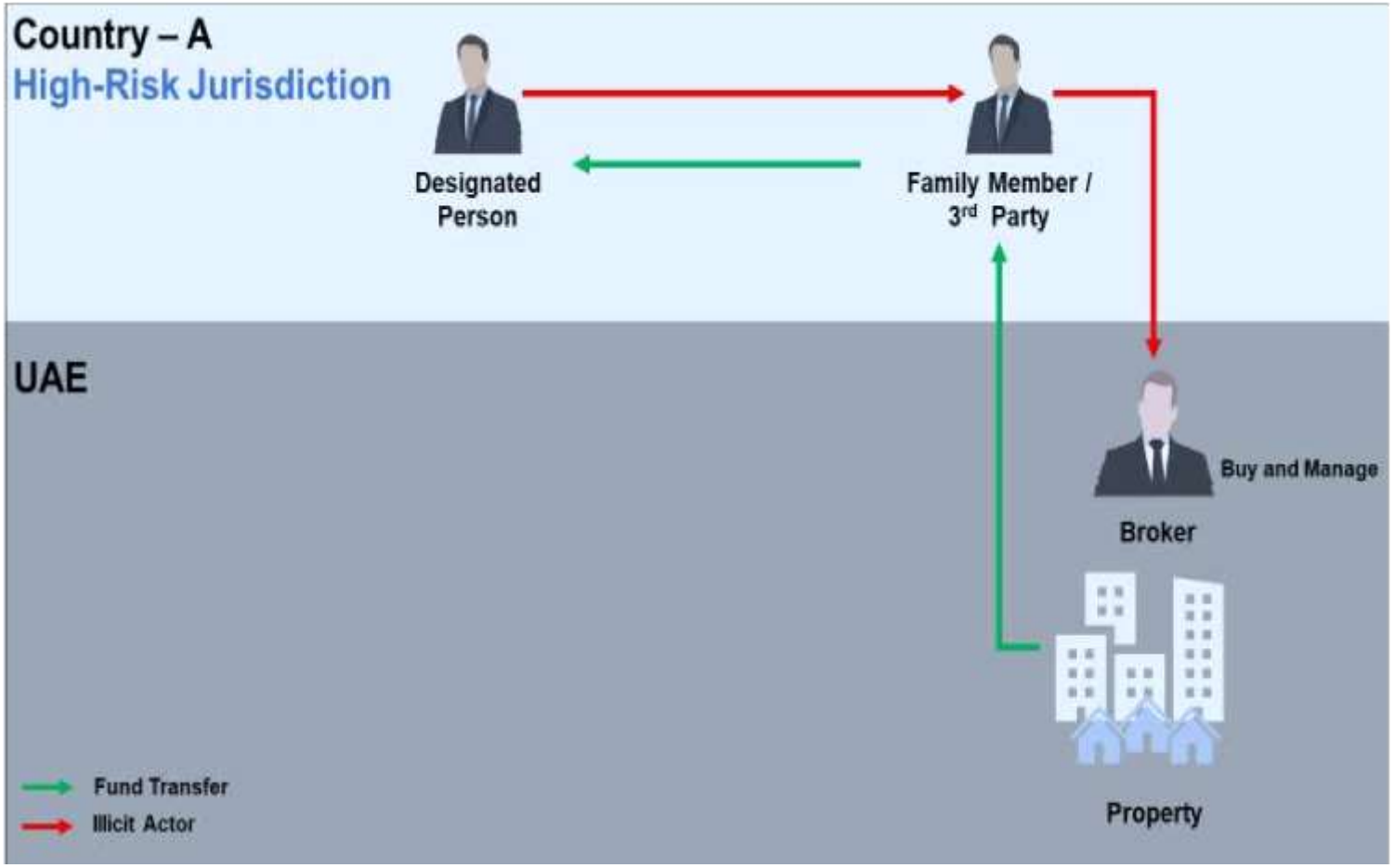


Second Pattern /Typology: Using third party or family member.

STR was submitted by a local bank that a real estate broker in UAE received remittances from high-risk jurisdictions.

The Investigation revealed that the remitter was acting on behalf of a Sanctioned family member to purchase properties in the UAE.

The proceeds of the properties were then returned to the family member residing in Country A who is working on behalf of a sanctioned individual.

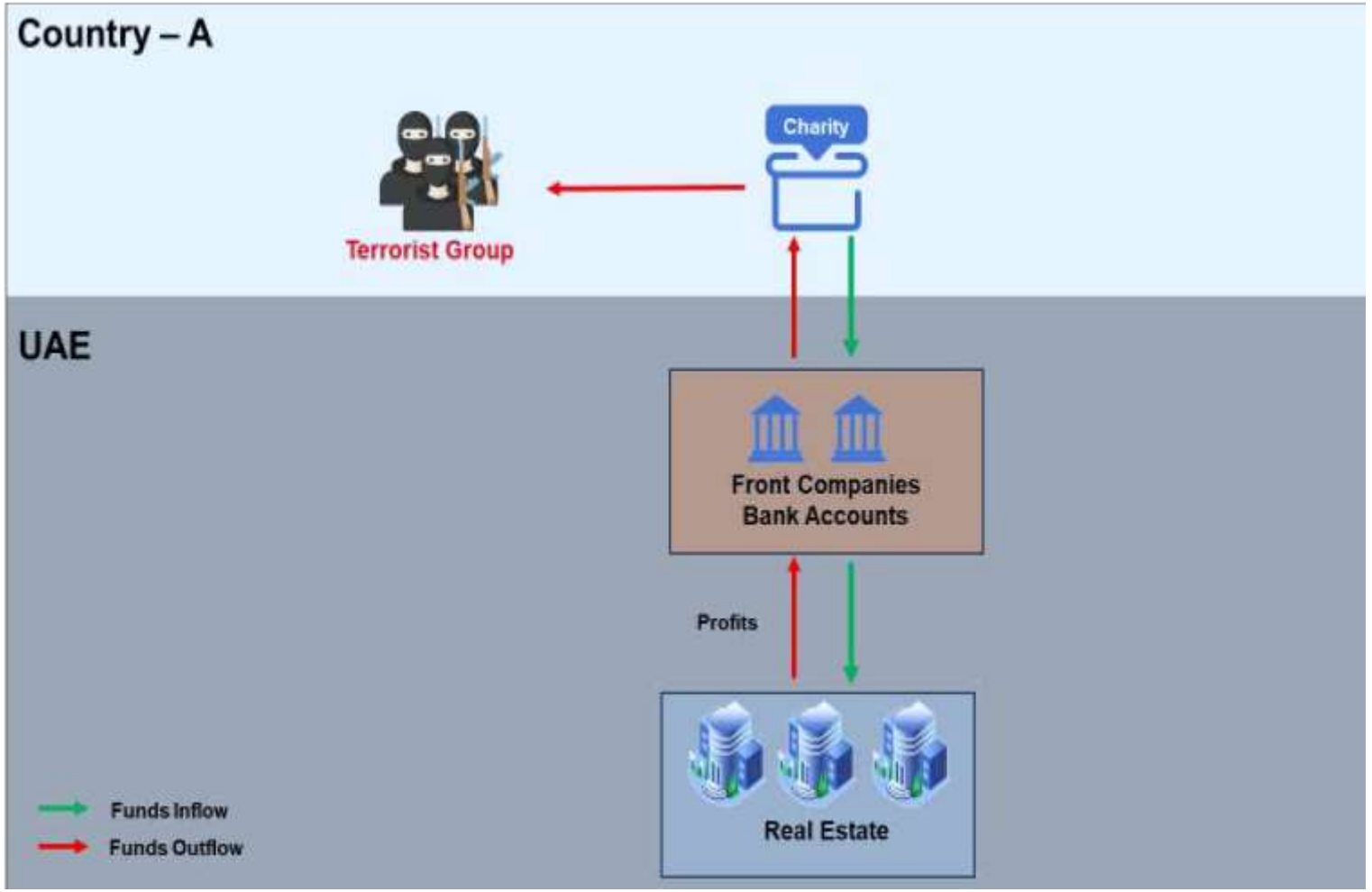


- **Third Pattern/Typology:** The Misuse of NPOs

STR was submitted by a bank on transfers from/to NPO located in country A.

The NPO was misused to operate as a front company on behalf of terrorist organizations where the holds bank accounts and purchases real estate on behalf of the terrorist organization.

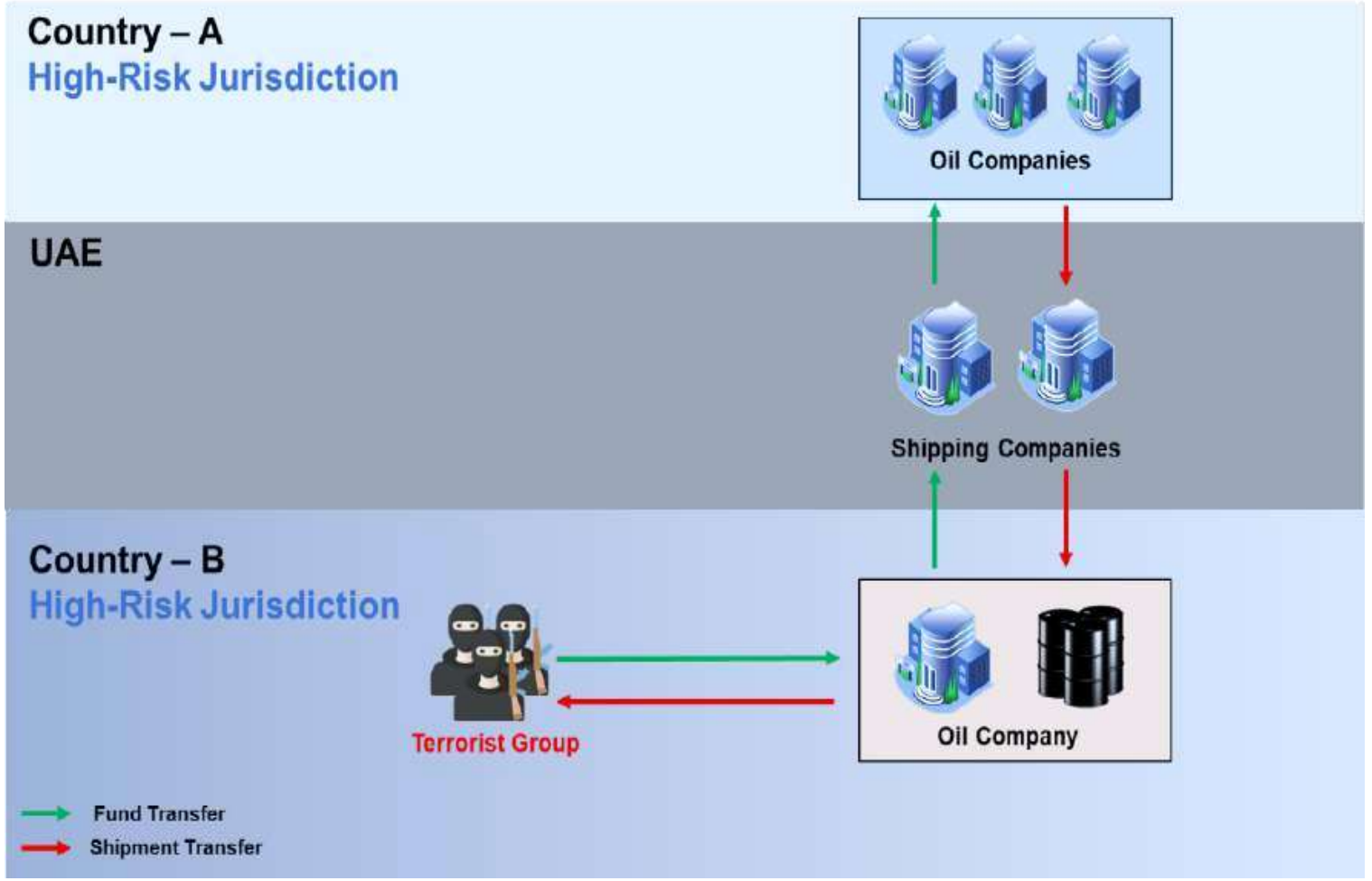
A Hawaladar was used to remit profits of the real estate to the NPO in country A that supports sanctioned terrorist group.



Fourth Pattern/Typology: Forged Documents and Bills

Intelligence information on the maritime industry found that illicit actors were forging documents and using the UAE as a transit point to ship oil for the benefit of sanctioned terrorist group located in country B.

The investigation revealed that the proceeds of selling the oil were transferred to country A through the shipping companies in the UAE.

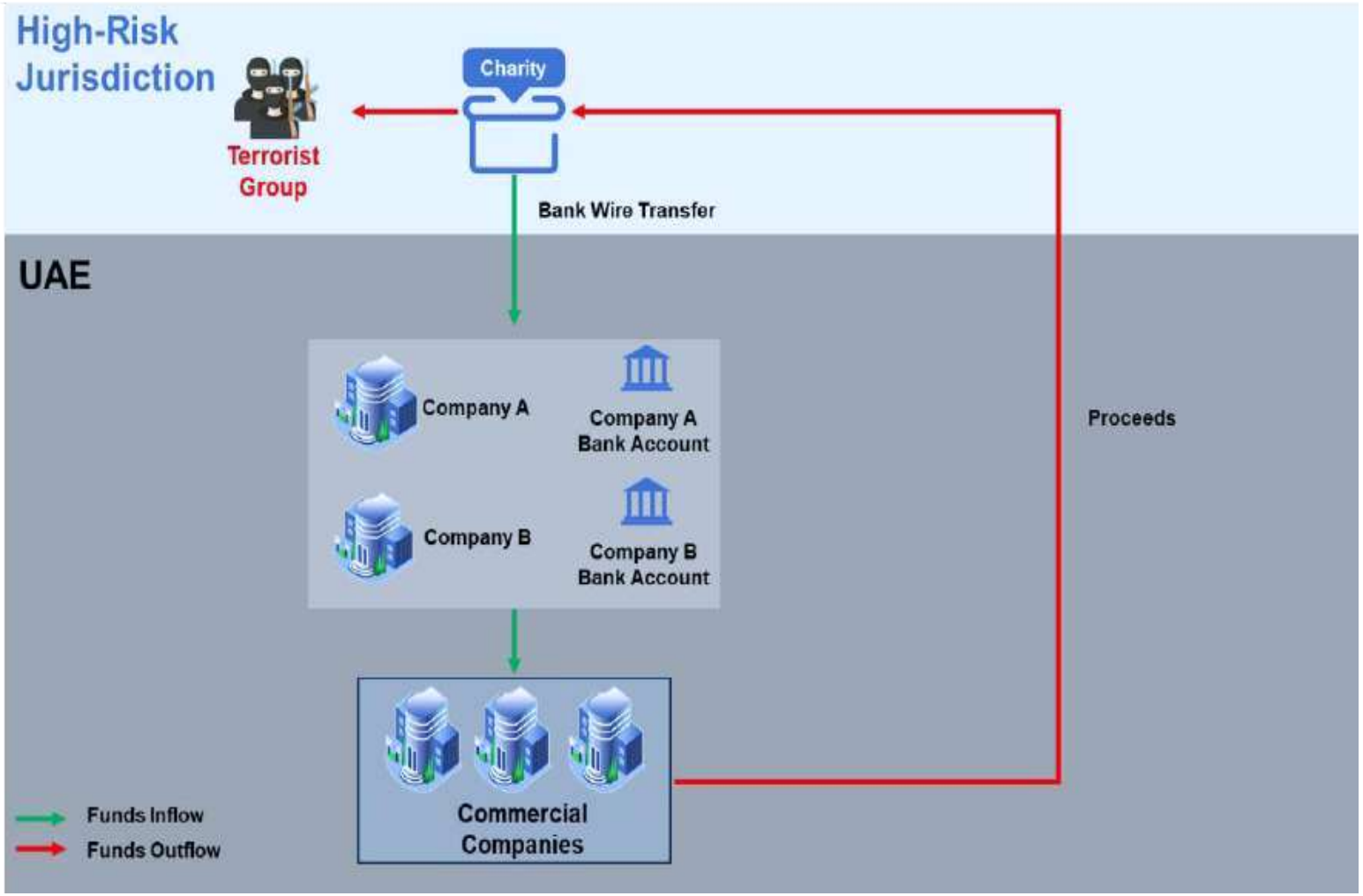


Fifth Pattern/Typology: Using Front Companies

A local bank filed STR regarding incoming wire transfers from a high-risk jurisdiction to a front company's bank accounts in the UAE.

The front companies used the funds received to invest in commercial companies.

The return of the investments were transferred to an NPO controlled by terrorist groups.



Targeted Financial Sanctions
Proliferation Financing Patterns & Typologies

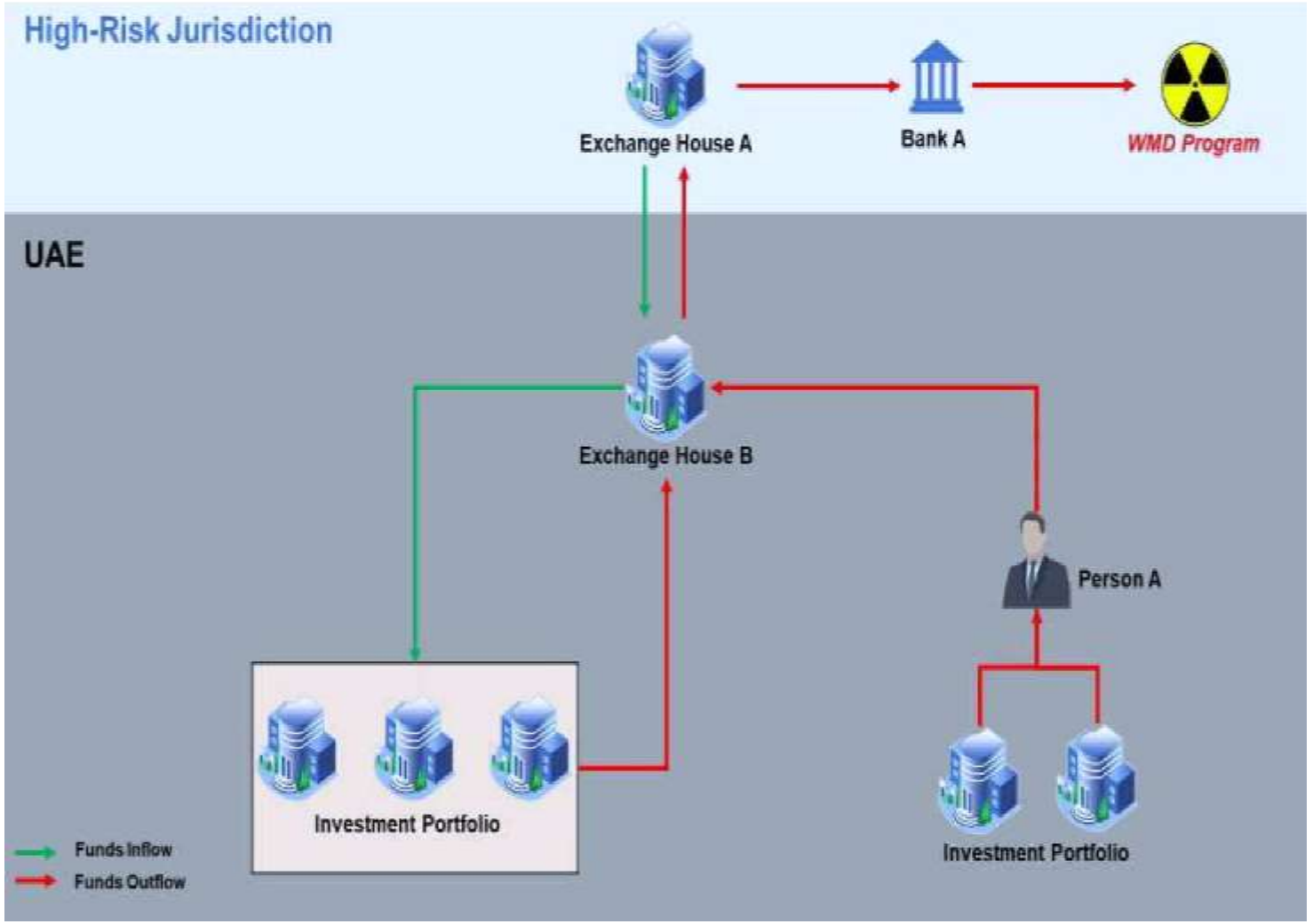
First Pattern/Typology: The use of financial system

A local exchange house B submitted STR on suspicious behavior of multiple high value inward/outward transactions conducted by 5 different companies working as investment portfolios.

Two of the five companies were obtaining funding from investment portfolios and transferring the funds to exchange house B via person A who manages the two investments.

The other three investment portfolios transferred the funds directly to exchange house B to ultimately move them to the high-risk jurisdiction.

Investigations revealed that exchange house A and bank A are controlled by an entity that supports WMD programs.

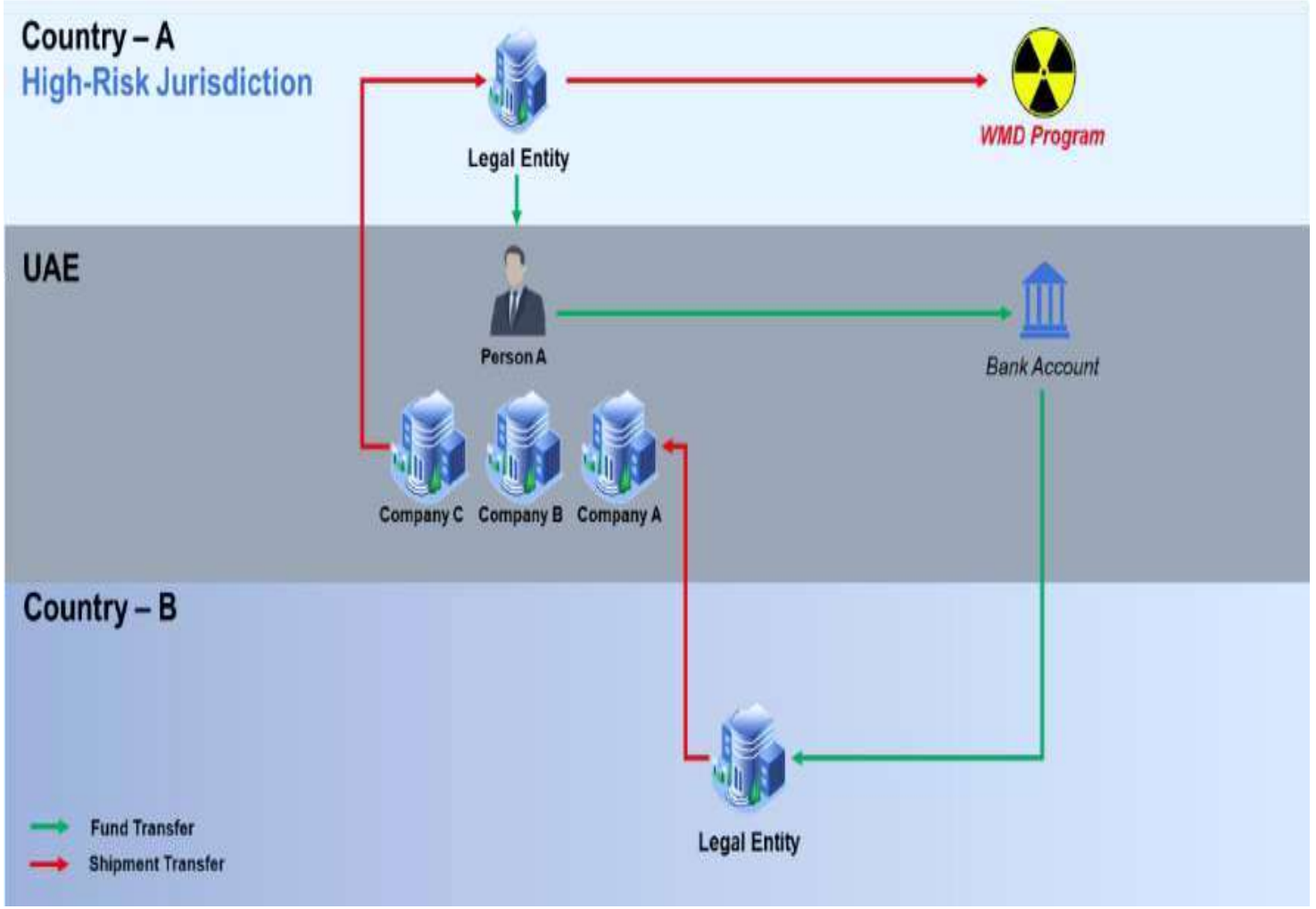


Second Pattern/Typology: The Shipment of Dual-use Items

An export control entity identified that the technical description of an electronic tool was manipulated where the item specification was slightly below the threshold to be considered controlled during the permit request by company A.

The investigation revealed that person A owns three companies and uses them for transhipment of the electronic item. Additionally, he received money from a legal entity in high-risk jurisdictions to deliver the electronic item.

Furthermore, the investigation led to uncover transactions related to the sale, shipment, and export of dual use goods to a legal entity in a high-risk jurisdiction that supports WMD program.



Chapter 2: Classification of TFS Cases for the Period (2022 – 2023)

Based on Reporting Entity

The table below lists the 3 main reporting entities that contributed to building the 10 cases analyzed in this period. It is noticed from the table below that the highest reports came from the banking sector submitting STRs which then led to identifying TF/PF activities or sanction evasion from the UN Sanctions List and Local Terrorist List.

Furthermore, Exchange Houses come in second position proving the contribution of the private sector in uncovering TFS related issues.

Reporting Entity	*Number*
Bank	6
Exchange House	3
DPMS	1

Based on Suspicion Identified

The table below lists the 4 types of suspicions which the cases were based on. As shown in the results below, the highest type of suspicion for reporting methods used by criminals to disguise their support of TF/PF activities were mainly through establishing front companies and high-volume transfers to high-risk jurisdictions. A slight difference from chapter 1 where suspicions were from front companies in the first place and shipment of dual use items in the second place. These results show that TF and PF actors are trying alternative methods to achieve their goals.

Type of Suspicion	*Number*
Front Company to support TF/PF Group	5
High Volume to / from high-risk jurisdiction	3
Inconsistencies between annual income and business activity	1
Accounts belong to designated person	1

Based on Tools and Instruments Used

The table below lists the 4 tools and instruments used by criminals to transport funds and other assets to assist TF activities or PF programs. The most common tools and instruments used by criminals are, transfers via bank or exchange house. The table also shows that forging documents and bills still pose a high risk which was identified in the previous period

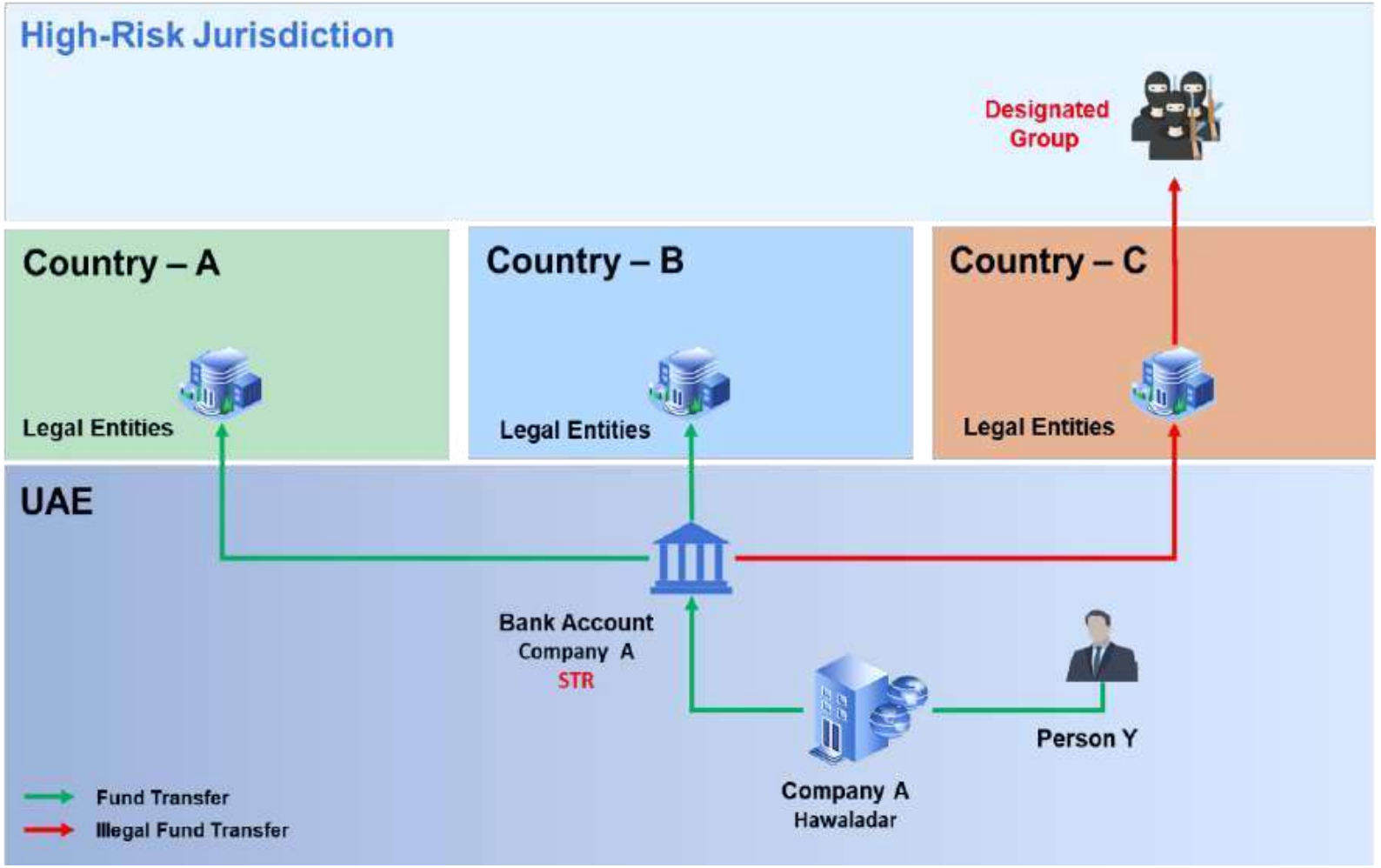
Tool or Instrument	*Number*
Wire Transfer via Banks	3
Transfer via Exchange House	3
Transfers via Hawala-Dar	2
Forge Documents and Bills	2

Targeted Financial Sanctions
Terrorist Financing Patterns & Typologies

First Pattern/Typology: Front Companies for TF Activities

Suspicious transaction report was filed by local bank regarding person Y who used his company's bank accounts as a hawaladar to transfer funds to a conflict zone.

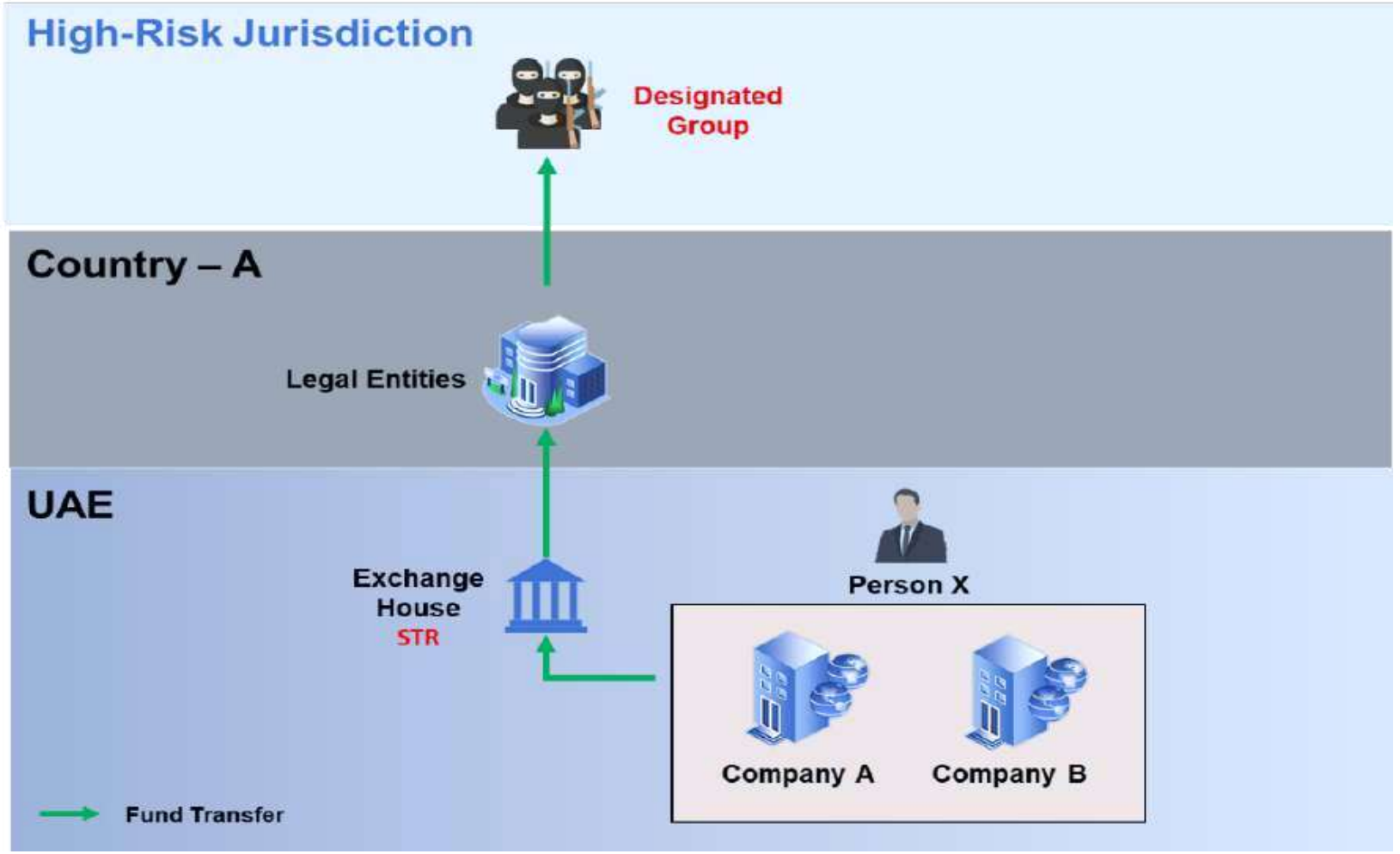
The investigation revealed transfers were conducted to three countries country A, country B, country C. Where it was confirmed that funds that passed through country C reached a terrorist group.



Second Pattern/Typology: High Volume Transfer to High-Risk Jurisdiction

An STR is submitted by an exchange house when person X transfers money to country A, a high-risk jurisdiction, through the exchange house using large amounts of cash.

Investigations revealed that person X established and managed two companies, company A and B, for the sake of raising funds and supporting terrorist groups in the high-risk jurisdiction.



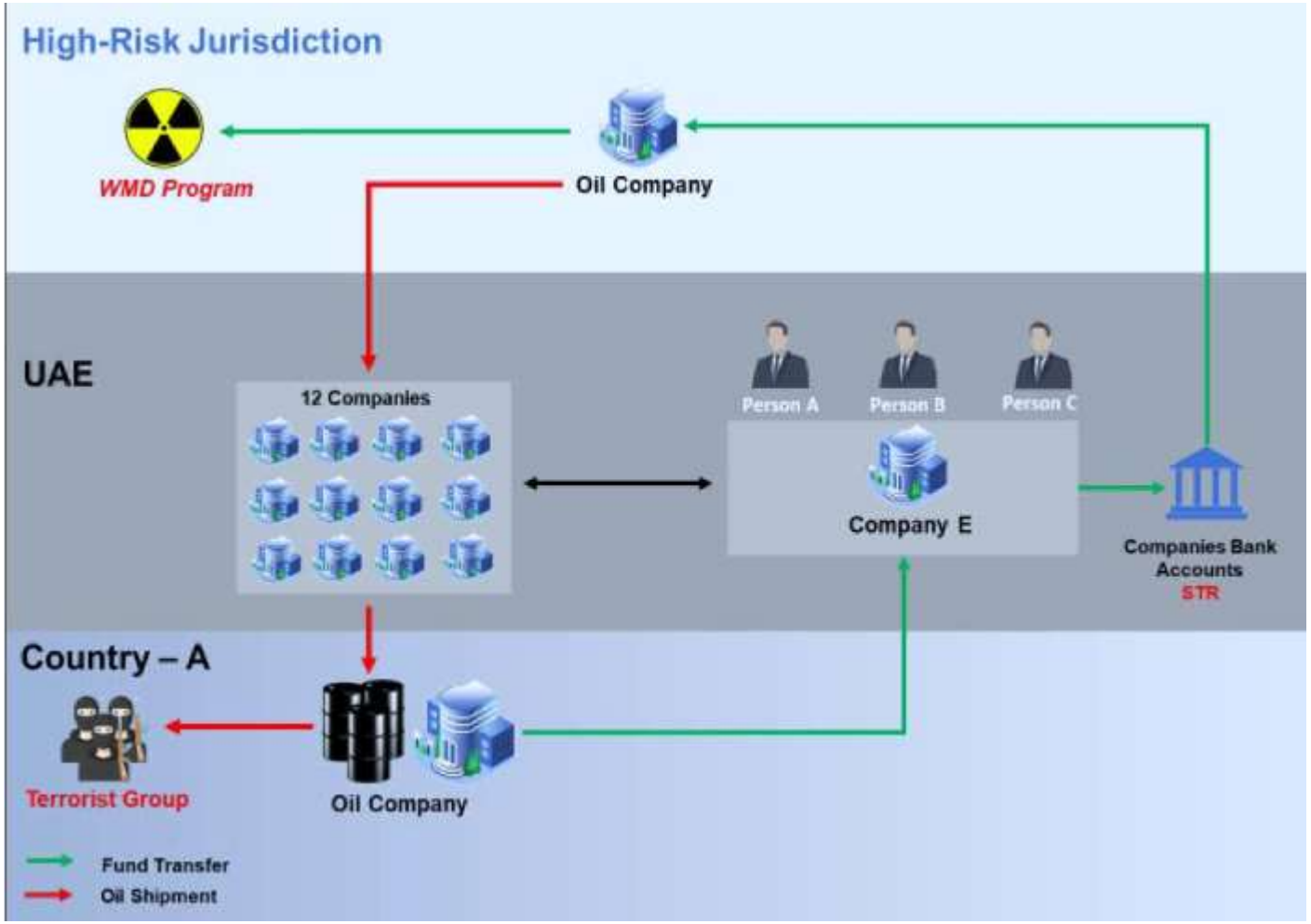
Targeted Financial Sanctions
Proliferation Financing Patterns & Typologies

First Pattern/Typology: Oil Trade

This case study was triggered through an STR from a local bank suspecting the multiple high-volume transactions occurring between company E and another 12 companies in the UAE.

Person A along with two other individuals established a front company (Company E) operating in ship supply and trade of oil and gas. Company E utilized 12 affiliated companies operating in the same sector to ship oil from high-risk jurisdiction to country A using the UAE as a transhipment.

The proceeds of selling the oil to the Terrorist group was sent back through the UAE financial system to support the WMD program.

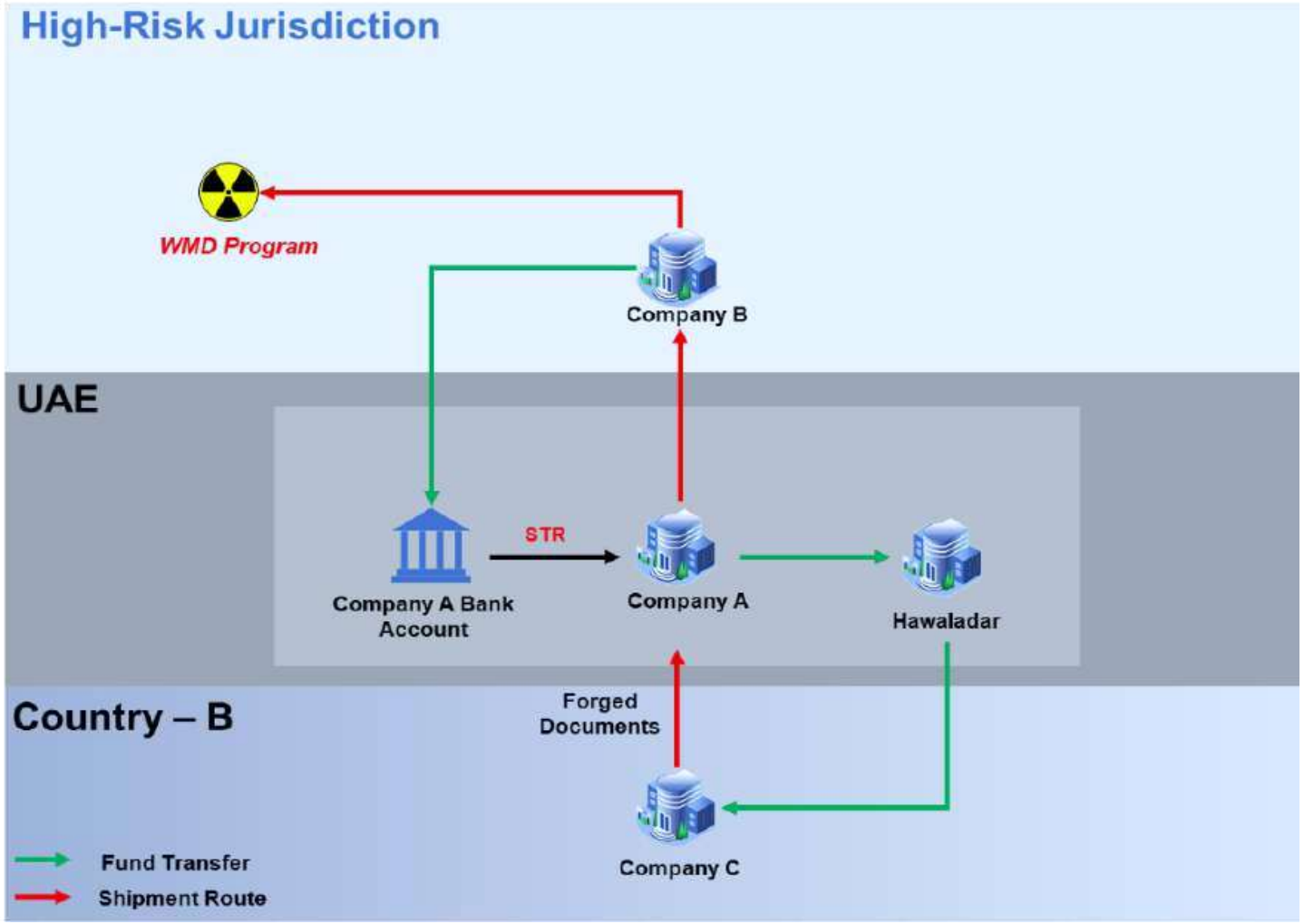


Second Pattern/Typology: Forged Documents and Bills

STR was received from a local bank on company A suspecting the high-volume transfers received from company B, which is located in a high-risk jurisdiction, intended to purchase goods. The declared value of goods purchased was significantly lower than the actual market price.

The investigation revealed that company A forged documents and falsified the end destination so they could hide the origin and nature of the goods to re- export them to a high-risk jurisdiction.

The investigation also uncovered that fund received from company B were transferred to company C via hawaladar to purchase devices that produce missiles and other WMD related systems.



Highlights and Conclusion

1. Through this document it was noticed that over the years illicit actors have diversified their TF, PF and sanction evading methods and techniques. Therefore FIs, DNFBPs and VASPs have to be constantly on the lookout for innovations in supporting illegal activities and sanctions evasion methods used by criminals to finance terrorist groups or WMD programs.

2. It was also noticed that the involvement of the private sector played a crucial role in identifying sanction evasion activities by reporting cases based on suspicions associated with their relevant sector risks. STRs that contained high quality information assisted the LEAs to build successful cases that later resulted in tracing and seizing funds related to TF/PF activities and eventually resulting in the disruption of illicit financial networks.

3. Through this document, the EOCN aims to provide a clear reference for the first lines of defence across all sectors aiming to disrupt illicit financial networks related to TFS regimes. The impact and importance of proactive information sharing by the private sector is demonstrated in more details in the "Targeted Financial Sanctions Implementation Guideline" published by the EOCN.

Thanks!