Study of Typologies of Financing of WMD Proliferation

Final Report

13 October 2017

Jonathan Brewer

For queries regarding distribution or other issues, please contact: alpha@kcl.ac.uk.

Project Alpha

Centre for Science and Security Studies

King's College London

Strand

London WC2R 2LS

United Kingdom

Telephone: +44 207 848 1342

Version 1, October 2017

Executive Summary

This report describes typologies of financing the proliferation of weapons of mass destruction (WMD).

Disrupting the financing of proliferation (FoP) is potentially a key tool to combat state-sponsored WMD programs. However, detecting FoP is difficult. The majority of governments and financial institutions are unclear about what FoP looks like and how to identify it. The tool is rarely exploited.

The most comprehensive study of FoP to date was published by the Financial Action Task Force (FATF) in 2008.[1] This includes a list of 20 "indicators of possible proliferation financing," including for example transactions connected with designated individuals or entities or with countries of proliferation concern. Since then, more information has become available, particularly related to the proliferation programs of DPRK and Iran, as well as other countries.

Project Alpha of King's College London carried out an analysis of data relating to DPRK, Iran, Syria, Pakistan and India provided by governments and financial institutions, contained in records of judicial proceedings and in UN Panel reports, and in media reports. The analyses are summarized in the form of 60 case studies. They enable identification of common elements between networks set up to finance proliferation or to circumvent financial sanctions, and of ways networks may mutate in response to sanctions.

Based on these cases, the indicators in the FATF 2008 Report have been modified and categorized as "potentially highly indicative," "potentially moderately indicative" or "potentially poorly indicative" of FoP. The study identified additional possible indicators, including transactions involving individuals connected with countries of proliferation concern, the use of cash, the involvement of small trading or intermediary companies, unlicensed money-remittance businesses, businesses linked in some way (for example, the same physical or IP address or whose activities are coordinated), the involvement of universities in countries of proliferation concern, non-specific descriptions of goods or materials, the involvement of goods and materials subject to export controls, fake or fraudulent documentation, and the use of personal bank accounts.

By illustrating different types of FoP, the case studies are intended to support the work of governments and financial institutions worldwide in identifying FoP. They are intended to facilitate FoP risk assessments, to support regulators in providing guidance to financial institutions and to support financial institutions in complying with sanctions or other WMD controls.

Above all, combating proliferation of WMD by identifying and disrupting the financing is most likely to be successful when governments and the private sector cooperate and

[1] Report on Proliferation Financing, 2008 (http://www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html).

coordinate in sharing information. It is hoped that the FoP case studies included in this report will help this process.

Acknowledgments

Several government authorities devoted significant resources to providing information for this study, including those of Sweden, Belgium, Luxembourg, Spain, the Netherlands, the United Kingdom, Australia, Canada, Norway (including the Norwegian Police Security Service (PST)), and others. Several financial institutions also did so.

The author is grateful to all who contributed.

Early versions or excerpts of the report benefited greatly from comments provided by Aaron Arnold, Tom Neylan, Graham Finding, Kerri-Ann Bent, Ian Stewart, Andrea Viski, John Druce, Stephan Blanke, and others. Editing and additional comments were provided by Alexandra Dzero and Christina Krawec. Glenn Anderson turned text into diagrams, with assistance from Maila Beniera.

This study was funded between August 2016 and July 2017 by the Export Control and Related Border Security (EXBS) program of the US Department of State, under Award No. S-LMAQM-16-GR-1138.

Contents

Part One

Background

The UN Security Council has put in place a framework of measures to prevent the financing of proliferation (FoP) with the implementation of resolution 1540 (2004) on non-proliferation, 2231 (2015) on Iran and 1718 (2006) and seven successor sanctions resolutions on DPRK. These resolutions include requirements on UN member states to implement controls on financial transactions, and on financing of goods and services related to the proliferation of nuclear, chemical and biological weapons and their means of delivery (WMD) together with related goods and materials.[2]

The Financial Action Task Force (FATF) has also introduced standards for implementing targeted financial sanctions imposed under the UN Security Council resolutions on Iran and DPRK.[3] In addition, many states have introduced national measures against FoP.

However, identifying and tracking FoP is difficult because most transactions occur within normal business transaction pathways. Most states, as well as banks, other financial institutions and designated non-financial businesses and persons (all hereafter referred to as "FIs") are unclear about what constitutes FoP and how to recognize it.[4] This is potentially serious because identification of proliferation-related financial transactions may enable the use of financial tools to combat WMD proliferation. Investigations into financial transactions may provide information on identities and activities of entities or individuals, perhaps based overseas. Financial information may be used to initiate an investigation, prosecute an offender or disrupt networks by seizing funds, for example.

By default, FoP appears to be given low priority.[5] To financial authorities, FoP may seem less of a threat to national financial systems than better-understood risks from other forms of financial crime such as narcotics-related money laundering (ML). Authorities responsible for counter-proliferation may focus on more familiar methods for stopping goods and materials such as export controls or interdictions of shipments, rather than on disruption of financial support channels. In addition, FoP may be regarded as less of an immediate threat to national security than terrorist financing.

The low priority assigned by most states to FoP also reflects, at least in part, a lack of

---

[2] Throughout this report, the terms "weapons of mass destruction" or "WMD" are understood to include related goods and materials.

[3] Key financial elements of the UN resolutions, and relevant FATF standards, are described in Annex 1.

[4] Author's observations based on discussions with officials of UN Member States and FIs both as a member of the UN Panel on Iran created pursuant to resolution 1929 (2010) and while conducting research for this report; Emil Dall, Andrea Berger and Tom Keatinge, Out of Sights, Out of Mind? A Review of Efforts to Counter Proliferation Finance, RUSI Whitehall Report 3-16, June 2016; Report on Workshop on Trade Finance and Proliferation Finance: Mitigating the Risk, 20 June 2017. Available online at: http://projectalpha.eu/trade-finance-and-proliferation-finance-mitigating-the-risks/.

[5] Ibid.

information about its scale. Because most regulators do not require reporting on proliferation financing, most FIs do not look for it.[6] Some states may receive reporting through domestic investigations carried out by law enforcement, customs services or intelligence agencies, or through international liaison channels, but the majority of governments do not. Authorities may as a result lack the necessary knowledge or expertise to carry out FoP risk assessments. They may lack legal, regulatory and interagency frameworks to enforce obligations inherent in UN Security Council sanctions. They may also fail to ensure domestic departments and agencies coordinate work and share information, and they may be unable to act on information shared by partner countries.

A comprehensive report on the threat of proliferation financing and options to counter the threat was published by the Financial Action Task Force (FATF) in 2008.[7] This was based on FATF members' responses to a proliferation financing questionnaire, and meetings with experts and with the private sector. The report concluded that it was not possible to identify any single financial pattern uniquely associated with proliferation financing, but it listed twenty indicators of possible proliferation financing (these are listed in Annex 2).[8] Many of the indicators on FATF's list are evasion techniques and may also be indicators for other types of trade-based financial crime.[9] Some jurisdictions have published variations on this list, or specific advisories,[10] although the FATF list remains authoritative.

[6] In some jurisdictions, the US for example, financial transactions connected with a property involved in unlawful activity are categorized as ML. Statistics relating to cases of financing of unlawful exports of proliferation–related items, for example, would be recorded as ML rather than FoP, which may be an additional factor to be considered when conducting FoP risk assessments.

[7] The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. FATF's Proliferation Financing Report of 2008 can be accessed at http://www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html.

[8] Annex 1 of FATF's 2008 Report.

[9] See, for example, Appendix F of the Bank Secrecy Act Anti-Money Laundering Examination Manual, Federal Financial Institutions Examination Council, particularly the red flags for Trade Finance, (https://www.ffiec.gov/bsa_aml_infobase/pages_ manual/olm_106.htm)' and The Wolfsberg Group, ICC and BAFT Trade Finance Principles 2017 (http://www.wolfsberg-principles.com/pdf/home/Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017.pdf).

[10] For example, Guidance on Proliferation and Proliferation Financing, Jersey Financial Services Commission, Oct 2011; Advisories published by US Department of the Treasury.

Definition of Financing of Proliferation

A lack of understanding of FoP is exacerbated by the lack of a universally-recognized definition. For the purposes of this report, FATF's working definition is adopted:[11]

> Proliferation financing refers to: the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.[12]

This definition is comprehensive in terms of coverage of the range of possible relevant WMD-related activities, but the reference to "… *related materials (including both technologies and dual use goods used for non-legitimate purposes),"* perhaps needs more emphasis. Most government-led counter-proliferation actions conducted today are directed at goods and materials related to WMD programs, not finished weapons systems. Risk mitigation systems or compliance programs based solely on identification of finished weapons systems will miss this crucial point.

Combating Proliferation of WMD

The important role that countering proliferation financing can play in combating proliferation has been recognized for many years. UN Security Council resolution 1540 (2004) requires member states to implement measures to prevent terrorists accessing finance to use WMDs, or financing of WMD export or trans-shipment through their territory. The 2005 G8 meeting at Gleneagles called for "… enhanced efforts to combat proliferation networks and illicit financial flows by developing, on an appropriate legal basis, co-operative procedures to identify, track and freeze relevant financial transactions and assets."[13] The Proliferation Security Initiative set up a working group on the subject in 2015. The FATF President's December 2016 statement to the UN Security Council noted that financial intelligence provided advance warning of attempts to illegally transfer sensitive goods and materials, that financial investigation can be used to analyze proliferation networks and identify facilitators, and that many countries neither understand the risks of FoP nor fully exploit the opportunities financial intelligence provides to counter proliferation.[14]

---

[11] The FATF definition is not agreed by all FATF members and so remains provisional.

[12] Combating Proliferation Financing – A Status Report on Policy Development and Consultation, February 2010 (http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf).

[13] The G8 Statement on Non-Proliferation, Gleneagles Summit, 6-8 July 2005.

[14] FATF President Juan Manuel Vega-Serrano's remarks at the meeting of the UN Security Council, December 15, 2016, http://www.fatf-gafi.org/publications/fatfgeneral/documents/speech-vega-serrano-

Study Methodology

The study addressed the following: What does FoP by state-sponsored WMD programs currently look like; can characteristic typologies[15] be identified; and can the FATF 2008 indicators be updated? Initial results of the study were recorded in an Interim Report dated 5 February 2017.[16] This Final Report, which incorporates those earlier results, describes 60 case studies.

No attempt was made to identify typologies of financing of WMD or related goods and materials by terrorist organizations. Much work has been carried out by the UN Security Council Committee on ISIL (Da'esh) and Al-Qaida, by FATF and by others, on typologies of terrorist financing (TF). This report does not try to duplicate this.

There may be a degree of overlap between typologies of FoP and of procurement of conventional weapons, or of typologies associated with criminal activities such as money laundering. Much work has been carried out by FATF and others on such typologies.

Sources of data

The results and conclusions of the study are based primarily on collation and analysis of financial information provided by states and by FIs. Such data may be held by a variety of government departments and agencies, including financial intelligence units, Ministries of Finance, Ministries of Defense, customs services, security and intelligence agencies, and others. In FIs, such data may be held by financial intelligence units, compliance departments, units dedicated to investigation of suspicious transactions or equivalent bodies.

The study also analyzed financial material in UN Panel reports on Iran and on DPRK, and in media reporting, as well as in judicial proceedings relating to WMD (for example cases in Sweden, Singapore, and the US).[17]

The information analyzed fell roughly into two categories: cases in which WMD was clearly involved (for example transfers of WMD or related materials took place, or end-

---

joint-un-fatf-meeting-dec2016.html.

[15] For example, patterns involving different sectors (e.g., banks, money remitters, hawala), channels, products or services, entities, front and shell companies, circumvention techniques; trade finance and open account transactions, overlap with money laundering and terrorist financing; similarities and differences between proliferation finance with respect to nuclear, chemical or biological WMD.

[16] Study of Typologies of Financing of Proliferation Interim Report 5 February 2017 (https://projectalpha.eu/study-of-wmd-proliferation-financing-typologies/).

[17] See list of cases at Annex 5. These were selected on the basis that they contained sufficient financial information to be able to illuminate FoP mechanisms. US Treasury Department Office of Foreign Assets Control cases are listed at https://www.treasury.gov/resource-center/Pages/default.aspx, US Department of Justice records were accessed through a subscription-based repository of US courts documents: Public Access to Court Electronic Records (https://www.pacer.gov/).

users were involved in WMD), and cases that were possibly attempts to circumvent wide-ranging financial sanctions or other controls in order to carry out legitimate commerce. Cases in this second category did not enable a determination that WMD or related materials were specifically involved, but are included because the typologies could also be used for FoP.

The study focused on the proliferation programs of DPRK, Syria, Iran, Pakistan and India. These countries were chosen either because they have active WMD programs but as non-members are not bound by Non-Proliferation Treaty safeguards, or they are subject to UN Security Council resolutions or unilateral sanctions regarding previous or current WMD programs. On a few occasions, the study was provided with information relating to procurement by other countries even though WMD was not involved. Such information has been included for purposes of comparison.

Data Collection

Financial intelligence data may be restricted or classified in both public and private institutions, may be governed by banking secrecy, data protection or other considerations, or may be sensitive for geopolitical reasons. Under these circumstances, the study decided that the appropriate way to start collecting information was to send exploratory emails to government officials or FI representatives. These emails outlined the study's objectives, methodology, procedures to safeguard sensitive data, and requested meetings or telephone calls. If agreed, substantive discussions with stakeholders took place in government offices of the countries concerned, or in offices of FIs.

Those authorities and FIs that agreed to support the study subsequently trawled through their data for information related to FoP. A descriptive text was then agreed. In most cases the text was stripped of names of individuals or entities, or other sensitive details.

Attributions were agreed on a case-by-case basis. In some cases a state did not wish to be identified for reasons of geopolitical or data sensitivity. In no case did an FI wish to be identified.

The individual texts agreed with stakeholders form the case studies found in Part Two. Titles and, in most cases, diagrams, have been added as well.[18] Key points are listed at the end of each case. Titles, diagrams and key points are based upon the study's analyses of the texts.

The study was conducted in accordance with King's College London standards on data security and ethics. In particular stakeholders were provided with a written guarantee regarding the use to be made of their data, their right to review them, to decide how they should be attributed, and to withdraw them if wished from the study's published

[18] Two case studies were provided with diagrams included.

reports.

The case studies are categorized in Part Two as follows: Cases relating to DPRK; cases relating to Syria; cases relating to Iran; cases relating to Pakistan, cases in which the proliferating state is not specified; cases of circumvention of WMD-related financial sanctions; and cases of circumvention of non-WMD-related financial sanctions. In each category, the cases are listed chronologically on the basis of information available.

Distinguishing FoP from other Financial Crimes

One of the most difficult aspects of identifying FoP is that goods and materials involved are often industrial items that, if not clearly identified as subject to some sort of controls, may appear innocuous to those involved in the supply chains and working in FIs. Furthermore, most of the twenty possible indicators identified by FATF are not in themselves uniquely associated with FoP. They could also reflect trade-based money laundering (ML), avoidance of tax or duty on shipments of goods, or other issues, such as incomplete trade documentation.

There may also be a lack of understanding of differences and similarities between FoP and ML and TF. A chart in Annex 3 highlights some of these comparisons, although, as pointed out above, typologies may overlap in some areas.

Analysis of Case Studies

The details underpinning each of the 60 case studies vary according to the quality and completeness of information provided by government authorities or FIs (and perhaps in turn accessible to them), or available in court documents, UN Panel reports or media reports. The majority of information received from authorities or FIs covered the last ten years. Most related to Iran and pre-dated the JCPOA agreed in July 2015.[19]

Taken as a whole, therefore, the case studies almost certainly do not present a complete picture of the way different proliferation-related financial networks currently operate. For example, although it is not a typology specific to any of the case studies, DPRK may carry out some procurement using barter.[20] Furthermore, there are no cases relating to India's WMD program and so this report provides no insights into financial typologies connected with Indian WMD procurement.[21]

---

[19] The Joint Comprehensive Plan of Action, enshrined in UN resolution 2231 (2015).

[20] For example, according to US court documents a Chinese trading company, Dandong Chengtai Trading Limited, was involved in barter exchanges of DPRK coal for commodities such as cell phones, luxury items, sugar, rubber, petroleum products and soybean oil. (United States District Court for the District of Columbia Verified Complaint for Forfeiture *In Rem* and Civil Complaint, case 1:17-cv-01706 filed 22 August 2017, particularly Figure 1). Such arrangements could in principle extend to WMD.

[21] Although according to officials of an EU state, procurement for the Indian ballistic missile program is difficult to distinguish from procurement for the Indian conventional weapons program; for example the

There are also relatively few cases relating to Pakistan's WMD programs. Those included here are characterized by financial networks that appear relatively less complicated than networks supporting DPRK's, Syria's or Iran's programs. For example, there are no cases of companies acting as money remittance businesses, perhaps reflecting the absence of UN or unilateral financial sanctions on Pakistan's programs.

Pakistani procurement networks generally operate through front companies that are relatively easy to identify. Different front companies may use the same address, same phone numbers, and same managers, and issue identical requests for quotations to multiple suppliers over long periods of time (six months to two years).[22] There is also some evidence that although procurement by Pakistan used to be relatively open, more covert methods have been adopted recently (including use of false end-user addresses).[23] This may reflect implementation of better controls within manufacturing countries on exports of goods or materials intended for Pakistan's programs.

Some cases provide insights into ways in which financial networks adapt to sanctions. For example, prior to 2011, the Syrian Scientific Studies and Research Center (SSRC), thought to be the main body developing Syria's chemical weapons and ballistic missile program, procured foreign goods and materials mainly through a series of shell companies managed by SSRC employees (case study 11). Following imposition of sanctions in 2011, the SSRC also used Syrian businessmen acting as brokers. Following further pressure from sanctions, designations and interdictions, SSRC directors in 2014/15 approached trusted Syrian businessmen with existing overseas business networks. The businessmen extended these networks to facilitate procurement from other countries, particularly China, so that the SSRC could more readily procure from Chinese suppliers.

Although over half of the case studies in FATF's 2008 Report involved trade financing such as letters of credit, such cases constitute a small minority in the current report (for example, cases 11 (Syria) and 19 & 33 (Iran)). This trend may possibly reflect developments in FoP. But it may also be a result of inadequate data or decreasing use of letters of credit in international trade.[24] Trade finance-related transactions offer more opportunities for due diligence regarding sanctions risk or FoP than do open account transactions (essentially wire transfers). The latter provide financial institutions relatively limited information against which to screen or monitor for suspicious indicators. [25] Some of the cases involving trade finance involved apparent

---

same end-user address might be used.

[22] Comments to the author by officials of an EU member state during the course of this study.

[23] Comments to the author by officials of a different EU state during the course of this study.

[24] Trade Finance: Developments and Issues, Committee on the Global Financial System Paper No 50, January 2014, Bank for International Settlements, although figure 41 of the ICC Banking Commission's paper "2017 Rethinking Trade Finance" suggests a decrease in use of letters of credit since 2009 of only about 10%.

[25] However, even where trade financing documentation is available, it appears that many financial institutions conduct checks focused primarily on credit risk: Dubai Financial Services Authority Trade

misappropriation of funds (for example cases 15, 56 & 57).

Most of the overseas elements of the networks described in Part 2 appeared to be based in a relatively small number of countries including United Arab Emirates (UAE), Turkey, Singapore, Malaysia, Hong Kong, China and Taiwan. This concentration may reflect factors such as proximity to the proliferating state, the facilities of a regional trade and banking hub, and perhaps a perception of lax export controls or lax regulation of the financial sector.

Table 1 compares financial network characteristics, although it is not intended to be a comprehensive analysis and nor are all characteristics common to all cases.

Finance Report 2016 (http://www.dfsa.ae/Documents/ThematicReviews/TF-Report-FINAL%20Eng%2012%20october%202016%20mid-res.pdf).

Table 1: FoP Characteristics Common to the Case Studies

Characteristics:	Illustrated in Case Number:
Involvement of front companies (either set up for the purpose, or adapted from an existing entity) or shell companies	DPRK cases: 3 & 4; Syria case: No 11; Iran cases: 19, 27 & 33; Pakistan cases: 47. State is not specified: 52
The presence of nationals of countries involved in proliferation-sensitive activity (sometimes dual nationals of their host country)	DPRK case: 8, Syria case: 11; Iran cases: 20, 22, 25, 26, 28 & 37; Pakistan cases: 47 & 48. State is not specified: 49
The involvement of small businesses, in particular brokers, distributors, or trading companies	DPRK cases: 1 & 5; Syria case: No 10; Iran cases: 17, 25, 26, 28, 32, 40, 41; Pakistan cases: 47 & 48. State is not specified: 50
The involvement of universities in countries involved in proliferation-sensitive activity, either to place orders or to fund procurement[26]	Iran cases: 30, 43 & 44
The use of distinct channels (involving different entities, may be geographically removed) to order and transfer proliferation-sensitive goods and materials, and to fund their procurement	DPRK cases: 4; Syria case: No 11; Iran cases: 14, 21, 26 & 37. State is not specified: 53
The involvement of companies whose products would be exempt from sanctions because they would fall into the category of "humanitarian" provisions, for example food distribution companies	DPRK case: 8; Iran cases: 15, 23 & 27
Trade or payment documentation includes bland or non-specific descriptions of goods and materials, or the purpose of the financial transactions	Syria case: 10; Iran: 26
Persistence and resilience, despite evidence that authorities were aware of illicit activity	DPRK cases: 1; Syria cases: 11; Iran cases: 16, 19, 23 & 38
Elaborate overseas networks, based either on existing networks or constructed for the purpose	DPRK cases: 3 & 7; Syria case: 11; Iran cases: 14, 27 & 39
The use of personal bank or credit card accounts to procure proliferation-sensitive goods and materials	DPRK case: 8; Iran cases: 28, 43 & 44; Pakistan networks: 47

[26] According to the authorities of a European state, universities play an important role in procurement of dual-use goods by China, Russia, Iran and possibly Pakistan.

Companies acting as remittance businesses by processing financial transactions on behalf of companies in sanctioned countries	DPRK cases: 3 & 5; Iran cases: 17 & 35
The use of cash to finance trade[27]	DPRK cases: 1, 3, 7 & 8; Syria cases: 11; Iran cases: 25, 41 & 42
Networks used for two-way trade	DPRK case: 1; Iran cases: 16 & 23
Networks which appear to be to some extent self-financing (i.e. entities within them generate their own revenue)	DPRK cases: 6 & 8; Iran case: No 24
Multiple front companies make payments for a single invoice	DPRK case: 7; Iran case: 26
The companies involved are doing business that is not their normal business	DPRK case: 8; Iran cases: 13, 25, 28 & 46
The use of a "ledger" accounting system (also referred to as book-to-book), to facilitate circumvention of financial sanctions by related companies.	DPRK cases: 3, 7 & 8; Syria case: 11; Iran case: 45
The use of trade finance mechanisms.	Syria cases: 11; Iran cases: 19, 33 & 56

[27] Para 194(b) of UN Panel on Iran Final Report of 2012 (S/2012/395), Para 146 and FN 33 of UN Panel on Iran Final Report of 2013 (S/2013/331).

FATF's 2008 FoP Typologies – Updated and Revised

Table 2 below sets out proposed modifications to the indicators in FATF's 2008 report.

The analysis was carried out in two stages. First, each of the case studies was compared with the FATF indicators, and these were then modified if necessary by redrafting or adding detail. In some cases new possible indicators were identified. Additional information in UN Panel reports was taken into account during this process. A revised list of possible indicators was then compiled.

Second, the new list was divided into three categories:

1. Trade-related transactions potentially highly indicative of financing of proliferation (as opposed to money laundering, terrorist financing or other forms of financial crime). These indicators include specific references to countries of WMD concern, individuals or entities designated under WMD sanctions, dual-use goods, or other WMD factors. One or more of the indicators in this category characterized the majority of cases in this report, but they could also reflect legitimate trade;
2. Trade-related transactions that are moderately indicative of financing of proliferation. One or more of these indicators characterized many of the cases in this report. They could reflect other forms of trade-based financial crime, and also legitimate trade;
3. Trade-related transactions that are potentially only poorly indicative of financing of proliferation. These are indicators that could equally reflect a number of different types of trade-based financial crime as well as legitimate trade. By comparison with the two categories above, these indicators are seen less frequently in the case studies.

Table 2 lists the modified possible indicators and examples of case studies to which they contribute, in whole or in part.

Table 2: Indicators of Possible Financing of Proliferation

Typology	Indicator	The indicator is based on:	Case Examples	Could also be:
Trade-related transactions potentially highly indicative of FoP				
A1	Involvement of individuals or entities in foreign country of proliferation concern	FATF 2008 Report (Typology 1)	Multiple	Normal trade
A2	Involvement of individuals or entities in foreign country of diversion concern (such as a neighboring country or country actively engaged with country of proliferation concern)	FATF 2008 Report (Typology 2)	3 & 7 (DPRK), 10 & 11 (Syria), 23 & 33 (Iran), 47 (Pakistan), 54 (state not specified)	Normal trade
A3	Individuals or entities involved (for example, customers, counterparties, end-users), or their details (such as addresses or telephone numbers), are similar to, or may be connected to, parties listed at the time under WMD-related sanctions or export-control regimes, or they have a history of involvement in export control contraventions	FATF 2008 Report (Typology 14)	7 (DPRK), 11 (Syria), 16 & 21 (Iran), 51 & 54 (state not specified)	Normal trade
A4	Presence of items controlled under WMD export control regimes[28] or national control regimes	This report	1 (DPRK), 26, 40 & 43 (Iran), 47 & 48 (Pakistan), 53 (state not specified)	Legitimate trade (if licensed)
A5	Activity that does not match customers' or counterparties business profiles, or end-user information does not match end-user's business profile	FATF 2008 Report (Typology 10)	8 (DPRK), 13, 25, 28 & 46 (Iran)	Normal trade

[28] The relevant WMD export control regimes are the Nuclear Suppliers Group (NSG), Missile Technology Control Regime (MTCR), and the Australia Group (AG).

A6	End-user is not identified; for example a freight forwarding firm or bank is listed as consignee or final destination	FATF 2008 Report (Typology 18)	41 (Iran), UN Panel on Iran, [29] UK authorities[30]	Normal trade
A7	Involvement of an individual connected with a country of proliferation concern (for example a dual-national); may be dealing with complex equipment for which he/she lacks technical background [31]	This report	8 (DPRK), 11 (Syria), 20, 22, 25, 26, 28, 37 & 44 (Iran), 47 (Pakistan), 49 & 53 (state not specified), UN Panel on Iran[32]	Normal trade
A8	An order for goods is placed by firms or individuals from foreign countries other than the country of the stated or suspected end-user	FATF 2008 Report (Typology 11)	11 (Syria), 14, 19, 28 39 & 45 (Iran), 49 (state not specified)[33]	Normal trading activity (brokering)[34]
A9	Use of cash in transactions for industrial items	This report	1, 3 & 8 (DPRK), 11 (Syria), 25, 41 & 42 (Iran)	Rare for legitimate trade transactions
A10	Transaction involves shipment of goods incompatible with the technical level of the	FATF 2008 Report (Typology 6)	11 (Syria), 39 (Iran), 47 (Pakistan)	Normal trade (for example a trans-

[29] Paras 30 and 63 of UN Panel on Iran Final Report of 2014 (S/2014/394).

[30] According to UK authorities, recording an Iranian bank as the consignee on shipping documents for goods exported to the UAE or to Malaysia but destined for Iran is a method of circumvention practiced by procurers for decades.

[31] According to Swedish authorities, some individuals, following their acquisition of dual-national status, have set up companies dealing with technically complicated equipment despite lacking a technical background. They may be asked to cooperate by representatives of states of proliferation concern.

[32] Para 120 UN Panel Report on Iran of 2013 (UN document S/2013/331).

[33] According to Swedish authorities, a pattern of activity involving high-technology goods procured overseas and sent straight to Iran or a neighboring country was continuing in late 2016.[33] US authorities have highlighted the practice of international brokering in connection with WMD procurement: Brokering Controls – Department of State (https://www.state.gov/strategictrade/practices/c43181.htm).

[34] According to one large international FI such activity is not usual.

	country to which it is being shipped (*e.g.* semiconductor manufacturing equipment being shipped to a country that has no electronics industry)			shipment)
Trade-related transactions potentially moderately indicative of FoP				
B1	Involvement of front companies, also shell companies (e.g. companies that do not have a high level of capitalization or display other shell company indicators such as absence of online or physical presence)	FATF 2008 Report (Typology 17)	3 & 7 (DPRK), 11 (Syria), 19, 33 & 39 (Iran), 47 (Pakistan), 52 (state not specified), UN Panel on Iran,[35] Australian authorities[36]	Legitimate trade
B2	Involvement of a small trading, brokering or intermediary company (may be carrying out business inconsistent with their normal business)	This report	1 & 5 (DPRK), 10 (Syria), 17, 22, 26, 28, & 40 (Iran), 47 & 48 (Pakistan)	Legitimate trade
B3	Customer is a manufacturer/dealer in products which are subject to export controls	This report	19, 28, 38 & 40 (Iran), 53 (state not specified)	Legitimate trade
B4	Pattern of transactions of a customer or counterparty, declared to be a commercial business, suggest they are acting as a money-remittance business[37]	This report	3 & 5 (DPRK), 17 & 35 (Iran)	Legitimate trade is unlikely unless the money-remittance business is licensed

[35] Paras 70, 71 of UN Panel on Iran Final Report of 2014 (S/2014/394).

[36] Australian authorities consider the biggest enabler for transactions circumventing sanction controls to be the use of shell companies. The use of shell companies enables transactions to occur through the Australia-based entity to a designated entity without detection by the bank, and without subsequent reporting to authorities. On occasions Australia-based entities have been unaware that the shell company was acting on behalf of a designated entity.

[37] A remittance business is one that specializes in transfer of money. A license is usually required.

B5	Transactions between companies on the basis of "ledger" arrangements that may minimize the need for international financial transactions[38]	This report	3, 7 & 8 (DPRK), 45 (Iran)	Legitimate trade
B6	Customers or counterparties to transactions are linked (for example they share a common physical address, IP address or telephone number, or their activities may be coordinated)	This report	8 (DPRK), 12 (Syria), 24 & 46 (Iran), 49 (state not specified)	Legitimate trade
B7	Transaction demonstrates links between representatives of companies exchanging goods *i.e.* same owners or management	FATF 2008 Report (Typology 16)	11 (Syria), 19, 24 & 45 (Iran)	Legitimate trade, for example involving branches of multi-national companies
B8	Involvement of a university in a country of proliferation concern	This report	13, 43 & 44 (Iran), UN Panel on Iran[39]	Academic business
B9	Description of goods on trade or financial documentation is non-specific, innocuous or misleading	This report	10 (Syria), 26 (Iran), UN Panel on DPRK,[40] UK authorities[41]	Local practice in some areas of the world
B10	Evidence that documents or other representations (for example relating to shipping, Customs, or payment) are fake or fraudulent	This report	10 (Syria), 22 & 26 (Iran), 47 (Pakistan)	Other criminal activity

[38] A "ledger" arrangement refers to an accounting system in which linked companies maintain a record of transactions made on each others' behalf. Over a period of time the companies may need only infrequently to transfer funds to settle accounts.

[39] Footnote b, Table 1 of Annex 2 of UN Panel on Iran Report of 2014 (UN document S/2014/394). See also para 63 of UN Panel on Iran Report of 2015 (UN document S/2015/401) for individuals connected with universities in Iran that were subject to designations under UN sanctions.

[40] Paragraph 73 of Panel on DPRK Report of 2016 (UN document S/2016/157).

[41] According to UK authorities, shipping documents for proliferation sensitive items may refer to the goods being shipped only as spares or samples; such wording should be considered a suspicious indicator.

B11	Use of personal account to purchase industrial items	This report	28, 43 & 44 (Iran), 47 (Pakistan)[42]	Legitimate trade (but not usual)
B12	Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws	FATF 2008 Report (Typology 7)	3 (DPRK), 10 (Syria), 24 (Iran)	Legitimate trade
B13	Circuitous route of shipment (if available) and/or circuitous route of financial transaction, possibly through jurisdictions with weak financial regulation or weak financial regulation	FATF 2008 Report (Typology 15)	UN Panel on Iran[43]	To reduce costs, or avoid sanctioned entities or country or war zone
B14	Transaction involves shipment of goods inconsistent with normal geographic trade patterns (*e.g.* does the country involved normally export/import goods involved?)	FATF 2008 Report (Typology 5)	10 (Syria)	Legitimate trade
B15	Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws	FATF 2008 Report (Typology 3)	The location of network overseas hubs may be a reflection of this factor	Legitimate trade
B16	Transaction involves individuals or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws	FATF 2008 Report (Typology 4)	The location of network overseas hubs may be a reflection of this factor	Legitimate trade
Trade-related transactions potentially weakly indicative of FoP				

[42] Apparently rarely seen in DPRK networks (Case No 2) although a possible exception could be cases involving DPRK diplomats.
[43] Annex V of UN Panel on Iran Final Report of 2015 (S/2015/401).

C1	Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost	FATF 2008 Report (Typology 8)	10 (Syria), 48 (Pakistan), UN Panel on Iran[44]	Duty or tax avoidance, or trade-based money laundering
C2	Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.	FATF 2008 Report (Typology 9)	19, 22 & 36 (Iran), 49 & 51 (state not specified)	Sloppy practices[45]
C3	Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose	FATF 2008 Report (Typology 20)	26, 30 & 31 (Iran), 53 (state not specified)	Legitimate trade
C4	Customer vague/incomplete on information it provides, may be resistant to providing additional information when queried	FATF 2008 Report (Typology 12)	44 (Iran)	Other financial crime
C5	New customer requests letter of credit transaction awaiting approval of new account	FATF 2008 Report (Typology 13)		Legitimate trade
C6	Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation	FATF 2008 Report (Typology 19)		Legitimate trade

[44] Para 43 of UN Panel on Iran Report of 2013 (UN document S/2013/331).

[45] According to one international bank this would be a trigger for further investigations of possible financial crime.

Using Table 2 to Mitigate Risks of FoP

The risks of FoP need to be properly understood in order for states or FIs to be able to decide what measures to take to mitigate them, and the indicators in Table 2 can be used to identify and classify potential threats and vulnerabilities. Each FI will have its own policy regarding risk assessments, but even if FIs do not conduct a risk assessment specifically for FoP, they should consider proliferation finance within their wider risk assessments. In addition FoP should be included as a specific financial crime risk when providing training or conducting exercises to enhance staff awareness.

Financial institutions can also use Table 2 to strengthen due diligence procedures aimed at combating FoP. As pointed out above, identifying FoP is difficult because most transactions occur within normal business transaction pathways, and can be masked because of the "noise" associated with all legitimate transactions. Depending on their business model, FIs could incorporate the indicators in Table 2 into Know Your Customer (KYC) procedures, transaction screening procedures, transaction monitoring systems and suspicious activity investigations, regulatory reporting procedures, and due diligence connected to trade finance operations.

Because the indicators might reflect other financial crime or legitimate activity, a key challenge is to avoid a large number of false identifications. Individual FIs can perhaps make best use of Table 2 by basing an identification of FoP on patterns of financial transactions that match more than one indicator, or a number of indicators perhaps variously weighted. Weightings might be determined on the basis of FoP risk assessments and operational experience. The business products of an FI, its customer base, and its geographical footprint, amongst other factors, might also impact weightings. An FI might also determine that different indicators are applicable at different stages of a financial transaction cycle.

Possible Future FoP Typologies

Without exception, the case studies analyzed in Part Two involve classic and established financial mechanisms – wire transfers, trade finance products, cash, checks and in a few cases credit cards. There are no examples relating to digital currencies or new payment methods. However, momentum is building to exploit digital currency technology for legitimate trade purposes,[46] and digital currencies offer opportunities for cybercrime that could extend to FoP.

In the meantime, other forms of cybercrime may offer opportunities to finance proliferation. For example, cyber attacks that took place on 4 February 2016 targeting the Bangladesh Central Bank were intended to make fraudulent transfers totaling as much as USD 951 million from the Bangladesh Central Bank's account at the Federal Reserve Bank of New York. Most of the attempted transfers were blocked, but USD 81 million was routed to accounts in the Philippines and diverted to casinos there.

Research conducted by Symantec[47] and BAE Systems[48] indicates that elements of the code used in the malicious software deployed by the attackers were identical to code used in an attack on Sony's Hollywood studio in 2014. The group responsible is known as "Lazarus" and has carried out a wide range of attacks since 2009, including on banks. The group may be based in DPRK[49] or in North China.[50] The degree to which it works on behalf of DPRK interests is not clear.[51] It may be a mercenary organization.

Most of the funds stolen from the Bangladesh Central Bank are still missing. It would appear possible, and logical given the priority placed by DPRK on WMD, that at least some may have been diverted to finance DPRK's WMD program. The funds sit outside DPRK and could have been placed relatively easily into the international financial system for this purpose.

---

[46] European banks to launch blockchain trade finance platform, Martin Arnold, Financial Times, 26 June 2017 (https://www.ft.com/content/6bb4f678-5a8c-11e7-b553-e2df1b0c3220).

[47] North Korean hacking group behind recent attacks on banks: Symantec, Jim Finkle, Reuters, Mar 15 2017 (http://www.reuters.com/article/us-cyber-northkorea-symantec-idUSKBN16M37J).

[48] Bangladesh heist linked to attack on Sony: BAE researchers, Jim Finkle 13 May 2016, Reuters (http://www.reuters.com/article/us-usa-fed-bangladesh-malware-idUSKCN0Y40MC).

[49] Group IB Report Lazarus Arisen (http://www.group-ib.com/lazarus.html).

[50] North Korea, cyberattacks and 'Lazarus': What we really know, Eric Talmadge Associated Press 12 June 2017 (https://www.novetta.com/2017/06/north-korea-cyberattacks-and-lazarus-what-we-really-know/).

[51] Ibid.

Policy Implications

The world may be under a deeper shadow from WMD than at any time since the Cold War. DPRK's nuclear and ballistic missile programs, rapidly assuming global reach, are controlled by an unpredictable regime. The nuclear arsenals of India and Pakistan, countries characterized by long-running and deep-seated mutual mistrust, remain a serious threat to regional stability. Despite commitments to destroy its chemical weapons,[52] the Syrian government has deployed them on the battlefield. If States that currently rely for their security on US guarantees begin to lose trust in those guarantees, global nuclear proliferation could increase dramatically. In addition, within eight years, many of the restraints on Iran's nuclear program under the JCPoA will fall away.

Under these circumstances it is important that States ensure they have every means available to detect and disrupt proliferation. Every aspect of proliferation has a financial component and the ability to detect and disrupt FoP is central to this objective.

This report provides authorities with a large number of case studies that illustrate what FoP looks like in practice. Armed with this information, states and FIs authorities should consider the following measures to mitigate FoP risks:

- Authorities should carry out national FoP risk assessments, and task departments and agencies to address any gaps identified;
- Authorities should treat FoP as a separate subject to ML and TF, even if some of the indicators may appear similar. This will ensure information relating to FoP is clearly identified as such for the purposes of risk assessments by governments or financial institutions;
- Where obligations to report on FoP are absent, regulators should approve legislation, regulations or guidance for FIs as appropriate;
- Regulators should consider whether existing communication with FIs regarding FoP can be made more effective;
- Authorities should consider how to maximize the potential role that identification and disruption of FoP can play in combating proliferation of WMD, including partnerships with FIs;
- Authorities should ensure effective channels of communications with partner countries and international organizations, capable of handling and protecting sensitive financial information.

[52] UN Security Council resolution 2118 (2014).

Conclusion

The objectives of this Final Report are to illustrate what FoP currently looks like and to characterize the underlying typologies. The multiple case studies described enable identification of current indicators of possible financing of proliferation. In addition to those listed in the FATF 2008 Report, such as transactions connected with designated individuals or entities or with countries of proliferation concern, additional indicators include transactions involving individuals connected with countries of proliferation concern, the use of cash, the involvement of small trading or intermediary companies, unlicensed money-remittance businesses, businesses linked in some way (for example, the same physical or IP address or whose activities are coordinated), the involvement of universities in countries of proliferation concern; non-specific descriptions of goods or materials, the involvement of goods and materials subject to export controls, fake or fraudulent documentation and the use of personal accounts.

The report is intended to help government practitioners to identify FoP and thus provide additional options to identify and disrupt underlying WMD procurement networks. It will help governments to carry out national FoP risk assessments and will assist regulators in providing guidance to financial institutions. The report will also assist financial institutions to carry out FoP risk assessments and ensure that due diligence procedures are fit to counter the threat; it will help financial institutions to remain compliant with WMD-related sanctions and other controls, and to identify and report transactions as required by regulators.

Many of the cases described here demonstrate that FoP networks can be persistent, resilient and adaptable to pressures imposed by sanctions and other controls.

Identifying and disrupting FoP is potentially a key tool to combat WMD, but is most likely to be successful when governments and private sector cooperate and coordinate in sharing information. By illustrating what FoP currently looks like this report actively facilitates this goal.

Annex 1. Provisions Relating to FoP Contained in UN Security Council Resolutions and FATF Standards

UN resolution 1540 (2004) and successor resolutions: the following provisions relating to FoP:

- Operational paragraph (OP) 2 requires all States to have effective laws to prohibit non-state actors to finance nuclear, chemical or biological weapons (WMD) and their means of delivery;
- OP 3(d) requires all States to implement effective controls to prevent financing of exports or trans-shipments of WMD and their means of delivery.

UN resolution 1718 (2006) on DPRK, and successor resolutions:[53] the following provisions related to financial sanctions:

1718 (2006)

- Imposes an assets freeze on individuals or entities designated for their involvement in DPRK's WMD programs. The requirements extend to those operating on their behalf or at their direction;

1874 (2009)

- Calls upon Member States to prevent provision of financial services or transfer of financial resources that could contribute to prohibited programs/activities;
- Designates additional individuals and entities.

2094 (2013)

- Bans provision of financial services, or transfer of financial assets or resources that could contribute to DPRK's WMD or other prohibited activities;
- Designates additional individuals and entities.

2270 (2016)

- Expands financial measures, including an assets freeze on Government of DPRK and its Workers' Party entities associated with prohibited programs and activities;
- Prohibits DPRK banks from opening new branches; requires States to close existing DPRK bank branches in their territories; prohibits Member States from opening branches in DPRK; requires States to close existing offices in DPRK if related to prohibited programs or sanctions violations;
- Imposes sectoral sanctions with bans on sales of coal, minerals and fuels;
- Designates additional individuals and entities.

2321 (2016)

[53] As of 21 August 2017, successor resolutions are 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017) and 2371 (2017).

- Prohibits the provision of insurance or re-insurance services to vessels owned, controlled operated or flagged by DPRK;
- Expands sectoral sanctions by including copper, nickel, silver and zinc to items banned for sale by DPRK;
- Strengthens financial measures by requesting closure of existing representative offices, subsidiaries or banking accounts in DPRK; prohibiting public and private financial support for trade with DPRK; expelling individuals who are believed to be working on behalf of or at the direction of DPRK banks or financial institutions;
- Designates additional individuals and entities.

2371 (2017)

- Imposes full ban on sales of coal, iron and ore; adds lead and lead ore to commodities subject to sectoral sanctions;
- Expands financial sanctions by prohibiting new or expanded joint ventures and cooperative commercial entities with DPRK;
- Includes companies performing financial services in the definition of financial institutions, for the purpose of implementing financial sanctions;
- Designates additional individuals and entities.

2375 (2017)

- Introduces a full ban on the supply, sale or transfer of all condensates and natural gas liquids, and restricts refined petroleum products and crude oil, to DPRK;
- Introduces a ban on the export by DPRK of textiles;
- Expands financial sanctions by prohibiting all joint ventures or cooperative entities or expanding existing joint ventures with DPRK entities or individuals;
- Designates additional individuals and entities.

UN resolution 2231 (2015) relating to Iran includes the following financial provisions:

- Imposes restrictions on provision of financing or financial services related to Iran's nuclear, ballistic missile or conventional weapons programs;
- Imposes an assets freeze on individuals or entities designated for their involvement in Iran's ballistic missile or conventional weapons programs, or the Islamic Revolutionary Guards Corps.

The FATF standards of 2012: the following recommendations relevant to FoP:

- Recommendation 7: Requirement to implement targeted financial sanctions in compliance with UN Security Council sanctions related to WMD and its financing;
- Recommendation 2: Requirement for domestic authorities to cooperate and coordinate over policies and activities to combat FoP.

The effectiveness with which FATF countries implement these recommendations are

measured in the course of mutual evaluation reviews under:

- Immediate Outcome 1: WMD risks understood and actions to combat them are coordinated domestically;
- Immediate Outcome 11: Individuals and entities involved in WMD are prevented from raising, moving and using funds.

Annex 2. FATF 2008 Report on Proliferation Financing: Indicators of Possible Proliferation Financing[54]

1. Transaction involves individual or entity in foreign country of proliferation concern.
2. Transaction involves individual or entity in foreign country of diversion concern.
3. Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
4. Transaction involves individuals or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
5. Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import good involved?).
6. Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
7. Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
8. Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.
9. Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
10. Customer activity does not match business profile, or end-user information does not match end-user's business profile.
11. Order for goods is placed by firms or individuals from foreign countries other than the country of the stated end user.
12. Customer vague/incomplete on information it provides, resistant to providing additional information when queried.
13. New customer requests letter of credit transaction awaiting approval of new account.
14. The customer or counterparty or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control

[54] Page 54 of the Report (http://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf).

contraventions.

15. Circuitous route of shipment (if available) and/or circuitous route of financial transaction.
16. Transaction demonstrates links between representatives of companies exchanging goods i.e. same owners or management.
17. Transaction involves possible shell companies (e.g. companies do not have a high level of capitalization or displays other shell company indicators).
18. A freight forwarding firm is listed as the product's final destination.
19. Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.
20. Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.

Annex 3. Comparison of ML with TF and FoP[55]

	Money Laundering	Terrorist Financing	Financing of Proliferation
Source of Funds	Internally from within criminal organizations	Internally from self-funding cells (centered on criminal activity) Externally from benefactors and fund-raisers	State-sponsored programs
Conduits	Favors formal financial system	Favors cash couriers or informal financial systems such as hawala and currency exchange firms	Favors formal financial system
Detection Focus	Suspicious transactions such as deposits uncharacteristic of customer's wealth or the expected activity	Suspicious relationships, such as wire transfers between seemingly unrelated parties	Individuals, entities, states, goods and materials, activities
Transaction Amounts	Large amounts often structured to avoid reporting requirements	Small amounts usually below reporting thresholds	Moderate amounts
Financial Activity	Complex web of transactions often involving shell or front companies, bearer shares, offshore secrecy havens	Varied methods including formal banking system, informal value-transfer systems, smuggling of cash and valuables	Transactions look like normal commercial activity, structured to hide origin of funding
Money Trail	Circular – money eventually ends up with the person who generated it	Linear – money generated is used to propagate terrorist groups and activities	Linear – money is used to purchase goods and materials from brokers or manufacturers

[55] This chart is based on a presentation by James R Richards, Wells Fargo, 2005, quoted in the CAMS Examination Study Guide 5th Edition. The author has added to this presentation the right-hand column, headed Financing of Proliferation.

Annex 4. Criminal Cases

Case 1: US District Court Northern District of Illinois Eastern Division, United States of America v. Hsien Tai Tsai and Yueh-Hsun Tsai, Case 12CR829, indictment filed 26 June 2013; Affidavit of FBI Special Agent in Support of Extradition.

Cases 3, 4: United States District Court District of New Jersey Criminal Complaint Case 16-06602 filed 3 August 2016, United States of America v. Dandong Hongxiang Industrial Development Co Ltd, and others, and related Verified Complaint for forfeiture in rem dated 26 Sep 2016.

Case 5: Public Prosecutor v Chinpo Shipping Company (Private) Ltd [2016] SGDC104; Chinpo Shipping Co (Pte) Ltd v. Public Prosecutor [2017] SGHC 108, 12 May 2017.

Case 10: In the United States District Court for the Middle District of Pennsylvania, United States of America v. Harold Rinko and others, Case 312CR294, filed 20 Nov 2012.

Case 16: Indictment US District Court Southern District of New York 13 CR 00144 filed 28 April 2014, Complaint 14CV3015, dated 29 April 2014,

Case 17: Umeå, Sweden, District Court records (Case B 58-10 date 3 May 2010).

Case 23: United States District Court Southern District of Texas Houston Division, United States of America v. Barham Mechanic and others, 15CR204, 16 April 2016;

Case 40: US District Court Eastern District of New York, Case 16M134, 18 Feb 2016.

Case 47: United States of America v. Naeem Malik and Nadeem Akhtar, Indictment filed in the US District Court for the District of Maryland, case 10CR00103, 11 March 2010.

Case 48: US District Court for Middle District of Pennsylvania US v. Shafqat Rana, Abdul Qadeer Rana, Shahzad Rana, Optima Plus International LLC, Afro Asian International Pvt Ltd Case 14CR29, 22 January 2014. The case has yet to come to court.

Case 50: United States District Court Southern District of New York, United States of America v Peter Gromacki, case 12CR00302, 19 April 2012.

Case 56: Press Release: Investigation result of Illegal transfer case of Iran fund of 1.9 trillion won, 24 January 2013, Seoul Central District Public Prosecutors' Office;56 Affidavit of Sue Chambers in support of Verified Complaint, Case. 3:14cv65 of 2 May 2014; United States District Court for the District of Alaska Indictment Case 3:16cr00142 of 14 Dec 2016.

[56] http://www.spo.go.kr/seoul/notice/notice/notice01.jsp?mode=view&article_no=549099&pager.offset=0&search:search_val:search=%25C0%25CC%25B6%25F5&search:search_field1:equals1=A.etc_char5&search:search_key:search=article_title&search:search_val1:equals1=&board_no=116&stype=&info_id=&seq_id=.

Annex 5. Further Reading

Typologies Report on Proliferation Financing, Financial Action Task Force, 18 June 2008.

Combatting Proliferation Financing: A Status Report on Policy Development and Consultation, Financial Action Task Force, February 2010.

Javier Serrat, Financial Interdictions to Curb Proliferation, Arms Control Association, 5 July 2012.

Financial Controls and Counter-Proliferation of Weapons of Mass Destruction, Nikos Passas, Case Western Reserve Journal of International Law, Vol 44, Issue 3, 2012.

The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction, Financial Action Task Force Guidance June 2013.

Emil Dall, Andrea Berger and Tom Keatinge, Out of Sight, Out of Mind? A Review of Efforts to Counter Proliferation Finance, Whitehall Reports, 20 June 2016.

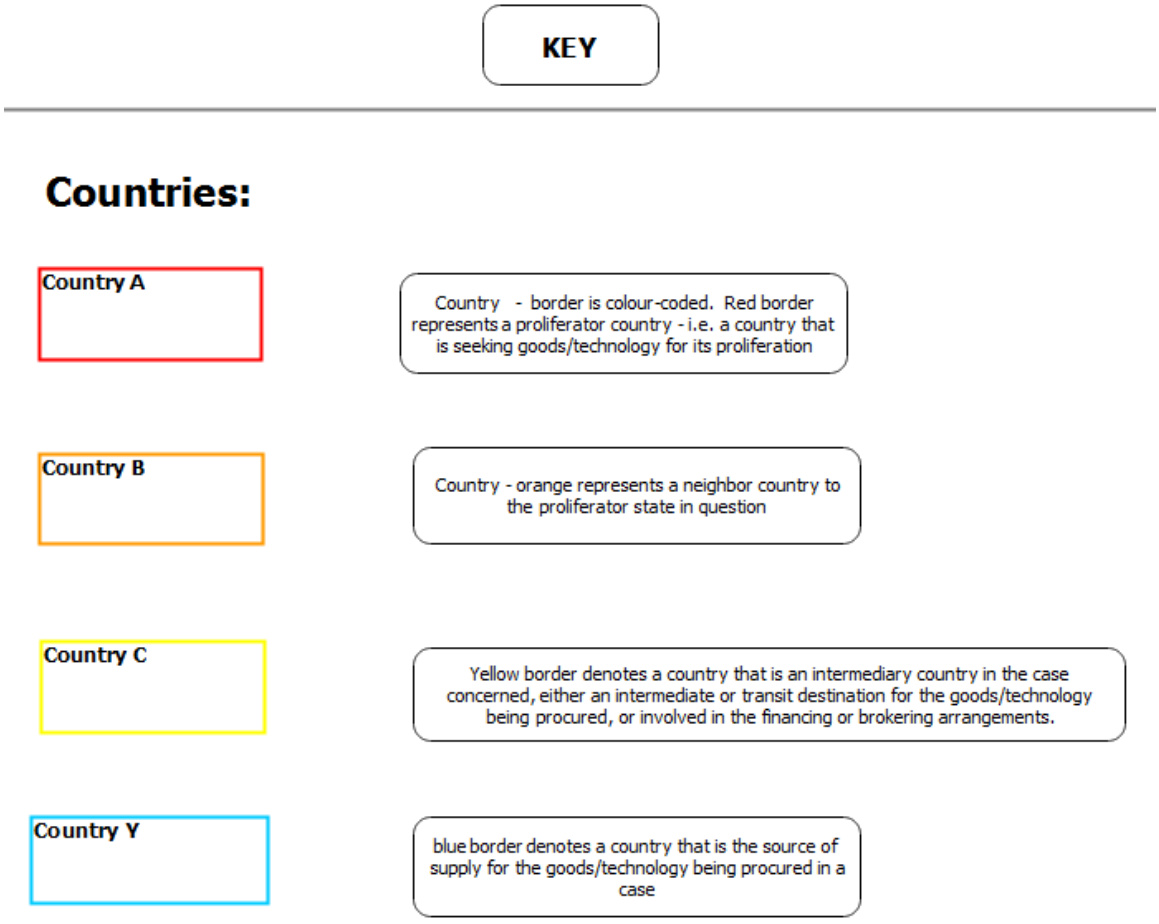
Emil Dall, Tom Keatinge and Andrea Berger, Countering Proliferation Finance: An Introductory Guide for Financial Institutions, RUSI, Other Publications, 19 April 2017.

Andrea Berger and Anagha Joshi, Countering Proliferation Finance: Implementation Guide and Model Law for Governments, RUSI, Other Publications, 21 July 2017.

Part Two

Case Study Analyses

The following cases are categorized by country program where specified, or type of activity. Within each category, cases are listed chronologically according to dates of activity specified in the text. Where dates are not specified, the chronology is estimated. A key to the figures is provided below.



Entities (selection shows commonly used icons)

Individual

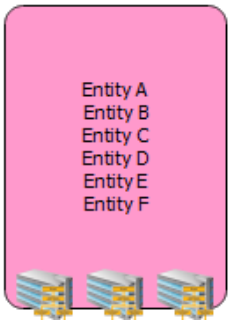
Commercial company or other organization

Bank account

Bank or other financial institution

Manufacturer/supplier of goods

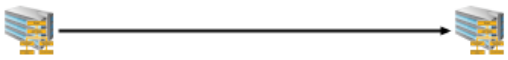
Government department or agency



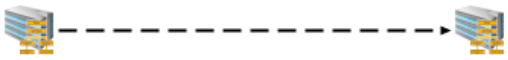
List of entities - where several entities are shown grouped on a chart, and it would not be practical to put an individual symbol on the chart for each entity, a text box with the list of entities written within is used. If the entities are all of the same general type, then three appropriate entity icons and colour shading may be used to designate this. In this example, rose box filling is used to indicate companies involved in the export or movement of goods

Links and flows:

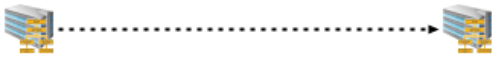
Thick gray line line denotes an unspecified link between two entities, e.g. ownership, organizational connection, etc. Text on the link label may be used to give information regarding the nature of the link. In some cases an arrow may be included to show the direction of some relationships, such as ownership.



Black line with arrowhead denotes financial transfer between two entities, arrowhead shows direction of movement of funds



Black dashed line indicates some kind of value transfer arrangement of unknown type, or bank guarantees/similar arrangements put in place (text annotation gives specifics in a particular case).



Black dotted line with arrowheads denotes a suspected or unconfirmed transfer of funds, or a planned future ttransfer

Rose dashed line denotes movement of goods/technology being purchased

Blue line indicates negotiations for the purchase of goods/technology or the placing of an order for goods/technology, or arrangements being made for the export/supply of goods.

Democratic People's Republic of North Korea (DPRK)

Case 1: A resilient procurement network adapts to designations (2009)[57]

According to 2015 US court documents, a network of individuals including Individual 1, based in Taiwan and his son Individual 2, based in the US, were under investigation from 2009 for export of US-origin goods and machinery that could be used to produce weapons of mass destruction.[58]

According to the documents, the network consisted of at least three Taiwan-based companies set up and managed by Individual 1: Global Interface Company Inc; its subsidiary, Trans Merits Co Ltd; and Trans Multi Mechanics Ltd. Individual 1's wife was an officer in Global Interface Company Inc, and Trans Merits Co Ltd. Individual 1 and Trans Merits Co Ltd were convicted by Taiwanese authorities in 2008 in connection with shipping restricted materials to North Korea.

In January 2009 the US Treasury Department designated Individual 1, his wife, Trans Merits Co Ltd and Global Interface Company Inc for support to the Korea Mining Development Trading Corporation (KOMID), an entity closely linked with DPRK's WMD programs. In effect, US persons could only do business with Individual 1 and his designated companies with a license from the US Treasury Office of Foreign Assets Control (OFAC).

According to a separate report, a few months later in mid-2009, US authorities learned that Individual 1 was due meet a KOMID representative in Singapore to receive a payment, possibly for shipment of equipment worth over USD 850,000, possibly in cash.[59]

Despite his designation in January 2009, later that year Individual 1 imported a precision machine tool from the US through his third, non-designated, Taiwanese company, Trans Multi Mechanics Ltd, and with the assistance of his son.

Trans Multi Mechanics Ltd was represented on the related export documents as purchaser and end-user. Although payment was initiated by Trans Merits Co Ltd, the involvement of a designated entity in the transaction was hidden because the wire transfer, to Individual 2's US bank account, took place from Trans Multi Mechanics Ltd's bank account in Taiwan.

Similarly, subsequent financial transfers from Individual 1 to his son took the form of two wire transfers from a bank account in Taiwan controlled by his daughter, in effect hiding from the US banking system the involvement of a designated individual (Figure

[57] This case was Case No 1 in the Interim Report of 5 February 2017.

[58] For example, indictment filed 26 June 2013, US District Court Northern District of Illinois Eastern Division, Case 12 CR 829, United States of America v. Hsien Tai Tsai and Yueh-Hsun Tsai, and Affidavit of FBI Special Agent in Support of Extradition.

[59] US Department of State cable dated 14 April 2009, quoted by Wikileaks (https://wikileaks.org/plusd/cables/09STATE36855_a.html).

1). Individual 2 also set up a US-based company, Factory Direct Machine Tools, to help develop business with his father's companies.

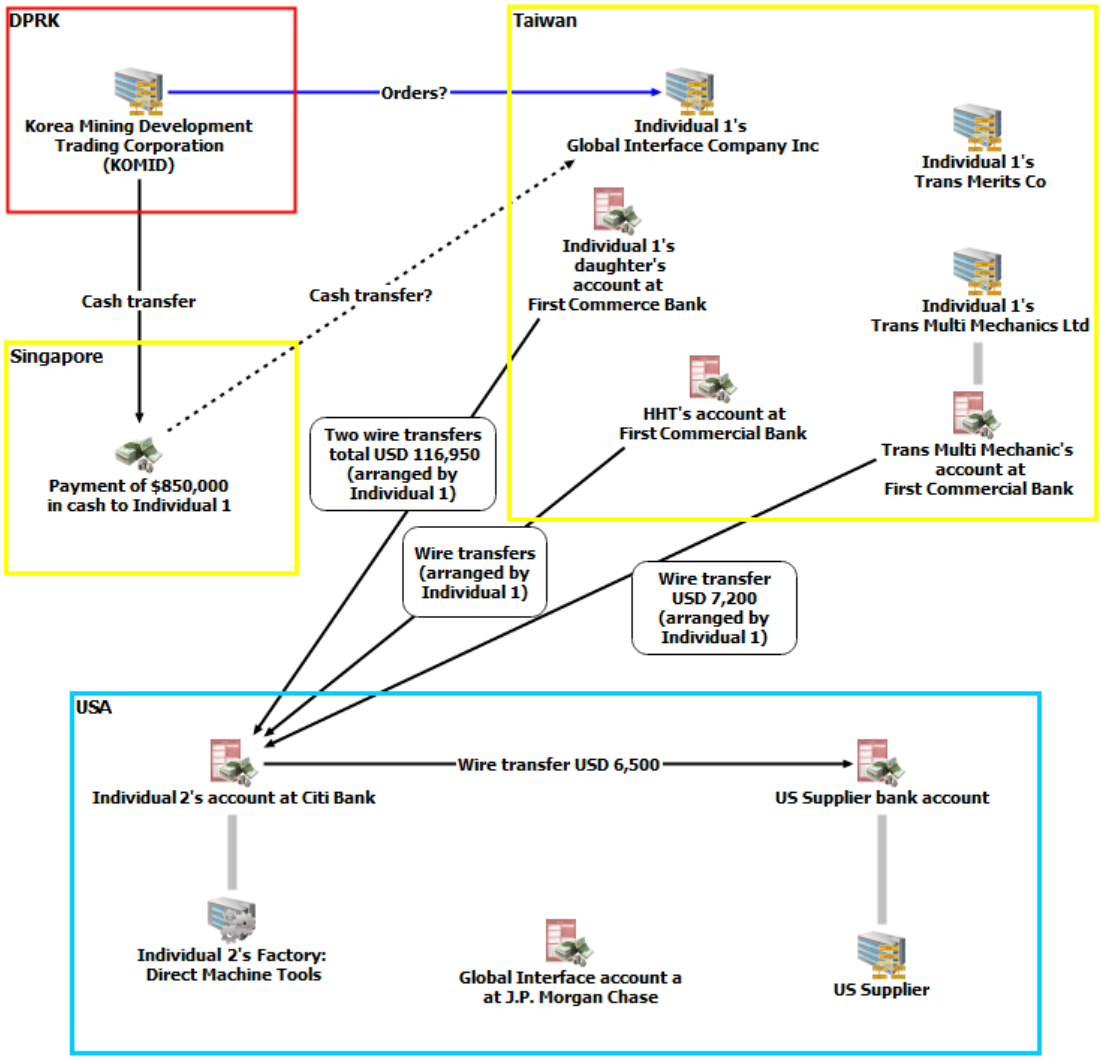


Figure 1. DPRK procurement network involves father's and son's companies in Taiwan and US

Key Points

- A small family company was involved: family members were connected with the state through which goods and materials were being diverted (trans-shipped);
- The network was resilient: despite designation of the main figure (Individual 1) and two of his companies, the network adapted by creating additional companies, and expanded its proliferation and non-proliferation trading activities;
- It is not clear how the network was financed by KOMID. At least one cash transfer may have taken place in Singapore;
- The network was also used for non-proliferation-related business (including procurement to the US).

Case 2: FoP by avoiding international financial transactions (2010)[60]

In December 2012, North Korea launched an Unha-3 rocket. Debris recovered from the launch was found to contain pressure transmitters. Investigation of these by the UN DPRK Panel of Experts revealed that they were purchased by a Taiwan-based company, Royal Team Corporation (RTC), from a UK-based company.

Transfer of the pressure transmitters from Taiwan to Pyongyang took place in two transactions, in December 2006 and May 2010.[61] After the transmitters were shipped from the UK to Taipei, RTC hand-carried them on flights via Beijing to Pyongyang,[62] where they were delivered to a North Korean company, Korea Chonbok Trading Corporation (KCTC).

RTC said that KCTC paid for the 2006 transaction by a transfer via a Malaysian bank of 71,700EUR. The transfer may have involved the representative of the Bank of East Land in Malaysia (see Figure 2).

For the 2010 transaction, RTC provided two different descriptions of its reimbursement by KCTC (no documentation was provided to support either scheme). The first method (method 1) was by means of a payment offset arrangement: RTC and a second Taiwan-based company, Company A, took part in a trade fair in Pyongyang. The fair was organized by a North Korean company, Korean International Exhibition Corporation (KIEC). Company A owed KIEC for participation of Taiwan-based companies in the fair a sum of money similar to that KCTC owed RTC for the pressure transducers. The parties' commitments were met by KCTC paying KIEC a sum equivalent to the cost of the pressure transducers and Company A transferring an equivalent amount to RTC.

RTC subsequently claimed that it had been paid in cash by KCTC in Pyongyang (method 2) and that Company A was not involved. RTC said it used this cash to pay KIEC for the participation of Taiwan-based companies in the trade fair.

[60] This case was Case No 2 in the Interim Report of 5 February 2017.
[61] The summary of this case is taken from the UN Panel on DPRK's Final Report of 2016 (S/2016/157). The UK company was not made aware of the ultimate end-user.
[62] Without declaring them to Customs authorities.

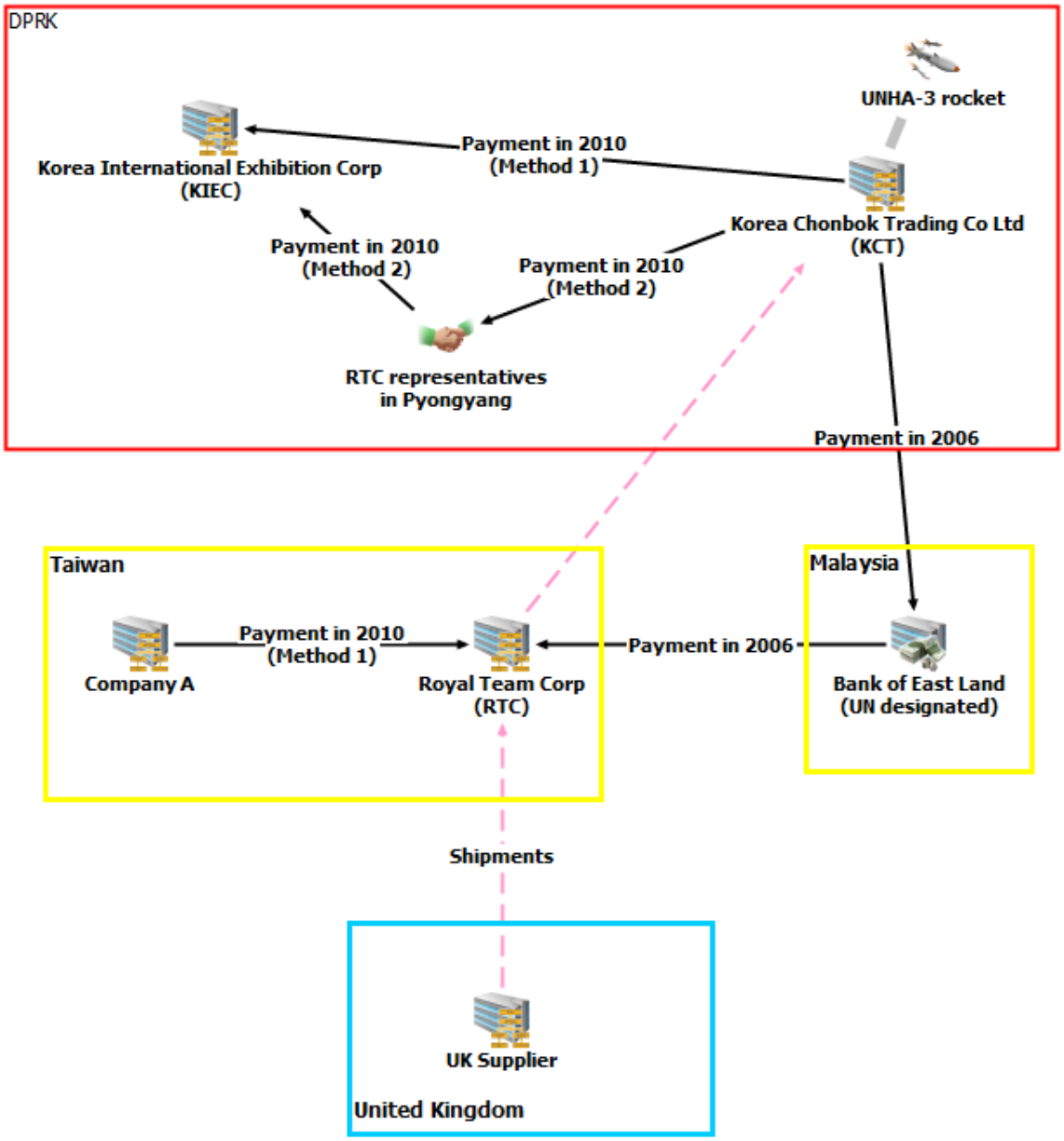


Figure 2. Procurement of pressure transducers by Korea Chonbok Trading Co Ltd and payment methods

Key Points

- The payment offset arrangement described here would have been difficult for financial authorities or institutions to track; no financial transactions took place through the international financial system;
- Similar offset arrangements in connection with circumvention of financial sanctions on Iran were described by the UN Panel on Iran.[63]

[63] Para 59 of the UN Panel on Iran Final Report 2015 (S/2015/401).

Case 3: A designated DPRK bank maintains financial operations through DHID front companies (2009-2015)

The following is based on the contents of US court documents.[64]

Korea Kwangson Banking Corporation (KKBC) was listed by OFAC on 11 Aug 2009 for providing financial services in support of DPRK's WMD and ballistic missile programs. Dandong Hongxiang Industrial Development Co Ltd (DHID) is a trading company based in Dandong, China, on the border with DPRK. DHID management personnel created a series of front companies, and opened corresponding bank accounts, in China and overseas, to facilitate transactions funded by and/or guaranteed by KKBC. According to its owner, DHID, a China-based trading company, accounted for over 20% of China's trade with DPRK in 2010. At times, DHID and its front companies managed the full logistical chain of commodity contracts; at other times they facilitated US-dollar transactions between DPRK-based entities and suppliers in other countries.

According to US court documents, a US-dollar account held by DHID at a KKBC branch in Pyongyang was used by KKBC to fund DHID for commodity purchases made by DHID's front companies overseas. A bank statement (figure 3) shows deposits from a variety of sources (including cash) that frequently correspond to withdrawals (including cash) of equivalent or similar funds around the same time.

According to US court documents, these bank statements show that a "ledger" accounting system was in operation between KKBC and DHID although the documents do not specify how this system operated in practice. Some of the credits and debits to DHID's bank account in Pyongyang may have corresponded to records of equivalent debits and credits at different DHID front companies overseas. Withdrawals in cash may also have been physically transferred overseas and credited to DHID front companies. In some of the cases recorded in the documents, the KKBC Dandong Representative Office was responsible for managing DHID's proxy role with KKBC. Such mechanisms would have enabled KKBC to settle outstanding balances with DHID without transmitting funds in USD through the US financial system (where they would have been blocked).

[64] United States District Court District of New Jersey Criminal Complaint Case 16-06602 filed 3 August 2016, United States of America v Dandong Hongxiang Industrial Development Co Ltd, and others, and related Verified Complaint for forfeiture in rem dated 26 Sep 2016.

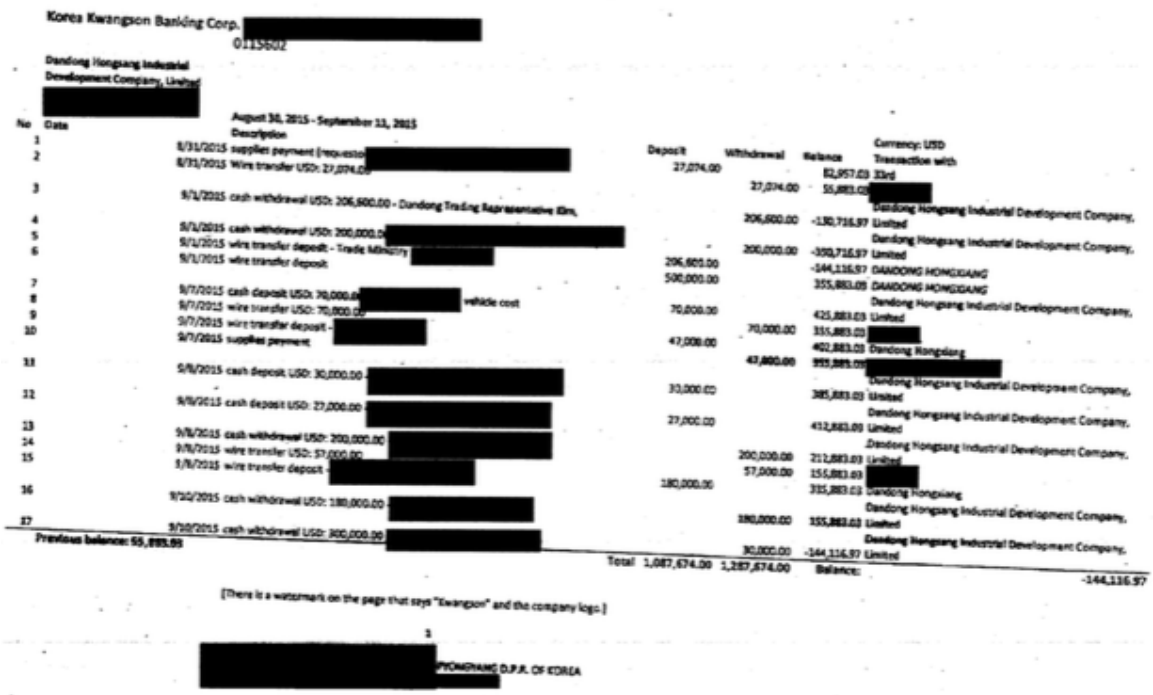


Figure 3. Bank statement for the DHID account held at a branch of KKBC in Pyongyang illustrating a number of contemporaneous matching deposits and withdrawals. Note that because the identities of payers and payees have been redacted it is not possible to determine whether all entries reflect activity by DHID and its front companies on behalf of KKBC, or whether some reflect other transactions by DHID within DPRK (Image taken from United States District Court District of New Jersey Criminal Complaint Case 16-06602 filed 3 August 2016).

As a further indication that DHID was conducting US dollar transactions on KKBC's behalf, court documents note that DHID's US interbank remittance transactions through Standard Chartered Bank in the US "increased from $1.3 million for the approximately three-year period prior to KKBC's designation to $110 million from 2009 to 2015, after KKBC was designated."

US court documents identify many front companies created or purchased by DHID and its executives for the purposes of transmitting and/or receiving money through the US on behalf of KKBC, and the banks involved (figure 4).[65]

[65] A separate case brought by US authorities alleges that Minzheng International Trading Limited, a company based in Hong Kong, acts as a front company for the Foreign Trade Bank of DPRK, sanctioned under UN and US legislation and owner of KKBC, similarly to the way in which DHID is described as acting for KKBC (Verified Complaint for Forfeiture *In Rem,* United States District Court for the District of Columbia case 1:17-cv-01166-KBJ, filed 14 June 2017).

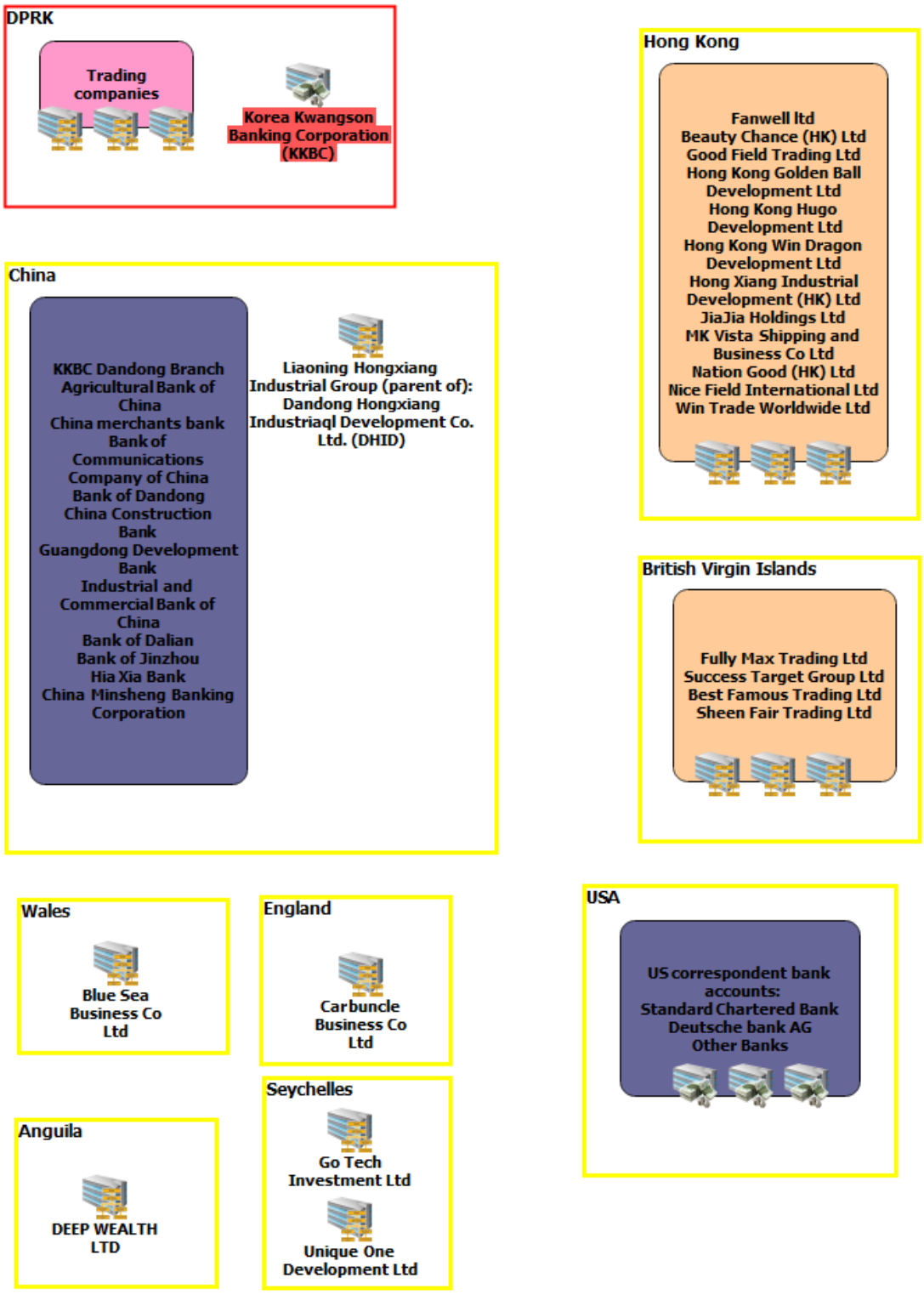


Figure 4. The network of DHID and its front companies supporting KKBC, and the banks used by them in China[66]

[66] Based on information referenced in United States District Court District of New Jersey Criminal

Key Points

- The US-dollar bank account of DHID at a KKBC branch in Pyongyang was used by KKBC to fund DHID for commodity purchases by DHID front companies overseas. This enabled KKBC to finance activities overseas indirectly, despite its designation;
- Multiple banks in China were involved in transactions subsequently carried out by DHID and its front companies;
- DHID made use of multiple front companies overseas, including in Anguilla, Seychelles, England, Wales, British Virgin Islands and Hong Kong;
- A “ledger” system was used to record transactions carried out by DHID and related companies.

Complaint Case 16-06602 filed 3 August 2016, and related Verified Complaint for forfeiture in rem dated 26 Sep 2016.

Case 4: DHID front company facilitates financing of urea trade by designated bank (2013)

The following is based on US court documents.[67]

The documents describe a number of cases of the use of the front companies to circumvent KKBC's listing by OFAC. The following is the most recent, involving purchase of urea fertilizer in 2013 (Figure 5). Although this does not involve WMD goods and materials, the methods of circumvention of financial sanctions by KKBC and DHID could readily be adapted to such procurement.

In March 2013 DHID agreed to sell 20,000 metric tons of urea fertilizer to a DPRK company, subject to a guarantee from KKBC that payment had been made by the company before the cargo was to be loaded.

Hongxiang Industrial Development (H.K.) Limited, a DHID front company in Hong Kong, subsequently arranged the purchase of 10,000 metric tons of urea from a Singapore Distributor.

Bank records show that Fully Max Trading Ltd, a BVI-based DHID front company, paid the Singapore supplier almost USD 3.9 million, in a series of seven installments between May and June 2013. All the payments transited the US financial system. Bank records also show that between May and June 2013, Fully Max Trading Ltd received a deposit of about USD 4.8 million into its account at China Merchants Bank from a DHID account.[68] These funds transited the U.S. financial system through a US correspondent banking account at Standard Chartered Bank. DHID made a profit of about 23% on the deal (DHID made similar profits on other deals described in the court records).

[67] Ibid.

[68] Based on details contained in US court documents the DHID account was almost certainly also held at China Merchants Bank.

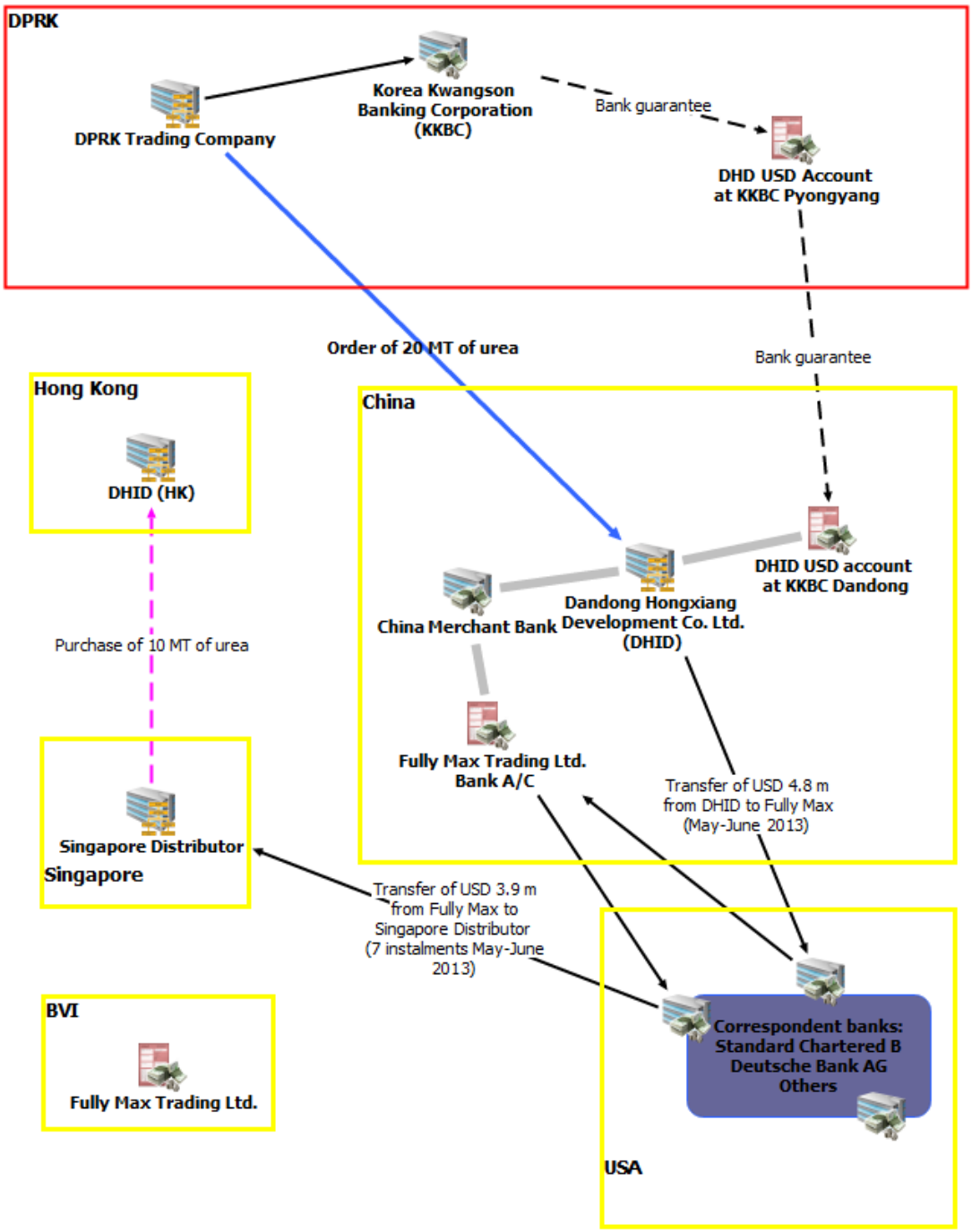


Figure 5. DHID and its network of front companies enable KKBC to finance the urea trade despite its designation

Key Points

- The network of DHID and front companies involved extended to China, Hong Kong and the British Virgin Islands;

- Payments made by the DHID network were based on a bank guarantee from KKBC;
- It is likely that the KKBC Dandong Representative Office was responsible for transferring funds to enable DHID to pay the Singapore supplier.

Case 5: A shipping agent convicted of FoP in 2013 (overturned on appeal)[69]

In July 2013, Panama Canal authorities detained a North Korean vessel, the Chong Chon Gang (CCG), while it was transiting the Panama Canal from Cuba to DPRK. Canal authorities found a shipment of arms and related materials concealed under other cargo.[70]

The CCG was operated and managed by Ocean Maritime Management Ltd (OMM), one of the largest North Korean shipping companies.[71] Costs in connection with the voyage of the CCG were paid by Chinpo Shipping (Private) Ltd, based in Singapore.

Following investigations, Singaporean authorities filed criminal charges. Chinpo was convicted of financing of proliferation[72] in connection with a sum of USD 72,016.76 that Chinpo had remitted by wire transfer from a Bank of China account to a Panama Canal shipping agent.[73] Additionally, Chinpo was convicted of carrying out an unlicensed remittance business (see Figure 6). However, Chinpo's conviction on charges of financing of proliferation was subsequently overturned on appeal.[74]

According to court documents,[75] Chinpo Shipping (Private) Limited was a shipping agent, chandlers and general wholesale importer/exporter. It was one of three companies run by a family that shared the same business address, employees, and an email account for communications with DPRK entities. The three companies also shared an account at the Bank of China (in Chinpo's name). DPRK Embassy in Singapore used the business as a postal address. Chinpo had business relationships with North Korean shipping companies since the 1980s, and with OMM since the mid-1990s.

Chinpo used its Bank of China account to manage funds on behalf of OMM. Monies due to OMM (for example, freight charges) were paid into the account. Monies were remitted from the account at OMM's request, for example to DPRK vessel owners (who were not able to set up their own bank accounts), or on their behalf for supplies, port charges or other disbursements, or from one DPRK ship owner to another. Chinpo also

---

[69] This case is an updated version of Case no 3 in the Interim Report of 5 February 2015. That case study was developed with the assistance of Andrea Berger, Center for Non-Proliferation Studies at Monterey.

[70] The arms and related materials: d 2 MiG-21 jet fighters, anti-tank rockets, and SA-2 and SA-3 Russian surface-to-air missile systems and their components.

[71] UN Panel on DPRK Final Report 6 March 2014 (S/2014/147).

[72] The specific charge was "transferring financial assets or resources that may be reasonably used to contribute to DPRK's nuclear programs or activities."

[73] Public Prosecutor v Chinpo Shipping Company (Private) Ltd [2016] SGDC104. Specifically, the Judge concluded that the arms and related material onboard the vessel could contribute to DPRK's overall nuclear capability, and thus the payment of USD 72,106.76 for transit fees through the Canal was in connection with DPRK's nuclear capability.

[74] Chinpo Shipping Co (Pte) Ltd v. Public Prosecutor [2017] SGHC 108, 12 May 2017. The High Court agreed with Chinpo's appeal on the grounds that it was not reasonable to conclude that the cargo on board the CGG "could reasonably be used to contribute' to DPRK's nuclear programs.

[75] Public Prosecutor v Chinpo Shipping Company (Private) Ltd [2016] SGDC104.

used the account to transfer funds to OMM.[76]

According to court documents, Chinpo kept track of these funds on OMM's behalf, and they were separate from Chinpo's chandlery and shipping agent services. Over three years, 605 remittances took place totaling more than USD 40 million, all related to DPRK vessels. Chinpo was effectively operating a remittance business although the company had no license to do so from Singapore authorities.

Chinpo tried to hide its involvement with DPRK companies by removing the names of DPRK vessels and other identifying details from remittance forms and email correspondence. Payments from Chinpo's account took place in the absence of invoices or other details.

The court documents record that the Bank of China rarely queried a remittance by Chinpo. It did so, however, in connection with the payment of expenses for the outward leg of CCG's voyage to Cuba. The bank requested details of CCG's cargo, its consignee in Cuba, and the bill of lading, all of which were provided.

[76] Although court documents refer only to an account, or possibly accounts, at Bank of China, media reporting of the case hearings suggests Chinpo also used accounts at other banks in Singapore for money remittance activities, including United Overseas Bank and International Commercial Bank (https://www.nknews.org/2015/09/court-case-reveals-chinpo-shippings-ties-to-north-korea/).

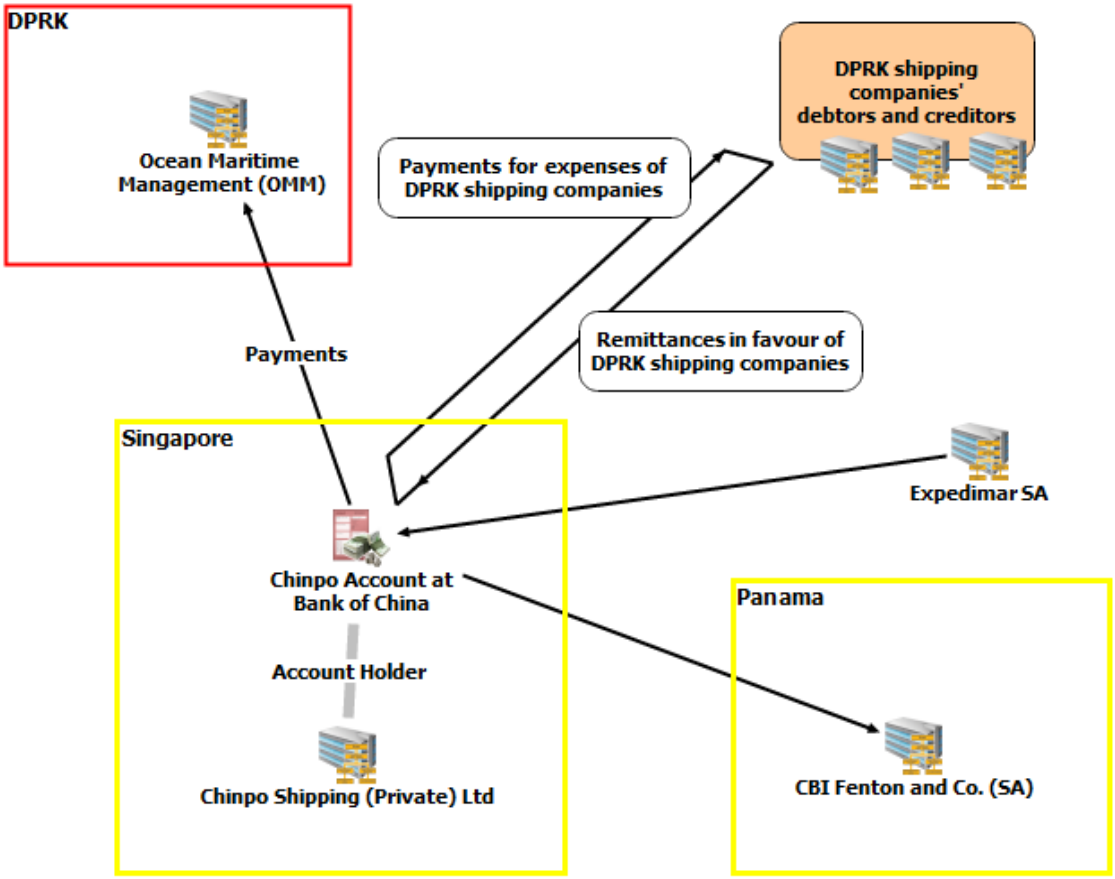


Figure 6. The proliferation-related payment to C.B. Fenton and Co S.A. from Chinpo's account at the Bank of China was funded from a remittance by Expedimar S.A. for a shipment delivered by CCG earlier in its voyage

Key Points

- Chinpo is an example of a small, family-run company involved in what was thought to be a proliferation network;
- Although transactions through Chinpo's Bank of China account triggered an alert in relation to US sanctions on Cuba, Chinpo's long-standing DPRK business connections apparently did not violate any triggers regarding DPRK;
- It is not clear to what extent Chinpo's bank accounts were being monitored for money laundering – sums transferred far outweighed those connected with Chinpo's declared shipping agent/chandlery business and might have been flagged as ML suspicious indicators. Furthermore, payments were made from Chinpo's account in the absence of invoices or other details, and details were removed from remittance forms. It is also unusual for ship agents to hold large amounts of money on behalf of ship owners;
- Chinpo's remittance business activities are similar to those of other commercial businesses involved in circumvention of financial sanctions (see for example Cases 17 & 35).

Case 6: Financial networks identified by a financial institution (2013-2016)

A recently published study[77] characterized DPRK proliferation networks as centralized around key entities and individuals, underpinned by a global centralized system of illicit finance reliant on key logistical "chokepoints." The study considered that the great majority of North Korea's trade activity between 2013 and 2016, both licit and illicit, may have been concentrated within just 5,233 companies, mainly located in China. The study is based on public records and it notes that in many cases there was no transaction-level financial data to confirm its analysis of suspected illicit activity.

Elements of C4ADS's study are in fact supported by analyses of transaction-level financial data as described in Case 8 below, and in the following information provided by an international financial institution:

The institution searched its database of transactions emanating to and from correspondent banks, in US dollars (database 1):

- The institution correlated database 1 with names of DPRK companies identified in the 2016 Report of the UN Panel on DPRK established pursuant to resolution 1874 (2009) (40 names in all).[78] This established that there were 12 names in common;
- The institution identified 179 counterparties (CP 1s) to these 12 names in database 1;
- The institution further identified 582 counterparties (CP 2s) to the 179 CP1s.
- The institution then established a second database (database 2) comprising the counterparties in database 1 to all of the above. Database 2 included names of 1300 entities.

The institution considered that it was reasonable to interpret database 2 as made up of individuals and entities conducting business directly or indirectly with DPRK-related individuals or entities. Analysis showed that there was a high degree of connectivity within database 2. A large proportion of the companies in database 2 engaged in transactions with each other to some degree.

The institution further correlated entries in database 2 with open source and other evidence of connections to DPRK, and identified 150 names (these were labeled "confirmed nodes"). The institution further identified the members of database 2 that conducted >33% of their transactions solely with other members of database 2. There were 26 of these, labeled "calculated nodes."

The institution then established a third database, database 3, consisting of "confirmed nodes" and "calculated nodes." Analysis of database 3 showed it to be a network of entities, including front companies or shell companies, based outside DPRK and registered in China, Hong Kong and elsewhere. The network was directly tied to DPRK,

[77] Risky Business A System-level Analysis of the North Korea Proliferation Financing System, C4ADS, 2017
[78] Security Council document S/2016/157 (http://www.un.org/ga/search/view_doc.asp?symbol=S/2016/157).

apparently generating its own business profits, and probably functioning to circumvent financial restrictions on DPRK.

Examples of identified business conducted by elements of database 3:

- Cigarette manufacturers, distributors, etc. transacted with 15 confirmed and calculated nodes.
- Coal and mineral companies transacted with 5 confirmed and calculated nodes.
- Oil companies (wholesalers, storage facilities) transacted with 23 confirmed and calculated nodes.

It was difficult to find evidence of FoP (for example, transfers of dual use goods, involvement of designated end-users) in any of the transactions involving elements of the databases described above.

The Institution's Caveat: This analysis covers probably only a small portion of DPRK financial network activities. DPRK networks almost certainly are much more extensive than database 3.

Key Points

- The networks were based outside DPRK (China, Hong Kong, also elsewhere);
- They appeared to have a high degree of interconnectivity; one network at least appeared to be self-funding.

Case 7: Financing of the Glocom Network (2016)

The following is based on the 2017 final Report of the UN Panel on DPRK established pursuant to resolution 1874 (2009).[79]

An interdiction of an air shipment from China to Ethiopia in July 2016 revealed 45 boxes of military radio communications products and related accessories. Some of the boxes and articles were labeled "Glocom," and almost all the interdicted items had been advertised on the website of the company Global Communications Co (Glocom).

According to the UN Panel, although Glocom is a Malaysia-based company, it is not officially registered there and has no presence at its listed physical address. It is in fact a front company of DPRK company Pan Systems Pyongyang Branch (Pan Systems Pyongyang[80]) linked in turn to a Singaporean company named Pan Systems (S) Pte Ltd (Pan Systems Singapore). The network has two Malaysian-based companies which act on Glocom's behalf: International Golden Services Sdn Bhd and International Global Systems Sdn Bhd (figure 7).

Payments made by the network

According to the UN Panel, Pan Systems Pyongyang and its front companies used a global network of individuals, companies and offshore bank accounts in China, Indonesia, Malaysia, Singapore and the Middle East to procure and market arms and related materiel. Pan Systems Pyongyang used the names of Pan Systems Singapore and International Global Systems to gain access to foreign currency accounts at banks in DPRK, which otherwise would not be available to DPRK companies due to domestic banking rules.

In particular, Pan Systems Pyongyang and its front companies used accounts in US dollars and euros at the UN-designated Daedong Credit Bank in Pyonyang to transfer funds through bank accounts in China to a supply chain of more than 20 companies located primarily on the Chinese mainland; in Hong Kong; and in Singapore.[81] These included transactions by Glocom that were initiated by companies registered in Hong Kong and cleared through US correspondent banks in New York. Payment for a single invoice was often done through a series of installments from multiple front companies.[82]

---

[79] UN Security Council Document S/2017/150.

[80] According to information obtained by the Panel, Pan Systems Pyongyang is operated by the Reconnaissance General Bureau (RGB), the country's main intelligence agency, designated under resolution 2270 (2016) for involvement in DPRK's conventional arms trade.

[81] In recent years procurement by the network shifted almost entirely to companies in China and Hong Kong due to lower prices, stringent Singaporean regulations and more direct logistics.

[82] Para 52, midterm report of the Panel of Experts submitted pursuant to resolution 2345 (2017), 5 September 2017 (UN document S/2017/742).

According to the UN Panel, transactions made on behalf of Daedong Credit Bank by front companies overseas were carried out on the basis of a ledger system similar to that deployed by KKBC and DHID (Case Study 3).[83] Daedong Credit Bank was able to continue to fund procurement overseas despite its designation.

Payments received by the network

Pan Systems Pyongyang regularly received bulk cash transfers. It also received large remittances from an account at a bank in Malaysia, and from companies in DPRK such as Hungbal Trading Co, Kumbong Trading Co and Mubong Trading Co. Transfers were also made from the Shenyang consulate of DPRK. Pan Systems Pyongyang in addition received funds from Korean Mining and Development Trading Corporation (KOMID) and Hyoksin Trading Corporation, both designated by the UN and members of another DPRK procurement network connected with the Reconnaissance General Bureau (see footnote 80).

Financing of Proliferation

The publicly available evidence indicates that the Glocom network is tied to DPRK's arms trade and to circumvention of financial sanctions, rather than to financing of DPRK's WMD program. However, given the network's connections to Daedong Credit Bank, designated under various sanctions regimes for financial support to DPRK's ballistic missile programs, it seems entirely possible that at least part of the network is also involved in this activity.

[83] Ibid para 53.

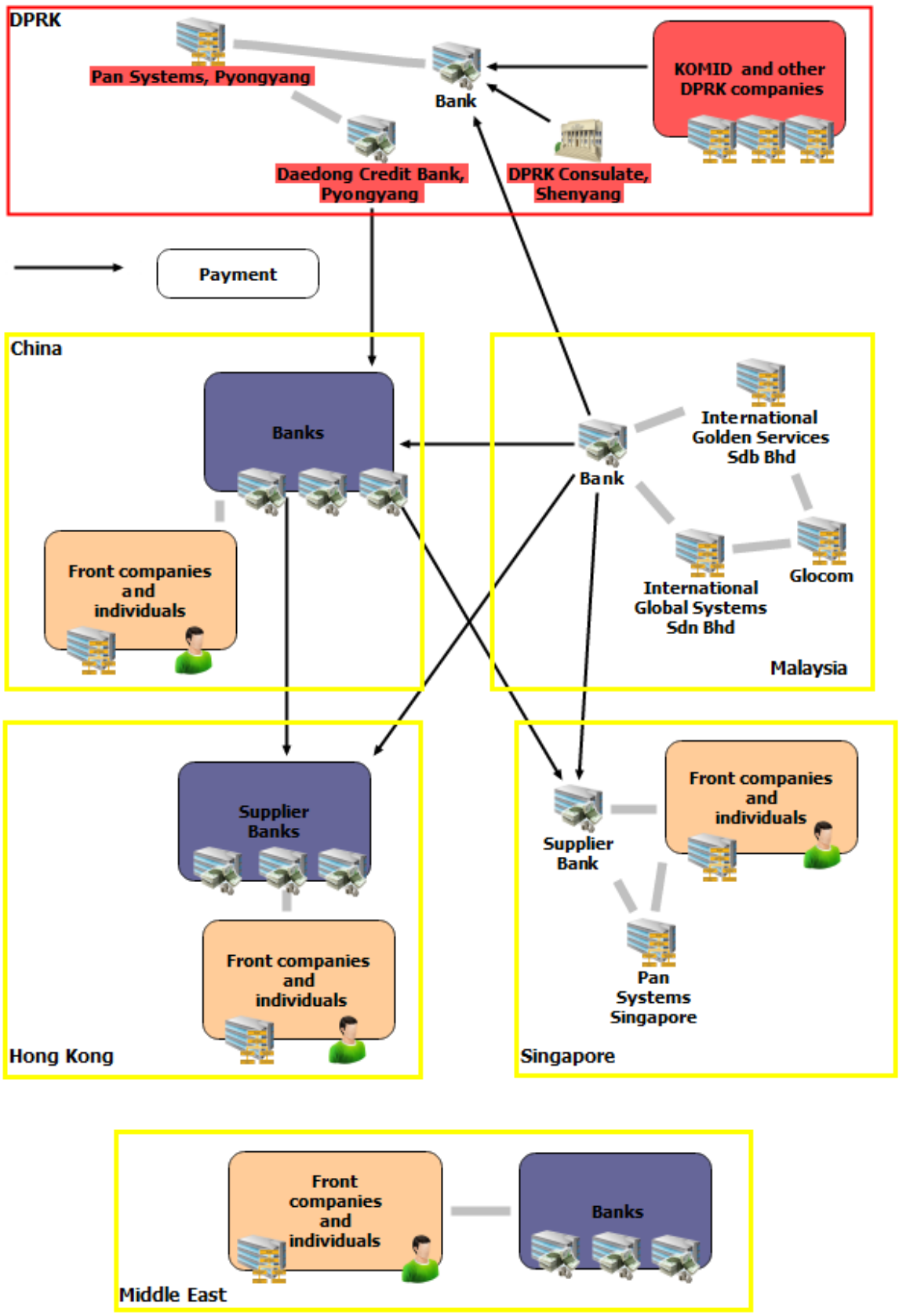

DPRK
Pan Systems, Pyongyang
Bank
KOMID and other DPRK companies
Daedong Credit Bank, Pyongyang
DPRK Consulate, Shenyang
Payment
China
Banks
Front companies and individuals
Bank
International Golden Services Sdb Bhd
International Global Systems Sdn Bhd
Glocom
Malaysia
Supplier Banks
Front companies and individuals
Hong Kong
Supplier Bank
Front companies and individuals
Pan Systems Singapore
Singapore
Front companies and individuals
Banks
Middle East

Figure 7. The procurement network centered on Pan Systems Pyonyang and its front companies

Key Points

- Pan Systems Pyongyang deploys a global network of individuals, companies and offshore bank accounts in China, Indonesia, Malaysia, Singapore and the Middle East for procurement and marketing purposes;
- A designated bank in Pyonyang, (Daedong Credit Bank), conducts transactions in US dollars and euros through bank accounts in China to suppliers in China, Hong Kong and Singapore. A “ledger” system is utilized to facilitate these;
- A single invoice may be covered by payments from multiple front companies (a pattern similar to Case 26).

Case 8: Characteristics of DPRK financial networks determined by a financial institution (2017)

The following is based on the investigative experience of a multinational financial institution.

The financial institution had found a number of common characteristics of financial networks that appeared connected to DPRK (and consistent with recent open source reporting on the subject[84]):

- A high proportion of the entities involved were Chinese. Many of these included a director who was ethnically DPRK (identified as such mainly by name since many held Chinese identity documents). Many were set up initially with Chinese directors after which directors with DPRK connections were added; Chinese entities were mainly based in Dandong and other border regions, and these entities often had directors in common or business addresses in common;
- A small proportion of entities were based outside China, mainly in SE Asia;
- Many of the entities ceased trading activity shortly after their creation, for example after 18 months;
- Goods and material traded by the networks included metals, chemicals and related products and foodstuffs. The networks often funded themselves through such trading and required minimal external funding;
- Individual commercial entities set up multiple bank accounts. Interbank transfers ("self to self"), with no obvious purpose, were common.[85] Personal accounts were rarely used for transactions;
- In many cases trade carried out by entities within the networks did not match their expected business profile (e.g. industrial goods traded by a company that normally dealt with agricultural products);
- Cash transactions were a feature of the networks (the sums tended to be moderate, for example $10ks, $100ks).

[84] For example, "Risky Business: A System-Level Analysis of the North Korean Proliferation Financing System." C4ADS, 2017.

[85] The financial institution agreed the plausibility of the proposition that these interbank transfers were the external manifestations of some sort of internal "ledger system", or value transfer system, that these companies were operating.

Case 9: Mechanisms to circumvent financial sanctions described by UN Panel on DPRK (2017)

The following is based on the 2017 Final Report of UN Panel on DPRK established pursuant to resolution 1874 (2009).[86]

The UN Panel identified multiple ways in which DPRK financial institutions and networks accessed the international banking system in order to circumvent or violate UN Security Council sanctions. These include:

- DPRK banks maintaining correspondent or payable-through accounts with foreign banks;
- DPRK banks forming joint ventures with foreign companies;
- DPRK banks maintaining representative offices overseas;
- Foreign companies establishing banks inside DPRK;
- DPRK trading companies opening bank accounts with foreign banks so as to perform the same financial services as banks (including by providing indirect correspondent bank account services using funds held on deposit);
- DPRK diplomatic missions providing financial support to the networks.

Despite designation by the UN Security Council, several DPRK banks continued to operate abroad by setting up representative offices as corporate entities rather than as financial institutions. For example, Korea Kwangson Banking Corporation (KKBC)[87] operated a branch in Dandong, China, and used the company Dandong Hongxiang Industrial Development Co Ltd to undertake financial transactions in US dollars on its behalf (see Case 3 above).

The Panel had information that showed that two additional banks designated by the UN, Daedong Credit Bank and Korea Daesong Bank, both operate on Chinese territory through representative offices in Dalian, Dandong and Shenyang.

Key Points

- Several DPRK banks continue to operate despite their designations under UN Security Council Chapter VII sanctions regimes;
- DPRK banks are operating abroad through offices of corporate entities.

[86] UN Security Council Document S/2017/150.
[87] Designated under resolution 2270 (2016).

Syria

Case 10: A small broker/intermediary plays a key role in a procurement network (1) (2008-2011)[88]

According to court documents filed in connection with his arrest and conviction, between 2008 and 2011 Individual 1 used his company, Global Parts Supply, Inc, based in Pennsylvania, USA, to export a range of chemical warfare-related agents and other items destined ultimately for Syria.[89] [90] These goods were procured from US suppliers and required US export licenses. They were typically shipped to third countries (UAE, UK, Jordan) against false or misleading invoices; goods and services involved were undervalued or mislabeled, and the purchasers and end-users listed on documentation were usually false.

Payments for the items were made by wire transfers to a Global Parts Supply account at the People's National Bank in the US. The wire transfers issued from banks in Lebanon (including the Lebanon and Gulf Bank of Beirut Central District), and in one case an exchange house (the Zourheir El-Ariss & Sons Exchange, Ras Beirut, Hamra-Adonis Str, Ariss Bldg, Beirut), and in one further case from a bank in Jordan (figure 8).

According to court documents, the wire transfers were typically accompanied by bland descriptions of the transactions they covered, such as "goods value," "laboratory spare parts" and "value of industrial machine spare parts."

[88] This case was Case No 17 in the Interim Report of 5 February 2017.
[89] https://www.ice.gov/doclib/news/releases/2014/140423philadelphia.pdf.
[90] https://www.ice.gov/news/releases/extradited-british-resident-pleads-guilty-conspiracy-illegally-export-restricted.

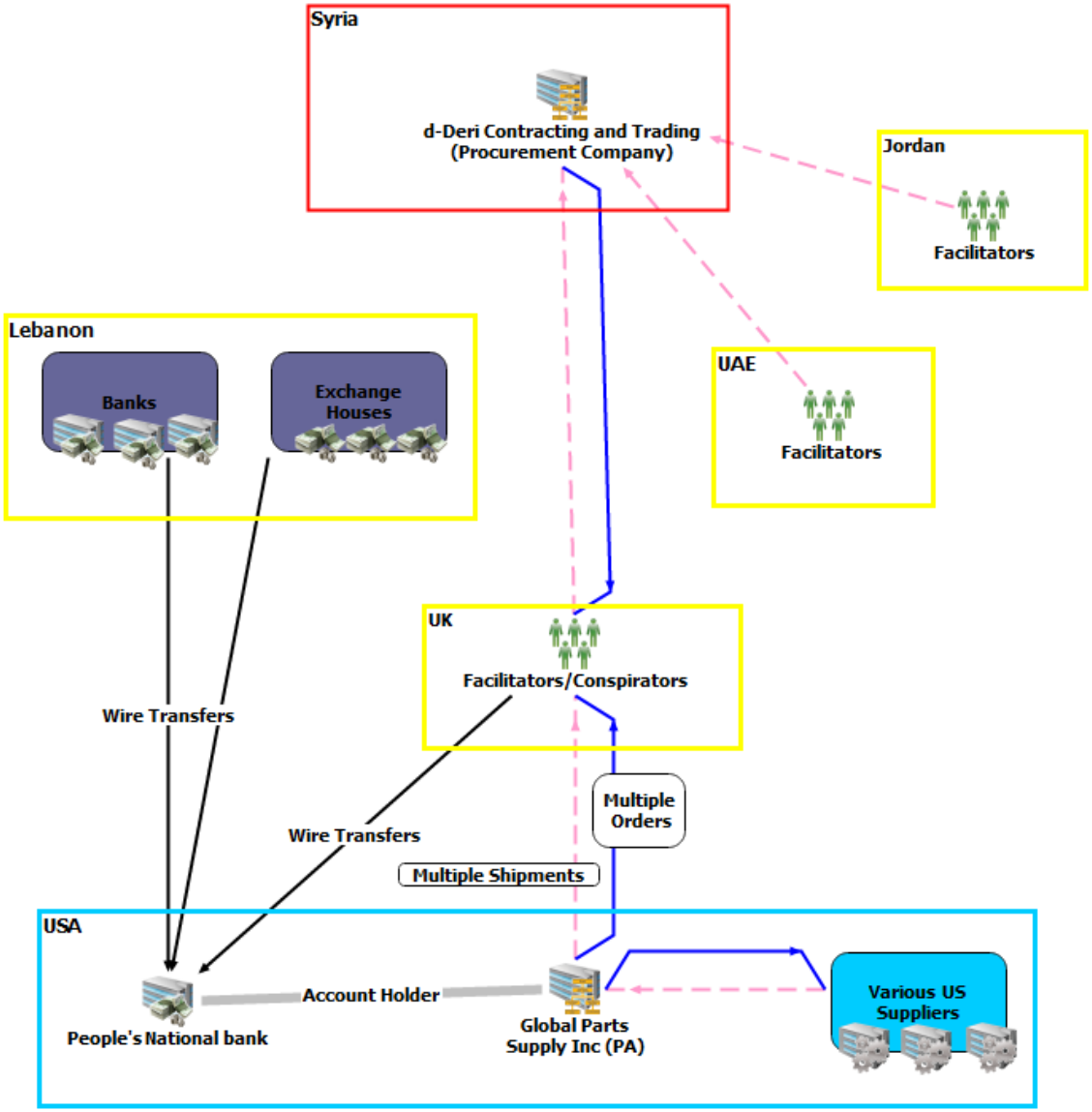


Figure 8. Procurement of chemical warfare-related agents and other items by customers in Syria

Key Points

- A small business acted as a broker/intermediary in this proliferation procurement network;
- Bland descriptions were attached to the wire transfers associated with the proliferation-sensitive goods and materials.[91] The intention may have been to avoid attracting attention;

[91] In the author's experience as a member of the UN Panel on Iran, bland descriptions on documentation were also a characteristic of goods and materials transferred by Iran's proliferation networks.

- Exchange houses were involved in financial transactions;[92]
- Neighboring states were used by the proliferation networks for transit or trans-shipment of goods and related financial transactions.

[92] The involvement of exchange houses in financial transactions associated with proliferation has been highlighted by US Treasury Department: "The Use of Exchange Houses and Trading Companies to Evade U.S. Economic Sanctions Against Iran 10 January 2013" (https://www.treasury.gov/resource-center/sanctions/Programs/Documents/20130110_iran_advisory_exchange_house.pdf).

Case 11: Procurement by the Syrian Scientific Studies and Research Centre (Pre 2011-present)

The following is based on information provided by a governmental source.

The Syrian Scientific Studies and Research Centre (SSRC) has made use of networks of different types to procure WMD-related as well as day-to-day goods and materials from foreign suppliers. Some of these networks previously existed, and some were developed by the SSRC. The networks mutated with time in response to sanctions and other developments.

WMD-related materials procured by these networks included controlled items but also below-control thresholds and non-controlled goods and materials. Controlled items made up about 10% of total WMD-related procurement. The governmental source observed that in early years SSRC procurement was focused on finished goods, including listed goods, but that over time an increasing proportion of procured items are less-sensitive, non-listed raw materials suitable for indigenous WMD manufacture.

Three main stages of network development can be identified.

Phase 1 networks – Procurement through cover companies run by personnel within the SSRC (pre-2011)

The first phase was in use prior to 2011 and before the imposition of sanctions on Syria. In this phase, personnel in the Syrian SSRC Procurement and Customs Clearance Department negotiated and ordered goods and materials directly with foreign suppliers (figure 9). Individual personnel purported to represent different Syrian-based companies, with different cover names.[93] Most suppliers they dealt with were based in China and Asia, but others were in Russia, North Korea, Europe and the US.

The cover companies had no means to transfer funds independently of the SSRC, so once deals were agreed the overseas suppliers were told that payment would be made by a partner company. These partner companies were typically trusts, based in Syria and overseas, including in tax-havens and offshore financial centers.[94] The partner

[93] According to the governmental source, these cover companies included: Industrial Solutions (sanctioned by the EU in 2011 and the US in 2012; Megatrade (Aleppo Street, PO Box 5966, Damascus, Syria, sanctioned by the EU in 2012 and the US in 2014), Experts Partners (Rukn Addin, Saladin Street, Building 5, PO Box 7006, Damascus, Syria) sanctioned by the US in 2014), Sigma Tech (Fayez Mansour Street, Bldg No 35, Floor No 2, Baramkeh, P.O. Box 34081, Damascus, Syria, sanctioned by the US in 2015). One of these cover companies operated with Technolab, a Lebanon-based supplier of science and technology materials (designated by OFAC in 2016, together with its Director General Aziz Allouch).

[94] According to the Governmental source, partner companies included for example Tredwell Marketing, PO Box 3321, Drake Chambers Road, Tortola, British Virgin Islands, registered in 2007. According to media reporting (Syrian BVI Firm linked to Magnitsky case paid Russia USD 37 million, Cyprus Business Mail, 19 June 2017) Tredwell Marketing shared the BVI address with at least one other company suspected of support to the SSRC, Balec Ventures Inc According to the media reporting, the Central Bank of Cyprus

companies were funded by wire transfers from the SSRC (directly from Syria or via Lebanon) and transferred funds to suppliers through accounts with international banks, including in one case an affiliate of a Russian bank in Cyprus. The Syrian source of the funds was concealed to the banks and the suppliers.

Suppliers in Russia or Iran were sometimes paid directly by the Russian Central Bank or the Central Bank of Iran on the basis of a credit arrangement with the Syrian Central Bank and, in the case of the Central Bank of Iran, cash transfers from Syria.

Shipments were typically sent by suppliers to companies in Syria or Lebanon (the companies, usually Hezbollah front companies, changed approximately every 6 months). These companies then transferred shipments directly to Syria. In line with normal commercial practice the front companies sent related shipping documents to the SSRC Procurement and Customs Clearance Department in order to facilitate clearing deliveries through Syrian Customs.[95]

suspected Tredwell Marketing of being a front company for the SSRC.

[95] International courier companies such as DHL were used for this purpose.

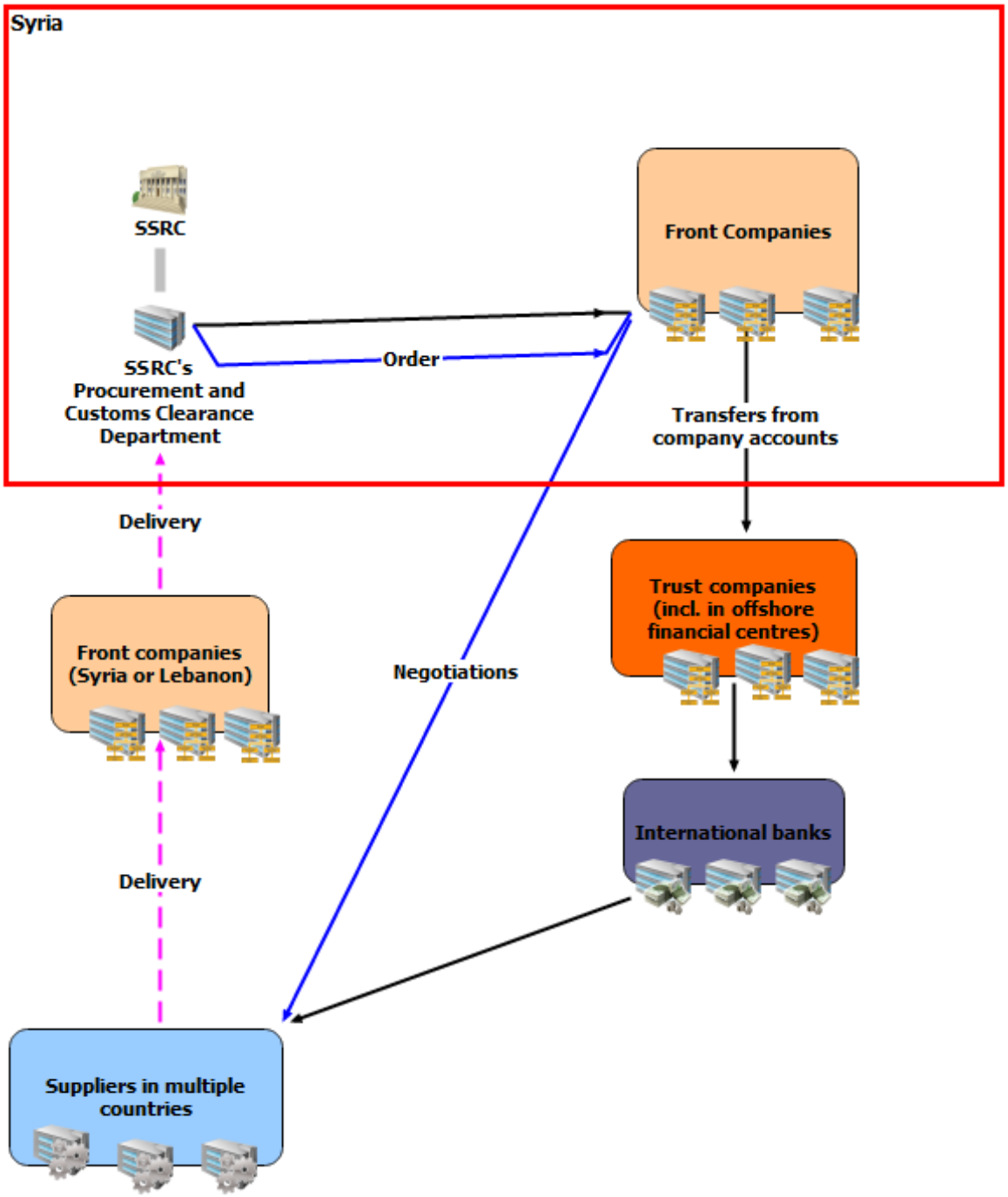


Figure 9. Syrian SSRC Procurement – Phase 1 (pre-2011)

Phase 2 networks – Syrian businessmen act as brokers (2011 to present)

Repeated rounds of sanctions on Syria imposed from 2011 by the US and EU and designations of Syrian SSRC cover companies undermined the effectiveness of the first phase network. It continued in operation but SSRC initiated a second phase of procurement by deploying Syrian businessmen based in Syria, UAE, Lebanon and Turkey to act as brokers. These businessmen fulfilled SSRC procurement requirements by placing orders with suppliers through their existing business contacts (figure 10).[96] They were acting in this way similarly to overseas Iranian businessmen supporting Iranian procurement networks.

The SSRC paid the Syrian brokers in cash. The cash was then effectively laundered through brokers' company bank accounts and payments to suppliers made (in currencies such as US dollars, Japanese Yen, Euros) via banks in Turkey, Lebanon, UAE or elsewhere. No trade financing was involved and suppliers typically released shipments only when payments were received. Sometimes suppliers were paid using money service businesses such as Western Union.

As before, shipments were typically sent to front companies in Syria or Lebanon for transfer to the SSRC.

[96] According to the governmental source, Syrian companies acting in this way included the Houranieh Company and the Anas Group, both important providers for the SSRC of metals and alloys.

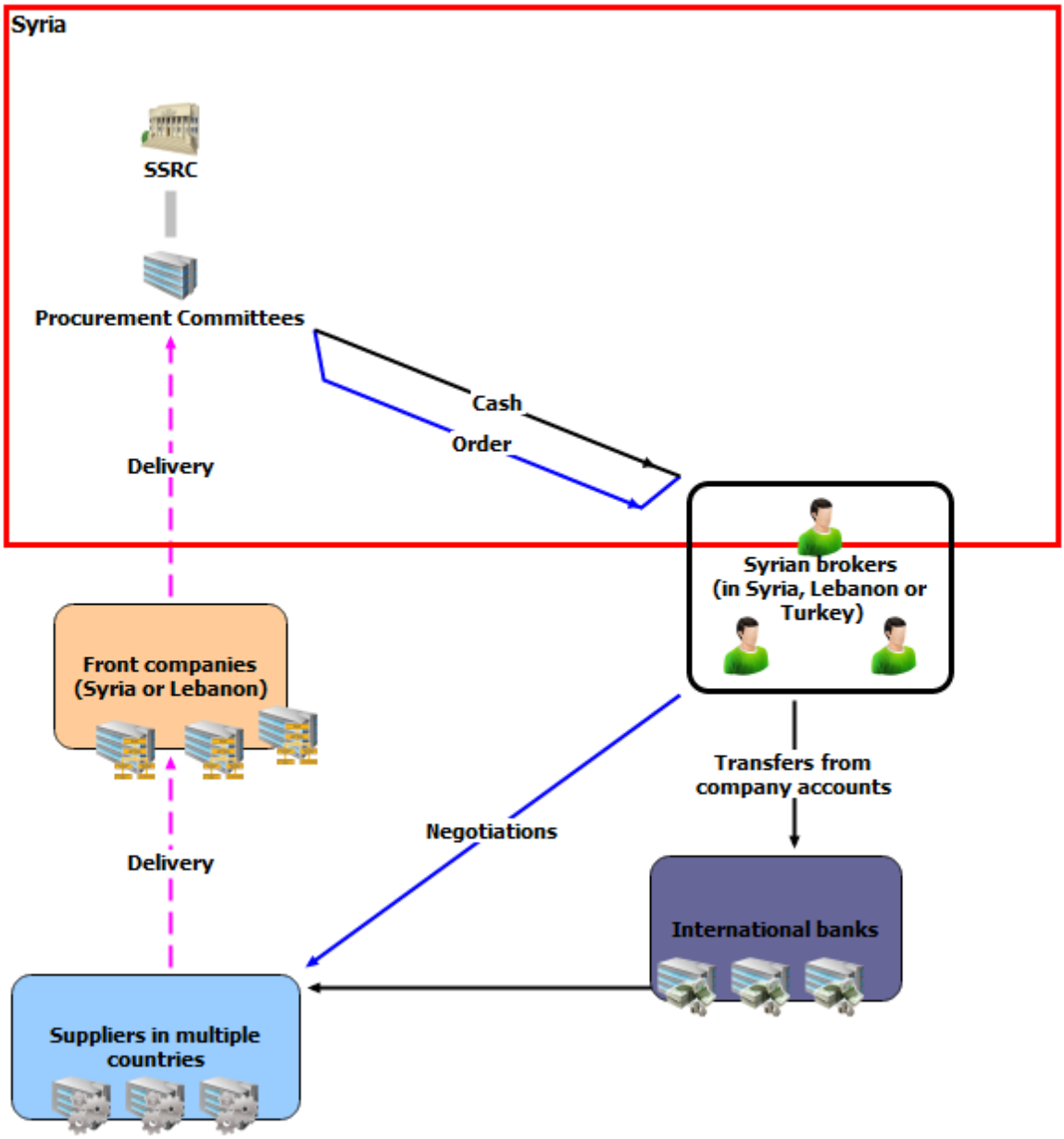


Figure 10. Syrian SSRC Procurement – Phase 2 (2011-2014/15)

Phase 3 networks – Syrian businessmen set up companies in China (2014/15 to present)

Following further rounds of sanctions and interdictions of shipments, SSRC initiated a third phase of procurement in 2014/15. This phase was based on trusted Syrian businessmen acting as procurement intermediaries, in particular to better access the Chinese market. This third phase operated concurrently with phases one and two.

SSRC directors tasked long-standing and trusted Syrian businessmen, who owned companies with subsidiaries in Lebanon, UAE and elsewhere, to set up additional subsidiaries in China and Hong Kong. These new subsidiaries were usually given Chinese names. At least three such networks were created (Figures 11-14).

SSRC directors placed procurement orders with the Syrian businessmen who in turn used their networks of Middle Eastern companies and Chinese subsidiaries to negotiate and agree terms with suppliers. As in Phase Two, the businessmen received cash directly from the SSRC that was transferred to company bank accounts in Syria. The cash was then effectively laundered through the networks either by transfers through formal banking channels or possibly through arrangements to offset payments made on behalf of each other (a “ledger” system). Suppliers were subsequently paid through normal banking channels. Some payments were made via banks in Lebanon and the UAE; others, to Chinese suppliers, were typically made through bank accounts held by the networks in an international bank in Hong Kong.

As before, shipments were sent by the suppliers to front companies in Syria or Lebanon for onward transfer to the SSRC.

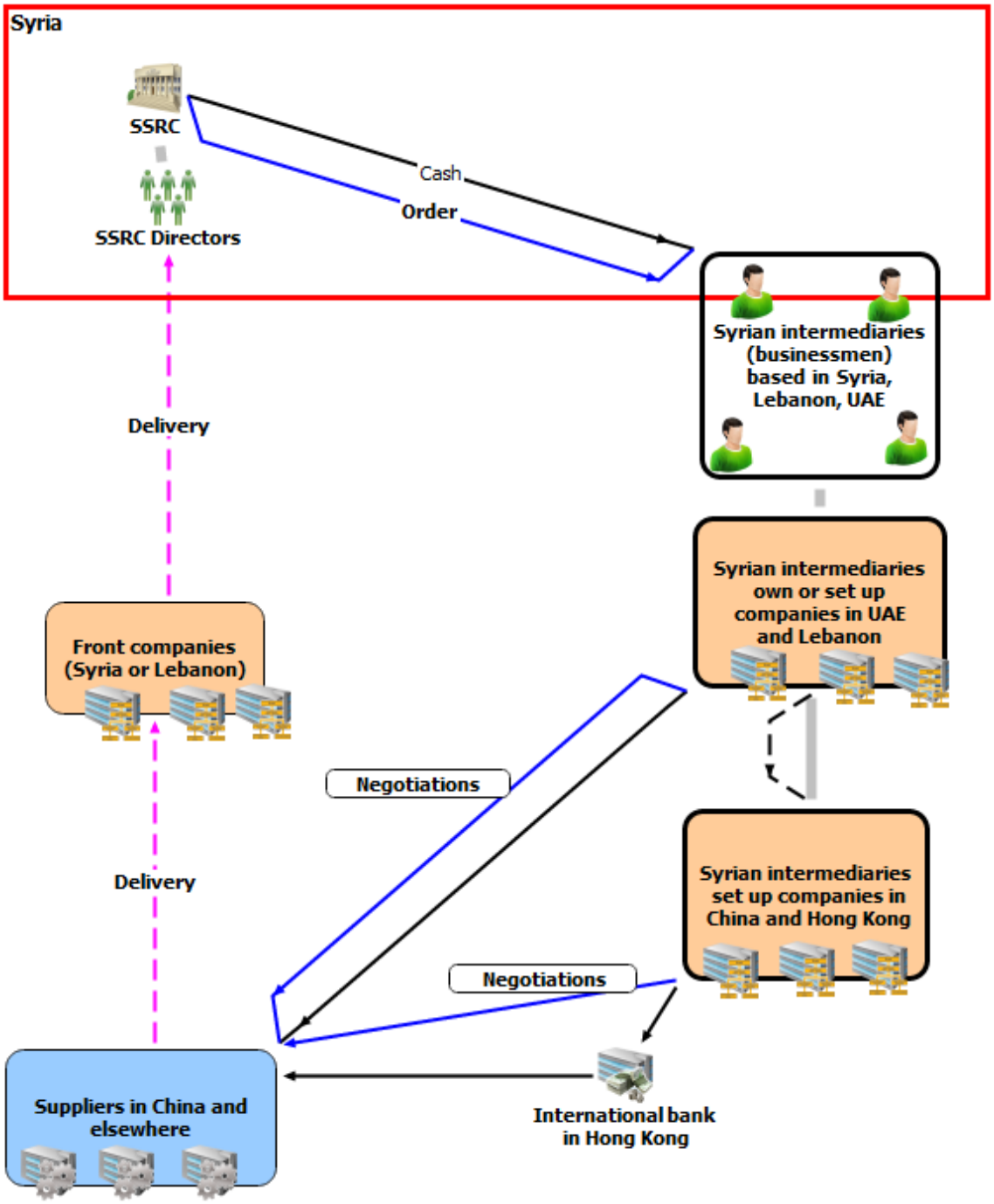


Figure 11. Syrian SSRC Procurement – Phase 3 (from 2014/15) – Overview of networks

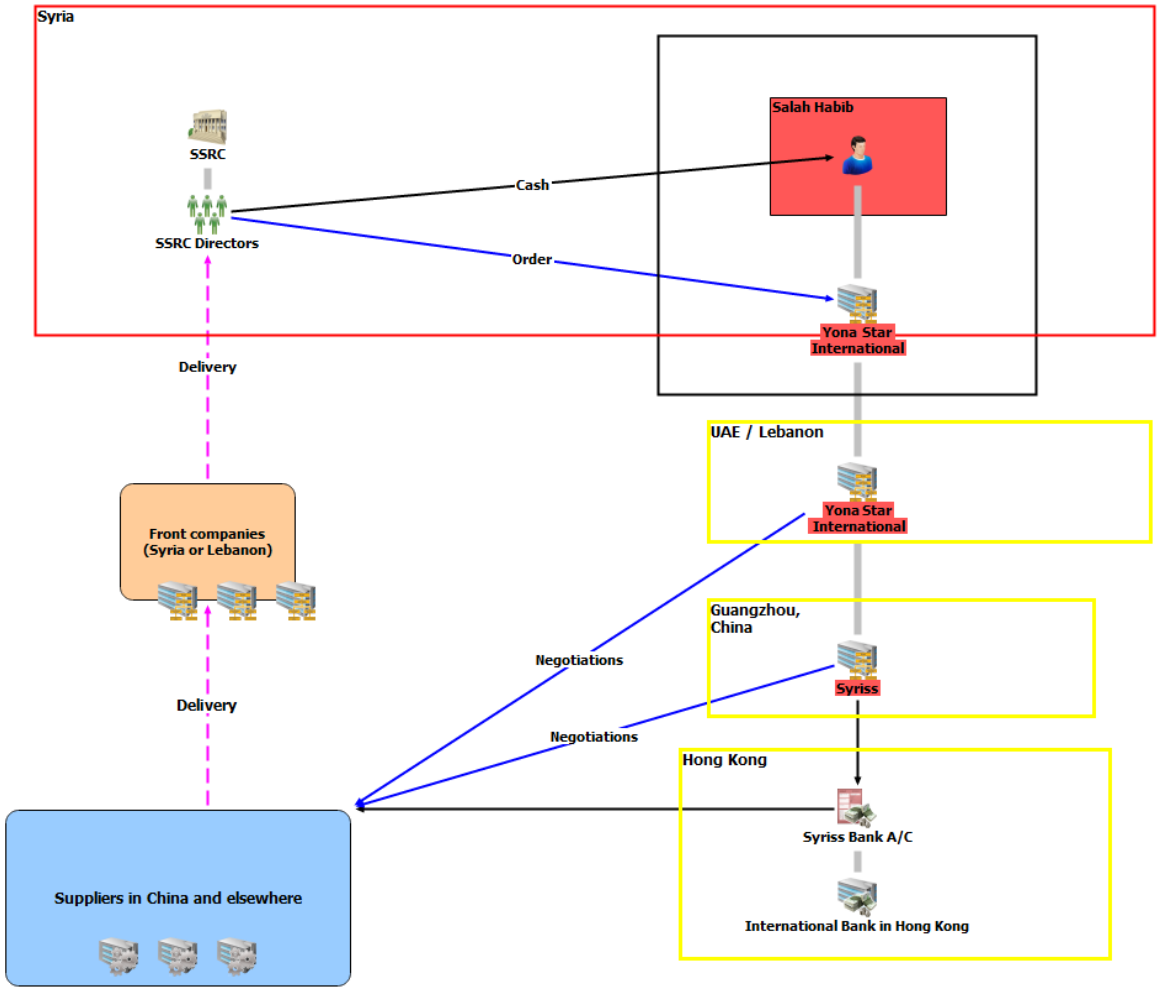


Figure 12. Syrian SSRC Procurement Phase 3, Network 1

(Key: Boxes in red indicate designated individuals or entities; Yona Star International and its managing director, Salah Habib, were designated by OFAC on 21 July 2016; Syriss was designated by OFAC on 23 Dec 2016.)

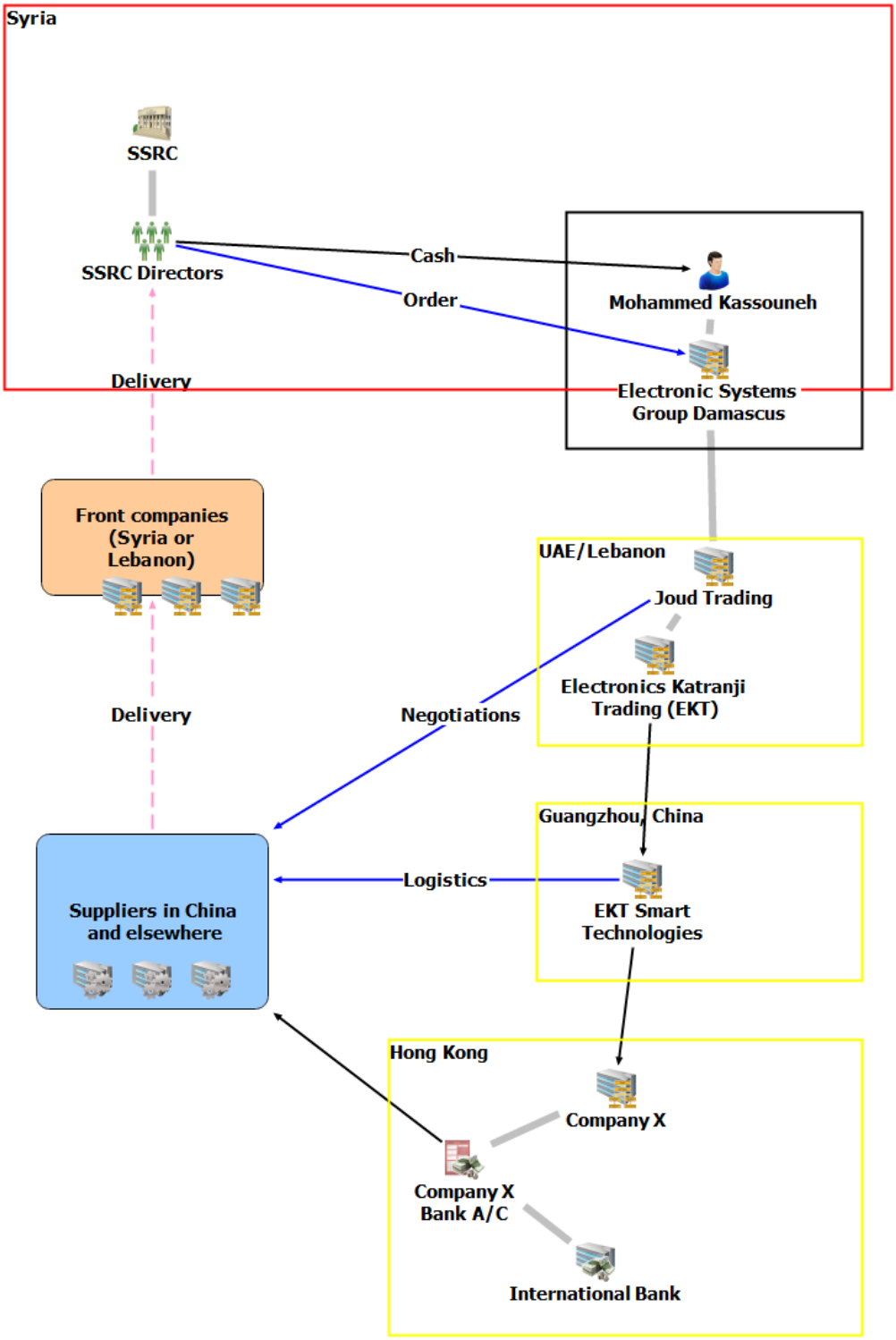


Figure 13. Syrian SSRC Procurement Phase 3, Network 2 (Key: According to the governmental source, Electronic Systems Group, Nasr Street, Damascus, is managed by Mohamed Kassoumeh, and has subsidiaries in Egypt, Kurdistan and the UK; Joud Trading is a shell company run from Syria based at 429 Citibay Business Centre, Dubai; Name of Company X not known).

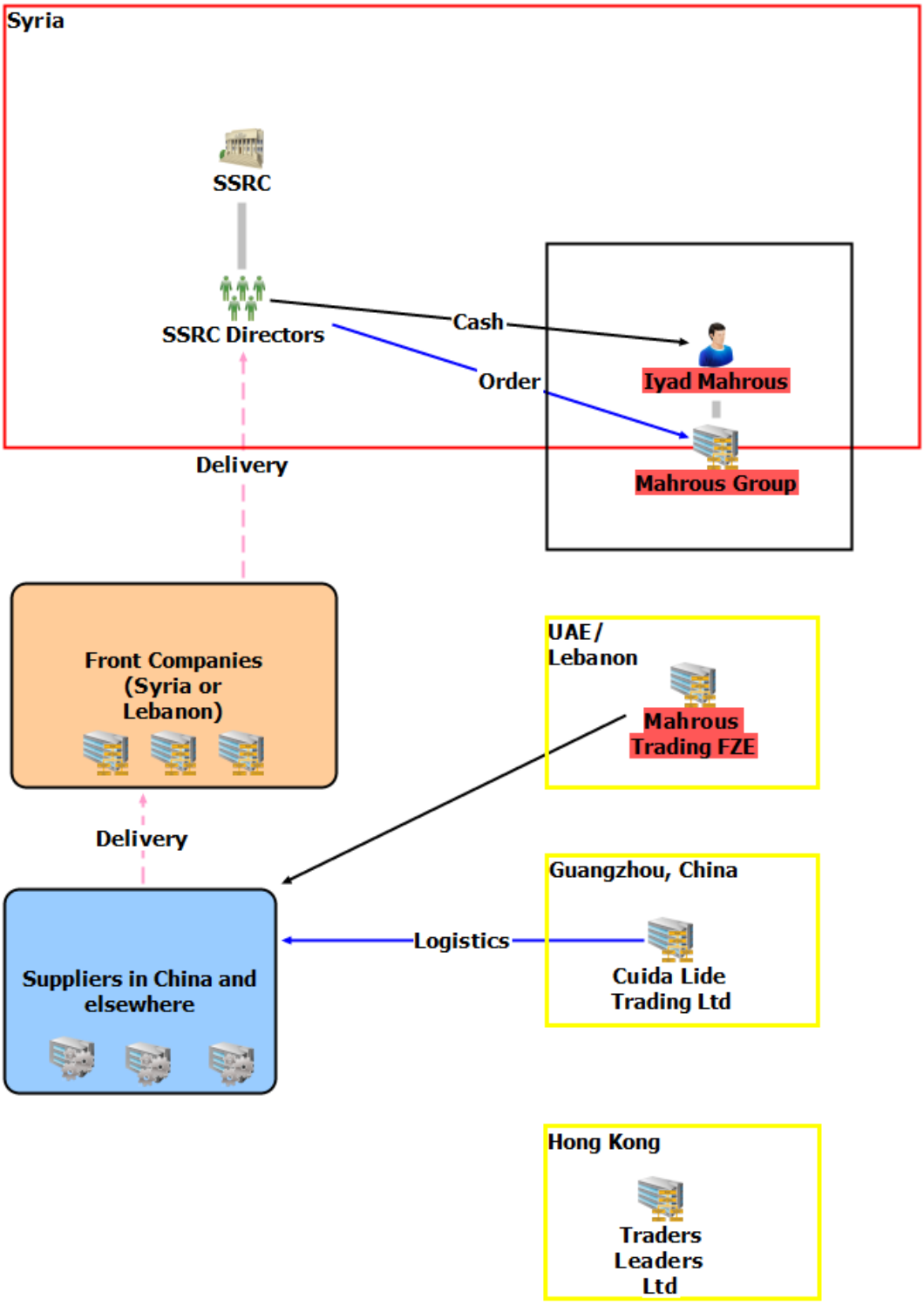


Figure 14. Syrian SSRC Procurement Phase 3, Network 3

(Key: Boxes in red indicate designated individuals or entities; The Mahrous Group, Iyad Mahrous and Mahrous Trading FZE were all designated by OFAC on 21 July 2016)

Key Points

- Syrian SSRC procurement networks are persistent and resilient; they adapted and developed in response to successive rounds of sanctions and designations;
- Many Syrian SSRC front companies and other co-opted companies were based in Syria, Lebanon and Turkey;
- The Syrian SSRC initially paid suppliers through trust companies in overseas tax havens such as British Virgin Islands;
- During the second and third procurement phases Syrian businessmen were paid by the SSRC in cash; this cash was laundered through the businessmen's subsidiary companies to pay suppliers.

Case 12: Procurement to Syria and Iran paid through companies in the UAE (2013)

The following is based on information provided by the Belgian Financial Intelligence Processing Unit (CTIF-CFI).[97]

In 2013, Company A, a Belgian trader in steel products managed by a Belgian national, exported goods to Company C LLC, based in the United Arab Emirates, worth nearly USD 300,000. The invoices drawn up by Company A for Company C mentioned sheets of steel.

Subsequently, an amount of nearly USD 300,000 was transferred to the account of Company A from the account of another company based in the United Arab Emirates, Company B LLC. The transfers referenced sheets of steel.

Following investigations, Belgian authorities determined that the final destinations of the goods exported by Company A was in fact Syria and Iran (figure 15).

Company B LLC (ordering the transfer of funds) and Company C LLC (referenced on the invoices) had their offices in the United Arab Emirates, probably at the same location as they used the same postal address. These companies were part of a group based in the Middle East, providing services to the offshore oil and gas industry. Company B LLC was said to manufacture ships and "fast patrol boats." Iran was particularly interested in these as assault vehicles.

In accordance with Decision 2012/739/CFSP concerning restrictive measures against Syria, in force at the time, it was prohibited to supply arms and related materials of all types, as well as equipment which might be used for internal repression.

Pursuant to Article 8 of Council Regulation (EU) No 267/2012 of 23 March 2012 concerning restrictive measures against Iran, in force at the time, it was prohibited to supply equipment or technology to any Iranian person, entity or body or for use in Iran.

Belgian authorities concluded that the financial transaction resulted from the sale of goods to embargoed countries via the United Arab Emirates. It was well known to the authorities that companies in the United Arab Emirates were sometimes used as a cover for Iran to acquire (dual-use) goods.

---

[97] According to the Belgian authorities, the banks involved in Cases 12, 21, 37 & 42 reported the transactions for a variety of different reasons, including:

- The transactions were originated by an Iranian company;
- Multiple cash deposits were made into a bank account;
- Negative media information was found about one of the companies involved, and the business sector concerned was sensitive;
- One of the companies involved was identified by the bank with a company listed by OFAC and the EU (the bank subsequently found this identification to be erroneous).

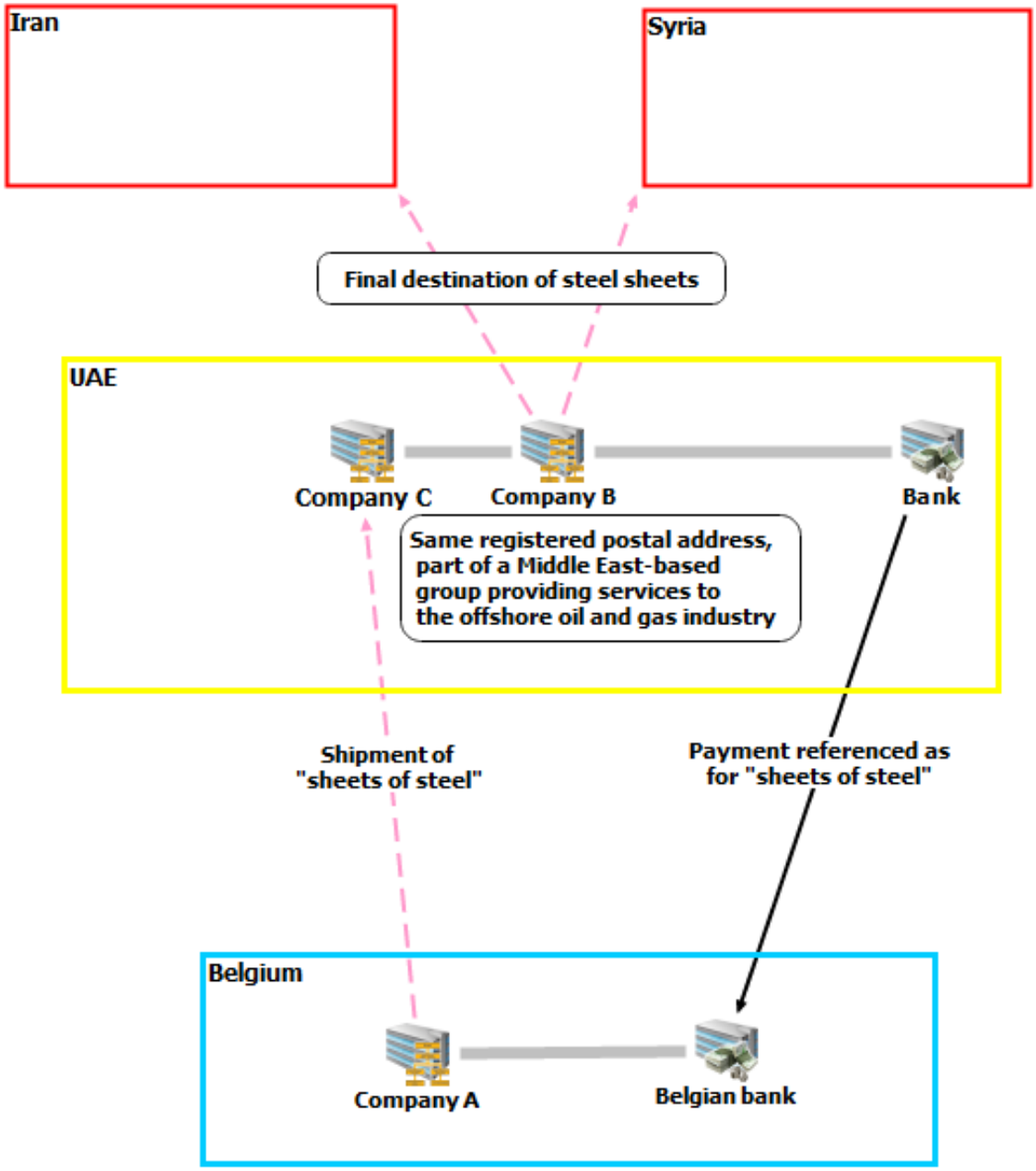


Figure 15. Payment from a bank in the UAE for steel shipments diverted to Iran and Syria

Key Points

- Networks were based in UAE and provided services to the offshore oil and gas industry. They were also used to procure goods and materials that were prohibited for transfer to Iran and Syria;
- Different companies located at the same address were used to order goods and to pay for them.

Iran

Case 13. Financing of Proliferation in 1999: Involvement of universities[98]

Although the purpose of this Study is to identify current typologies of financing of proliferation the following case is included as it shows that some typologies have changed little over the years. This case dates from 1999 and was provided by Swedish authorities to FATF for inclusion in the FATF 2008 Report on Proliferation Financing. The case is described in the 2008 Report as follows:

> In the spring of 1999 the Swedish Customs found out that a person (P) in Halmstad, via a pizzeria, had exported a thyratron to Iran that was classified as a strategic product and therefore was subject to export control. After an audit and interview with P, suspicions grew that it was a question of smuggling.
>
> A search was made in the apartment of P and a seizure of a thyratron was made at Arlanda Airport. It was on its way to a jurisdiction of proliferation concern. Earlier another thyratron was already exported.
>
> P stated that he had been contacted by his cousin in the jurisdiction of proliferation concern in the spring of 1998 who worked at a university in that jurisdiction. The cousin wanted P to get a thyratron to the university. The producer in the United States directed P to the branch in Sweden. P stated he would use it as a degree project at a Swedish university. He forged an end user statement in order to buy the thyratron.
>
> P paid the company 22 000 SEK and delivered the product to Halmstad. P contacted a forwarding company in order for them to export the thyratron to a university in the jurisdiction of proliferation concern. P wrote a pro forma invoice in the name of the pizzeria. The buyer was the university in the jurisdiction of concern. The thyratron was then exported.
>
> In November 1998, P ordered one more thyratron after an order from another university in the jurisdiction of concern. P paid the delivery and in 27 May 1999 the thyratron was delivered to P in Halmstad.
>
> The forwarding company got an assignment to send it to the jurisdiction of concern. The product was not exported because P had not paid the forwarding company for the cost of the freight terminal. P had the impression that Iran Air would once again be responsible for all expenses like last time.
>
> During the preliminary investigation the Swedish Customs found documents like dispatch notes for payment from abroad, inter alia, from the jurisdiction of proliferation concern.

[98] This case was Case No 4 in the Interim Report published 5 February 2017.

Swedish authorities provided the study with additional information as follows (see figure 16):

Individual 1 (referred to as person P in FATF's 2008 report), who originally came from Iran to study in Sweden, owned the Pizzeria Bambino in Halmstad. At one point in 1998 he received an order by telephone for a thyratron from his cousin. His cousin's telephone number placed him in Iran. Individual 1 was instructed by his cousin on how to prepare invoices. Individual 1 also took orders from Glen Mica Co, based in Tehran but Individual 1 was not engaged in any other trade with Iran, nor with other countries, nor within Sweden.

Individual 1 placed an order for a thyratron with a UK company. The UK company sourced the equipment from the US. Following receipt in Sweden on 11 June 1998, Individual 1 repackaged the thyratron and sent it to Amir Kabir University in Tehran.[99] According to open source information at the time, Amir Kabir University was identified as having procured goods and/or technology for weapons of mass destruction programs, in addition to doing non-proliferation related business. Swedish authorities subsequently determined that the thyratron was controlled for export.[100]

Individual 1 received payment for this order on 23 September 1998 by means of a wire transfer originated by an individual in Ontario, via Deutsche Bank.

Individual 1 was subsequently asked to procure a second thyratron. This he also sourced from the UK company and on receipt on 29 May 1999, repackaged it for dispatch to Amir Kabir University. On this occasion he was paid on 18 May 1999 by means of a wire transfer from Chase Manhattan Bank, New York, initiated by another university, the University of Elm va Sanat (University of Science and Technology) in Tehran.

This second thyratron was intercepted by Swedish Customs who subsequently interviewed Individual 1 (his personal details were on the Customs documents). At the request of Swedish Customs following this seizure Amir Kabir University supplied Swedish authorities with an end user certificate for the first thyratron.

Individual 1 also initiated two payments to the account of Individual 2 at Bank Melli, Iran: the first for 6,000 Kr on 2 November 1998 and the second, 8,500 Kr, on 3 March 1999. He also initiated a payment of 8,000 Kr on 26 May 1999 to Individual 3's account at Commerzbank, Hamburg. Swedish authorities speculated that these payments may have been kick-backs.

[99] Amir Kabir University was identified as the Industrial University of Amir Kabir. It possessed a US-supplied research reactor and hot cells.

[100] According to EU regulation 3381/94 Annex 1 item 3A228.

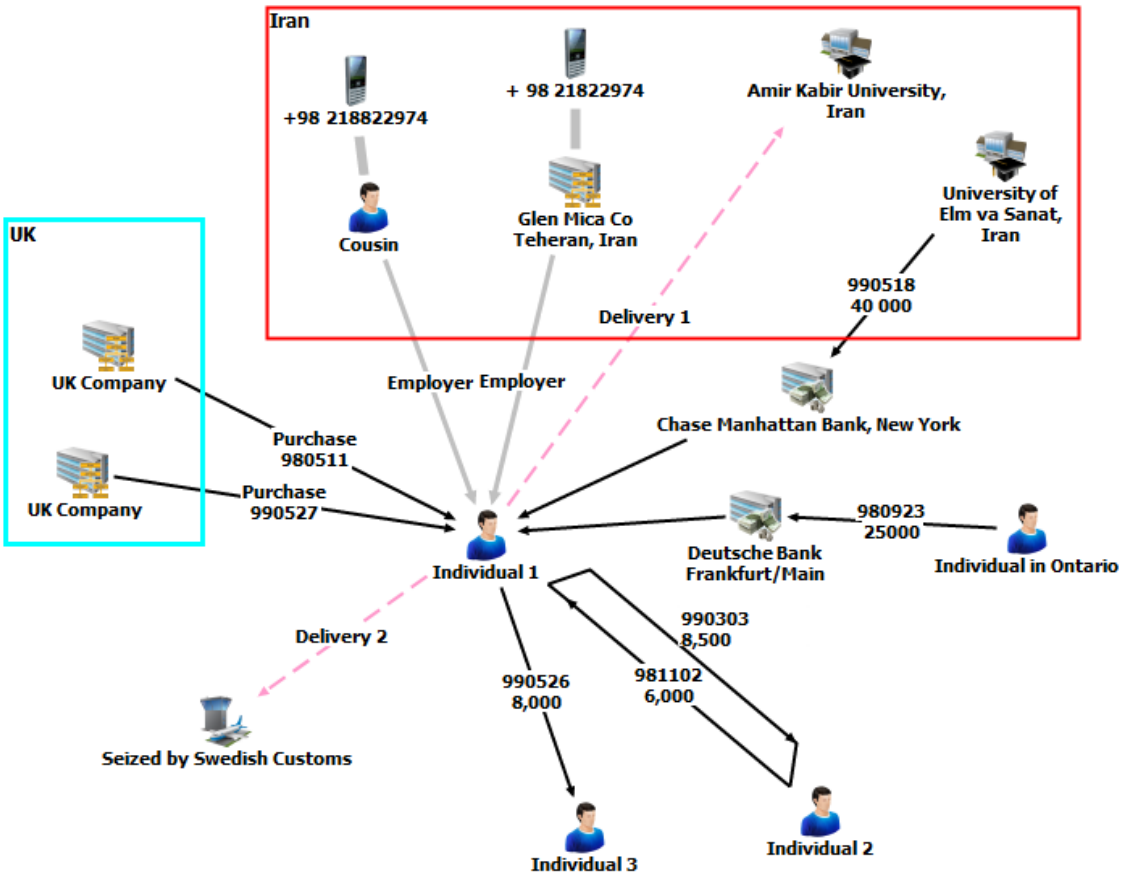


Figure 16. The elements of the thyratron procurement network (adaptation of i2 chart provided by Swedish authorities)

Key Points

- This case involved a national connected with a country under sanctions, and with no technical background in the equipment he was procuring;
- The pizzeria involved in procurement of these products (thyratrons) was clearly carrying out transactions inconsistent with its normal business;
- Channels for payment were far removed from the channels for procurement: the thyratrons were procured via the UK but payments were received via Canada, Germany and the US;
- Universities in Iran were involved in the supply of an end user certificate for the first thyratron, and in initiating payment for the second thyratron.

Case 14: FoP involving networks in multiple jurisdictions in order to obtain US products (2005-2009)

The following is based on information provided by Canadian authorities.

The case began with an open source media article published by a Canadian newspaper. This stated that two Canadian men, Farhoud H. and Ifran A., were indicted in the US on charges relating to trade sanctions violations involving Iran.

According to a grand jury indictment filed in the US in August 2013, the group shipped an assortment of US-made technical and mechanical gear to Iran via Canada, Mexico, the United Arab Emirates and Turkey, between 2005 and 2009. According to the indictment, the end purchaser for some of these items was the Iranian military.

Subsequent investigations by Canadian authorities and analyses of FINTRAC's database revealed that:

- According to media reporting, Farhoud H. would take orders from an Iranian associate on behalf of Iranian companies seeking to acquire sanctioned US technology. Two Canadian entities, Company D and Company B, were named as being involved in the alleged activity;
- Three other companies owned by Farhoud H. and Ifran A. (Company A, Company C, and Company E) were also involved;
- None of these companies appeared to have an online or physical presence;
- The financial patterns (see figure 17) involving Farhoud H., Ifran A. and their companies demonstrated a flow of funds involving numerous entities in several overseas jurisdictions, including to entities in various high-risk jurisdictions;
- Company D ordered EFTs to the benefit of Company Y in Tulsa, Oklahoma and to Company Z in Phoenix, Arizona;
- According to media reporting "using false names and concealing the identity of the end-users of the products Farhoud H. ordered high-tech mechanical equipment from companies in Tulsa, Oklahoma and Phoenix, Arizona."

Based on this pattern of financial activity, it appeared to Canadian authorities that incoming funds from jurisdictions of proliferation concern were being used to acquire sanctioned goods from the USA for transfer to Iran.

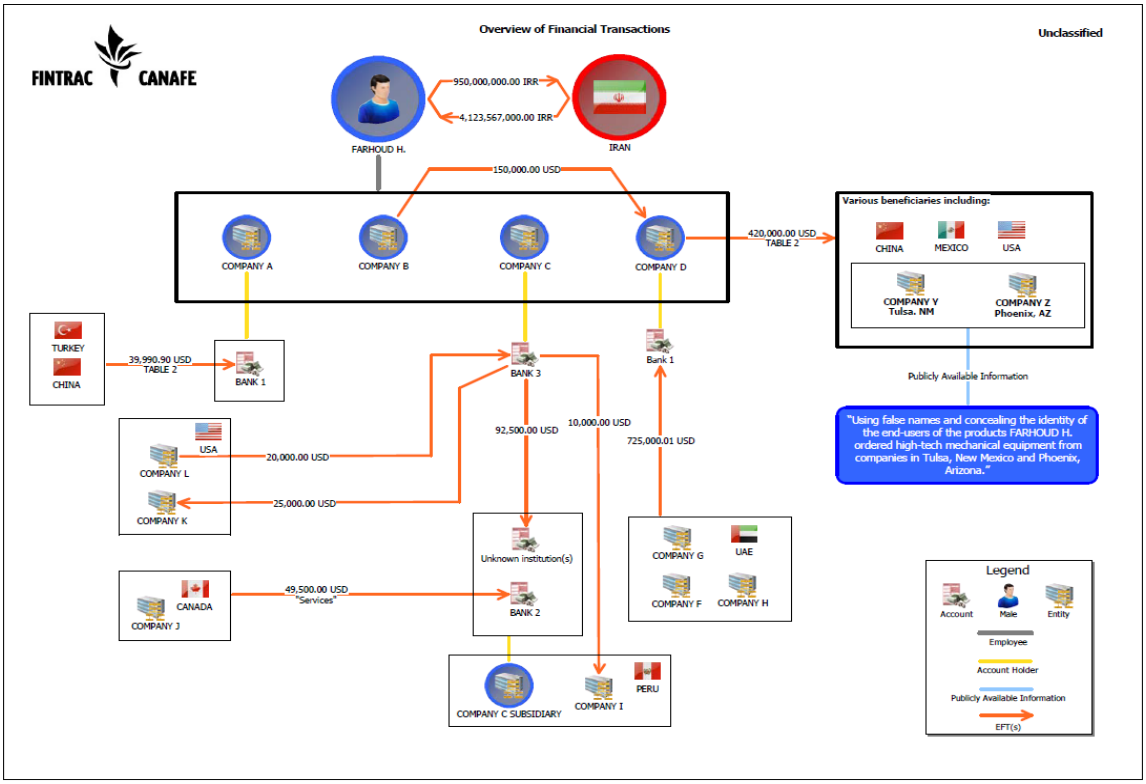


Figure 17. Overview of Financial Transactions (figure provided by Canadian authorities)

Furthermore, based on the adverse media reporting and their account activity, Farhoud H., Ifran A., two additional individuals, Simone P., Khomani A., as well as associated entities, were the subject of Suspicious Transaction Reports (STRs) filed by Canadian reporting entities.

According to the bank's grounds for suspicion when submitting the STR:

> Mr. Farhoud H. allegedly ran companies in Mexico and Canada that obtained American products by using false names and concealing the identity of the end-users of the products. The products were shipped through Turkey or the United Arab Emirates into Iran. The sanctioned goods appear to be relevant in the Iranian oil industry, and the indictment alleges some had potential military uses which ultimately ended up with the Iranian military, constituting a potential threat to national security.

The STRs identified several additional transactions and connections which were of proliferation concern including:

- Wires ordered by Company F in the UAE to the benefit of Farhoud H's Company D.
- Various credit card purchases and payments involving a Visa card held by Farhoud H. including a credit card payment "of USD 230.50 made to Company Z in Phoenix, Arizona, a company specialized in mechanical equipment."

Money-Laundering and Threats Indicators identified by Canadian Authorities

Money-Laundering Indicators

- No internet presence normally to be expected from the type of business conducted by entities owned by Farhoud H. and Ifran A.
- Sending or receiving funds by international transfers involving locations of specific proliferation concern
- Individual wire transactions conducted in large, even dollar amounts.
- Large unexplained movement of funds
- Reporting entity indicated a possible link to criminal activity
- Structuring – amounts transferred below reporting/identification threshold
- Unusual business activity
- Pass-through/in-and-out transactions (i.e. a number of almost equal credits and then debits in a short period of time), e.g. USD 50,000 wired in and then USD 50,000 wired out on the same day

Threat Indicators

- Transaction involves individual or entity in foreign country of proliferation concern
- Transaction involves individual or entity in foreign country of diversion concern
- Order for goods is placed by firms or individuals from foreign countries other than the country of the stated end-user
- Transaction involves individuals or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws
- Canadian individual/entity receives a majority of incoming funds from locations of proliferation or proliferation diversion concern with outgoing funds sent to companies involved in hi-tech, electronics, biosciences or chemicals industries located in highly industrialized countries (i.e. Canada, United States, Europe etc.)
- Transaction demonstrates links between representatives of companies exchanging goods i.e. same owners or management
- Individual has been charged and/or convicted by relevant authorities in relation to import/export violations involving restricted goods
- Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination

Canadian authorities concluded that all of the above indicators helped to give context to the transactions conducted by Farhoud H. and Ifran A., and various related companies and individuals, for the purpose of obtaining controlled technology from the United States. Furthermore, the transactional information corroborated the initial adverse media reporting identifying Farhoud H., Ifran A. and others to be engaged in proliferation activity on behalf of Iranian counterparties.

Case 15: Financing provided by an international organization for biological agents (2006)

The following is based on information provided by Norwegian authorities.

In 2006, an Iranian company approached a Norwegian supplier in order to procure a specific component of a laboratory. The company told the supplier that the laboratory was being built to handle biological agents and was under the sponsorship of the Iranian Veterinary Organisation. The Iranian company first presented the laboratory as designed to be food-stuff related. It was later changed to be described as a regional reference laboratory related to animal diseases.

The Iranian company presented documentation from an international organization confirming the approval and financial support of that organization. The international organization issued a tender on the specific component that the Iranian company sought to buy. This tender also guaranteed payment from or via that same organization.

The Norwegian supplier became concerned that the Iranian company wanted to purchase equipment of much higher specification than apparently needed. Norwegian authorities obtained copies of plans of the physical layout of the laboratory. Assessments suggested that it would be over-designed, unnecessarily expensive and lacking some necessary attributes for its stated purpose. Although it was supposed to be engineered to biological security level 2 or 2+, it appeared to be potentially capable of biological security level 3+ or 3+ Ag – sufficient to handle and develop biological agents suitable for a weapons program.

Norwegian authorities determined that the Iranian company was also ordering equipment for a laboratory from other international suppliers. Some of the orders seemed to be presented as financially supported by the same international organization, but not all.

Norwegian authorities alerted the international organization to the fact that it seemed to have been gravely misled over the purpose of the project.

The products sought by the Iranian company were available in several countries. Norwegian companies are not well known for producing biological equipment; furthermore, Norwegian companies produce high-quality products but at premium prices. The Iranian company was active in its approach and long after the order was rejected, actively tried to persuade the Norwegian company to sell the components.

It should be noted that the Norwegian company reacted to the approach and alerted the relevant authorities in response to outreach previously conducted by the authorities/The Norwegian Police Security Service (PST), to alert businesses to the risk of proliferation activities.

Key Points

- Financing of the biological agents was provided by an international organization;
- The Iranian company involved was persistent in its procurement efforts.

Case 16: Procurement from US involving multiple companies in China (2006-2013)

The following is based on information in a US court document dated 2014.[101]

Li Fang Wei, a Chinese businessman, controlled a large network of industrial companies in eastern China, some of which manufactured metallurgical goods controlled under Nuclear Supplier Group lists. Li used his networks to supply Iran's Defence Industries Organization and Aerospace Industries Organization, and they were (and probably still are) a major contributor to Iran's ballistic missile program.

Li's main company, LIMMT Economic and Trade Co Ltd, was listed by OFAC in 2006. Li himself was designated in 2009. He subsequently built a network of front companies, and since 2006 these companies have carried out more than 165 separate US dollar transactions worth over USD 8.5 million.

Details of Li's numerous front companies, listed in the US court document, are in Table 3. Many of them shared similar names and were based at the same address.

Table 3: Details of Li Fang Wei's front companies

Front Company	Address	Approximate period of use as of 2014
ABC Metallurgy Limited	No 190 Changjiang Road, Dalian, China	2008 - 2009
ABO Trading Co Ltd	China	2010 - 2014
ANSI Metallurgy Industry Co Ltd	No 100, Zhongshan Road, Dalian, China	2007 - 2008
ARA Steel Mills Company	China	2010 - 2014
Blue Sky Industry Corporation	N/A	2007
Dalian Carbon Co Ltd	No 08 F25 Yuexiu Mansion, Xigang District, Dalian, China	2006 - 2014
Dalian Sunny Industry & Trade Co Ltd	No 210 Bayi Road, Dalian, China	2007
Dalian Zenghua Trading Co Ltd	Dalian, China	2010 - 2014
Dalian Zhongchuang Char-White Co Ltd	Room 2501 Yuexiu Building No 82, Xinkai Road, Dalian, China	2010 - 2011
Karat Industry Co Ltd	No 110 Baiyun Street, Dalian, China	2012 - 2014
Liaoning Industry &	N/A	2007 - 2008

[101] Indictment US District Court Southern District of New York 13 CR 00144 filed 28 April 2014, Complaint 14 CV 3015, dated 29 April 2014, US District Court Southern District of New York.

Trade Co Ltd		
LIMMT (Dalian FTZ) Metallurgy and Minerals Co Ltd	2501-2508 Yuexiu Mansion No 82, Xinkai Road, Dalian, China	1998 - 2008
LIMMT (Dalian FZ) Minmetals and Metallurgy Co Ltd	2501-2508 Yuexiu Mansion No 82, Xinkai Road, Dalian, China	1998 - 2008
LIMMT (Dalian) Metallurgy and Minerals Co Ltd	2501-2508 Yuexiu Mansion No 82, Xinkai Road, Dalian, China	1998 - 2008
LIMMT Economic and Trade Co Ltd	2501-2508 Yuexiu Mansion No 82, Xinkai Road, Dalian, China	1998 - 2008
MMN Industry Corporation	899 Shenhe Road Shenyang, Liaoning, China	2010 - 2014
MTTO Industry & Trade Ltd	No 9 Hongji Street, Xi Gang District, Dalian City, China	2011 - 2014
SC (Dalian) Industry & Trade Co Ltd	No 188 Zhongshan Road, Dalian, China	2008
Sino Metallurgy and Minmetals Industry Co Ltd	No 8 F25 Yuexiu Building, Xigang District, Dalian, China	2007
Sinotech (Dalian) Carbon and Graphite Manufacturing Corporation	2501-2508 Yuexiu Mansion, No 82 Xinkai Road, Dalian, China	2011 - 2014
Sinotech Industry Co Ltd	No 190 Changjiang Road, Dalian City, China	2009 - 2014
Success Move Limited	No 1109 Zhongshan Road, Dalian, China	2011 - 2014
Summit Industry Corporation	Xinkai Road, Xigang District, Dalian, China	2006 - 2009
TA Industry Co	China	2010 - 2014
Tereal Industry & Trade Limited	No 9 Hongji Street, Xi Gang District, Dalian City, China	2013 - 2014
Wealthy Ocean Enterprises Ltd	No 08 F25 Yuexiu Mansion, Xigang District, Dalian, Chia	2007

Individual front companies were opened at different times. Many were subsequently closed down. An analysis carried out by the Alpha Project at King's College London suggests that they opened or closed in response to sanctions applied to Li's network by US authorities (see figure 18).

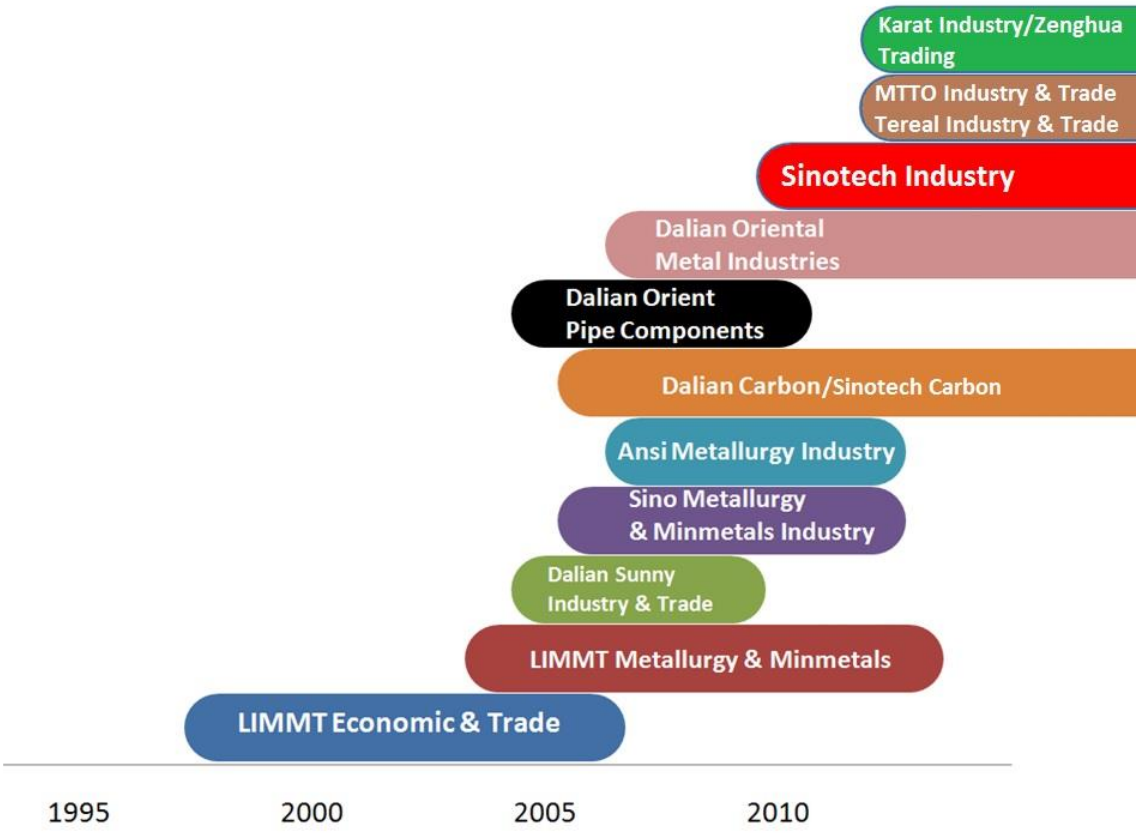


Figure 18. Dates of opening and closing of Li's front companies[102]

According to the court documents, between Jan 2007 and Nov 2013 accounts held by Li Fang Wei or his front companies at Shanghai Development Pudong Bank received about USD 6.9 million through correspondent bank accounts at Citibank, Standard Chartered Bank, JP Morgan Chase Bank, Wells Fargo Bank and Bank of America. In addition, a front company account at the Bank of China received funds through the Bank of China New York.

As an illustration of the way Li operated, according to court documents he caused 35 separate USD transactions, (totaling more than USD 2.4 million) to be carried out on behalf of LIMMT Economic and Trade Co Ltd by one of his front companies, Sino Metallurgy and Minmetals Industry Co. However, when banks began to refuse to facilitate payments through that company, Li switched to other front companies, including Blue Sky Industry Corporation, Wealthy Ocean Enterprises Ltd, Sinotech Industry Co Ltd and MTTO Industry and Trade Ltd.

With one particular customer, Li used five front companies between 2007 and 2012:

- Wealthy Ocean Enterprises Ltd

[102] Daniel Salisbury and Ian J Stewart, Li Fang Wei (Karl Lee), Project Alpha Proliferation Case Study Series 19 May 2014.

- Ansi Metallurgy Industry Co Ltd
- ABC Metallurgy Ltd
- Sinotech industry Co Ltd
- Success Move Ltd

Figure 19 illustrates one example of the way these companies operated. Between 2010 and 2011 Li carried out at least four US dollar transactions with a company in Iran. The Iranian company directed payment to two front companies in Dalian, China, Sinotech Industry Co Ltd and Success Move Ltd, via correspondent banks in the US. In order that the US dollar payments were not blocked by the US correspondent banks, the transactions appeared to originate from an “exchange house” operating outside Iran. The court documents do not state how funds were transmitted to the exchange house from Iran, but it is likely that they were transferred either in cash or via an overseas branch of an Iranian bank.

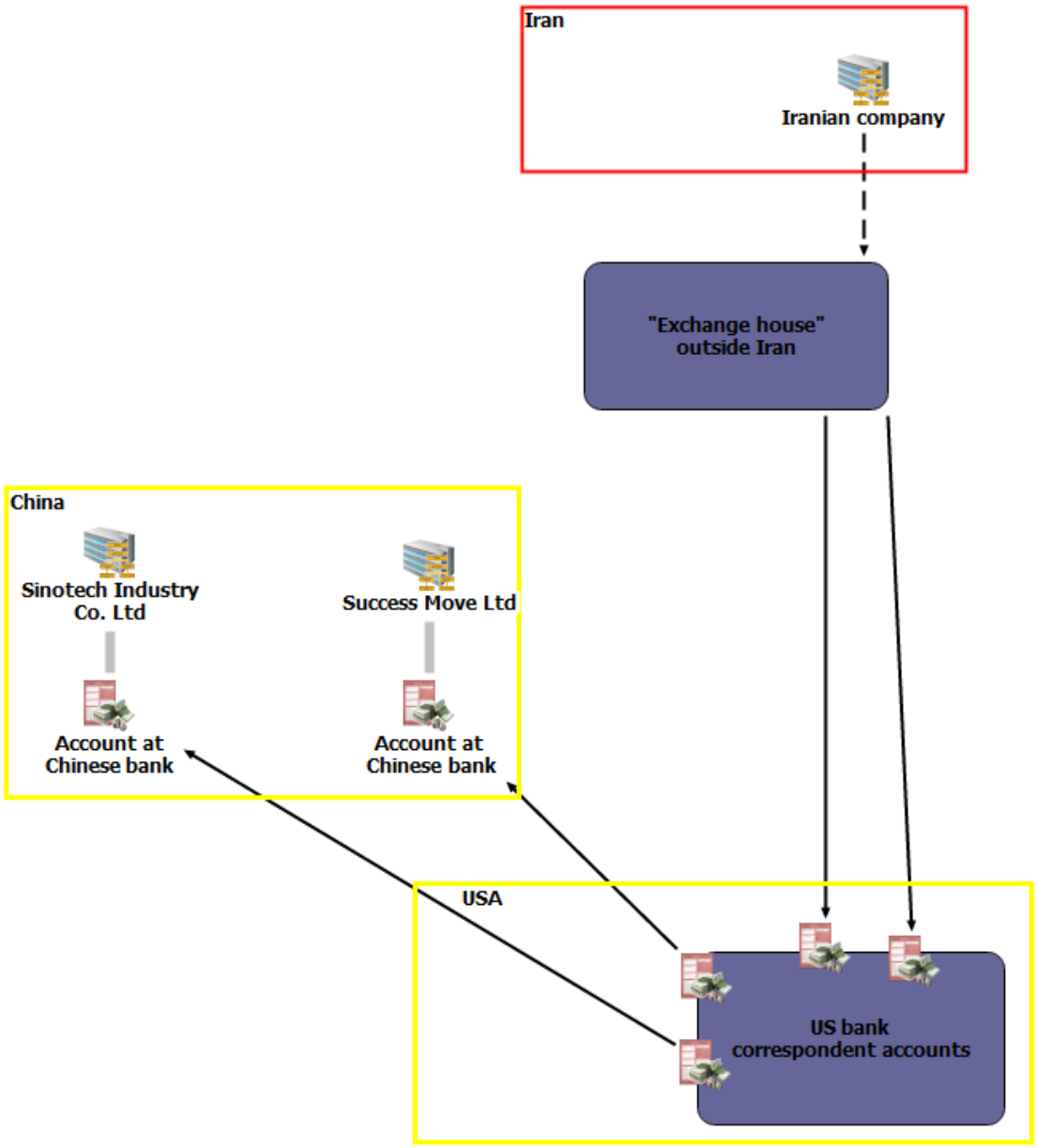


Figure 19. Procurement from companies in China financed through an "exchange house"

Key Points

- Li's network was persistent and resilient – front companies were opened and closed apparently in response to pressure from sanctions;
- Front companies shared similar names and often operated from the same address;
- An exchange house outside Iran was used to transfer funds from a procurer inside the country;
- Li's network was also used for sales to the US of items such as graphite, graphite rods, etc.

Case 17: Activities of a trading company (1): Turning into a money remittance business (2008)[103]

According to Swedish authorities, this case was initiated by an STR in December 2008, when the bank concerned raised awareness in relation to a deposit originating in Iran worth a billion Swedish crowns, and suspected violation of laws on international sanctions.

Individual 1, who came from Iran to Study at university in Sweden, established Aram Company AB in 1986. According to court documents in connection with his conviction in 2010 for accounting fraud, the company was registered with local authorities to conduct, amongst other business, export and import of industrial technical goods and services.[104]

In late-2007 and early-2008, Individual 1 established a business partnership with an Iranian currency broker, whose family had run a currency brokering business in Tehran for several generations. Individual 1 opened foreign currency bank accounts at Swedbank and other banks in Sweden through which funds from the currency broker in Iran were channeled to bank accounts of companies abroad (see Figure 20).

Aram notified the Swedish Financial Services Authority in 2008 that it would also carry out money transfer and currency exchange operations as a financial institution. Its customers would be Iranian small businesses dealing with Europe and China. Payments were to be made through Aram's bank account in a Swedish bank and Aram would receive commissions (about USD 20 for each service, cheaper than a bank would charge).

Between fiscal years 2007-08 and 2009-10, a total of 10,724 transactions amounting to about Kr 11.7 billion (roughly USD 1.3 billion) were processed through Aram accounts at banks in Sweden. By comparison Aram's sales were small.[105]

According to Swedish authorities, the funds was then transferred from Sweden to individuals and companies in countries in the EU, USA, Canada, Japan, China, South Korea, UAE, Russia and other countries. Swedish authorities strongly suspected that some of the transactions were related to proliferation financing, and connected with an investigation in another country about procurement of proliferation-sensitive items. The Iranian currency broker appeared to be a middle-man in a proliferation financing chain.

---

[103] This case was Case No 6 in the Interim Report published 5 February 2017.

[104] This account is based on Umeå District Court records (Case B 58-10 date 3 May 2010).

[105] Aram Company AB reported net sales of about 240,000 Kr in 2007-2008 and 580,000 Kr in 2008-2009 for example, and no sales were reported in 2009-2010.

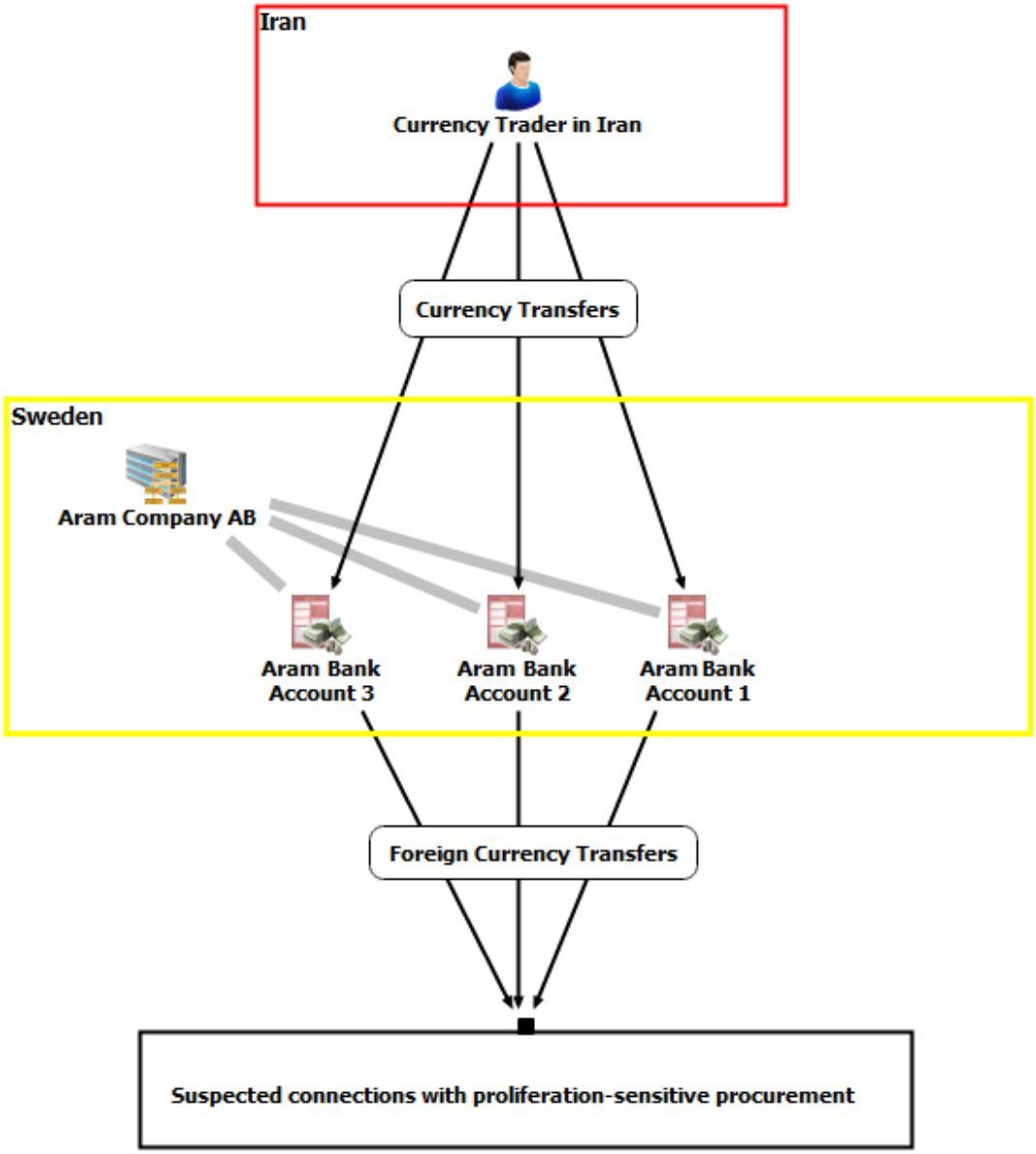


Figure 20. Elements of the Aram Company AB's remittance business

Key Points

- The successful investigation of this case by Swedish authorities was triggered by an STR submitted by a bank based on the fact that the scale of the transactions through the company's bank accounts did not match its stated business;
- The company was acting as an unlicensed money remittance business;
- The owner was connected with the country under sanctions, and managed a small export-import company.

Case 18: Activities of a trading company (2): Extending operations to a neighboring State (2009)

The following is based on information provided by Norwegian authorities.

An individual who originally came from Iran established a trading company in Sweden, Aram Company AB (see Case 17). The individual subsequently opened foreign currency bank accounts in Sweden through which funds from Iran were channeled to bank accounts of companies abroad. Swedish authorities strongly suspected that some of the transactions were related to proliferation financing.

A small number of the transactions from the Swedish account of Aram Company AB went to a handful of Norwegian companies. Some of these produced or sold dual-use goods, mainly with specifications placing them just under the threshold of international export control regulations. The companies carried out limited exports to Iran in the same period, deemed to be in accordance with national and international export regulations.

In 2009 Aram Company AB opened an account in a Norwegian bank. The timing of this coincided with the increasing concern and actions of Swedish banks and authorities. The activities and transfers through the account in the Norwegian bank had similarities to that of the activities in Sweden. There were transfers to a number of countries, to financial institutions, companies and private persons. Norwegian authorities suspected that some of these transactions were related to proliferation financing. Several transactions were reported as STRs.

Based on the suspicious nature of the activity, the Norwegian bank closed down the account and terminated Aram AB as customer of the bank within half a year of its opening. The total amount of funds transferred through the account in Norway was limited.

Key Points

- Typologies of FoP and financial sanctions circumvention in one country were replicated in a neighboring country.

Case 19: Procurement using letters of credit and a front company (2009-2010)

The following is based on information provided by Spanish authorities.

The 2014 Final Report of the UN Panel on Iran[106] includes the following:

> On 23 January 2013, Spain reported that it had initiated an investigation of a Spanish company regarding transfers from Bilbao, Spain, to an alleged front company in Turkey of electrical discharge machine tools and their components... Electrical discharge machines are not included in control lists, except for machines having two or more rotating axes, which is a function of the software used. The end user of the tools was identified as Mapna Turbine Blade Manufacturing Engineering Co, in Tehran. Although export licences were denied by Spanish authorities, seven electrical discharge machines were exported in April 2010. Mapna Turbine Blade Manufacturing Engineering Co is designated by Canada, the United Kingdom and Japan on grounds that it has ties to the Islamic Republic of Iran's prohibited nuclear and ballistic missile programs.

According to business directories and commercial databases, the Mapna Turbine Blade Manufacturing Engineering Co (PARTO) was owned by Iran Power Plants Projects Management-MAPNA, Tehran. MAPNA also owned Company A, based in the UAE. Company A was the parent company of a company set up in March 2009, Company B, based in Turkey.

The Spanish company initially negotiated the sale directly with Mapna Turbine Blade Manufacturing Engineering Co (PARTO) in Tehran. In March 2009, an Export Documentary Credit (Letter of Credit) to cover the sale was originated by a bank in Iran, Bank A. Payment to Bank B, Bank intermediary for this Letter of Credit of the Spanish supplier, was to be made by a bank in UAE, Bank C (Figure 21). Finally, Bank B would transfer the money to the bank account of the Spanish supplier in Bank D. The primary beneficiary was named as Company A in Dubai.

The Spanish company at the same time began negotiations to export the same electrical discharge machine tools and their components to Company B in Turkey. Following denial of export licenses for the sale to Mapna Turbine Blade Manufacturing Engineering Co (PARTO) (due to concerns that the equipment would be used in Iran's nuclear program) the Spanish company arranged for the electrical discharge machine tools and their components to be sent to Company B. Several shipments were made by land, routed through Germany. The machine tools were immediately re-exported from Turkey to Iran.

The Spanish firm told Bank B that the export license had been refused and the original Letter of Credit was cancelled.

However, in parallel with the export operation to Mapna Turbine Blade Manufacturing

[106] UN Security Council document S/2014/394.

Engineering P.J.S. Co (PARTO), another export operation of a wire EDM machine was under way, in this occasion bound for Mapna Turbine Manufacturing Engineering Co (TUGA); export authorized by the Spanish authorities and which would be carried out directly to Iran (although later exports of spare parts for this machine were sent to the Company B).

For this operation, it was tried to reuse the previous Letter of Credit, but MAPNA finally decided to make the payment from France directly to the bank account of Bank D, through the French Bank F, and with the Company A as payer.

A second bank, Bank D, located in a different part of Spain from Bank B, subsequently agreed to a letter of credit from a Turkish Bank, Bank E, to cover export of the same discharge machine tools and their components. This was issued in March 2010. Export declarations in connection with the shipment to Turkey made no reference to the attempted export to Iran.

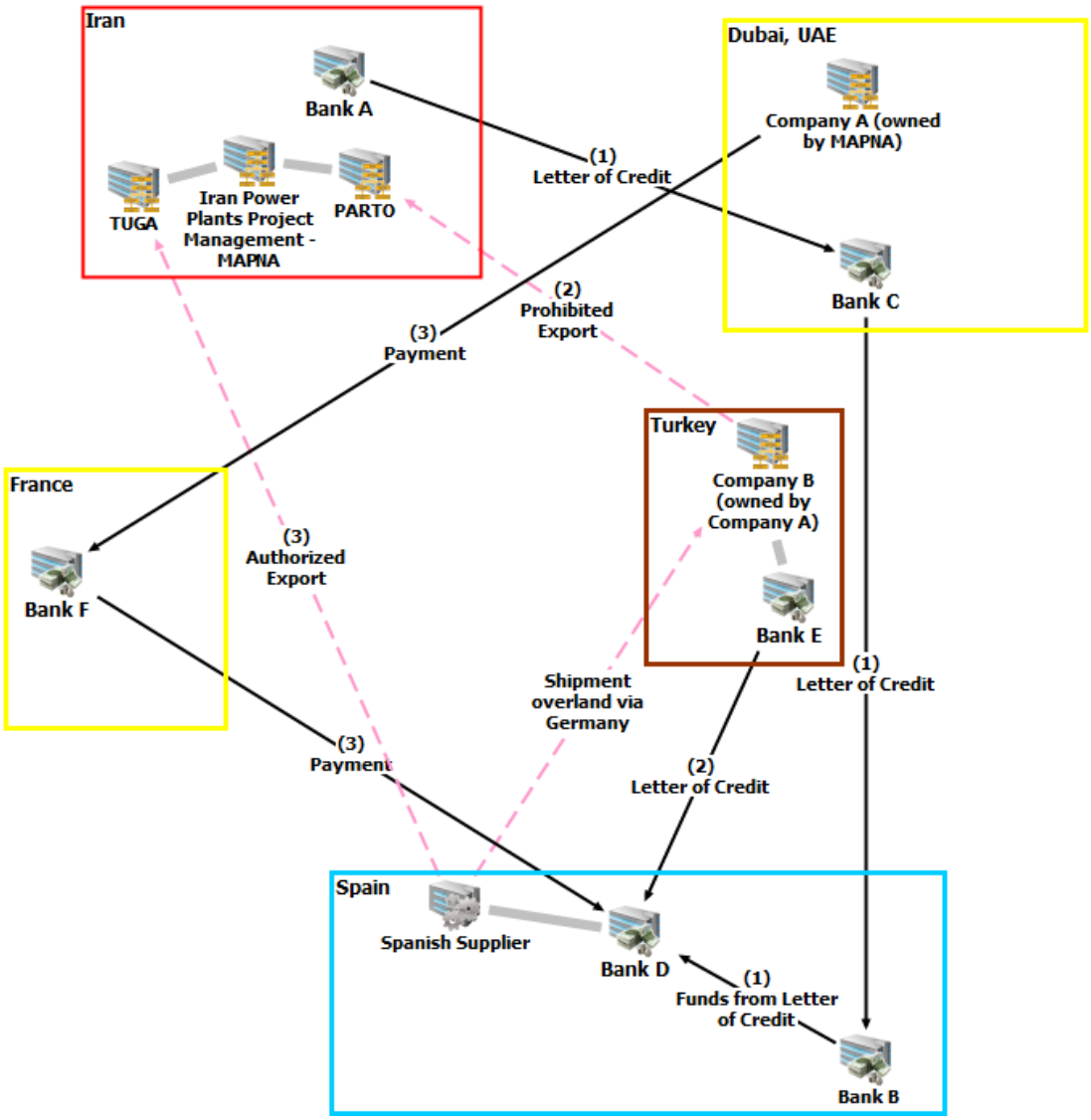


Figure 21. Key: (1) Proposed payment channel for shipment to Iran that was refused export license; (2) Actual payment channel for shipment that was illicitly sent to Iran via Turkey; (3) Payment channel for licensed shipment to Iran

Key Points

- This is a complex case. The company concerned was involved both in licit and illicit shipments to Iran of electrical discharge machines;
- Given the timing of the formation of Company B, it would appear that diversion of the transfer of the machines to Iran via Turkey was possibly pre-planned;
- The Iranian procurer was resourceful over payment arrangements: payment for the original shipment for which the export license was refused involved a letter of credit and a bank in the UAE; payment for the subsequent illicit shipment involved a letter of credit and a bank in Turkey; payment for the separate licit shipment was made by wire transfer through a bank in France.

Case 20: Procurement from EU suppliers by a broker registered in the British Virgin Islands (2009-2012)

The following is based on information supplied by the authorities of an EU Member State.

Procurement by Iran from suppliers in an EU Member State: The investigation of this case took place in 2011/2012, but related transactions can be traced back to 2009.

A broker was involved who was an Iranian and EU national, with a residence in an EU member state and a bank account in the EU member state.

The broker was registered in the British Virgin Islands (BVI) and operated through a front company. This front company could be linked by the Authorities to at least one Iranian company. The front company held an account at a domestic bank in Dubai and also had a bank account in a Balkan state, an EU member (figure 22).

An Iranian bank was the source of funds. Payment was initiated by a branch of this bank in Dubai in the form of a wire transfer to the account of the front company in Dubai. Funds were transferred from this account to suppliers in Luxembourg and also to private persons in several EU member states.

Investigators found no evidence that dual-use goods were involved in any of the financial transactions, but they suspected that the mechanism could be used for proliferation finance.

Iranian customers holding bank accounts in Luxembourg also wired money to the European account of the BVI-based broker. The channels were used more than once in some cases (when European suppliers were involved) and sometimes only once (when private persons were involved).

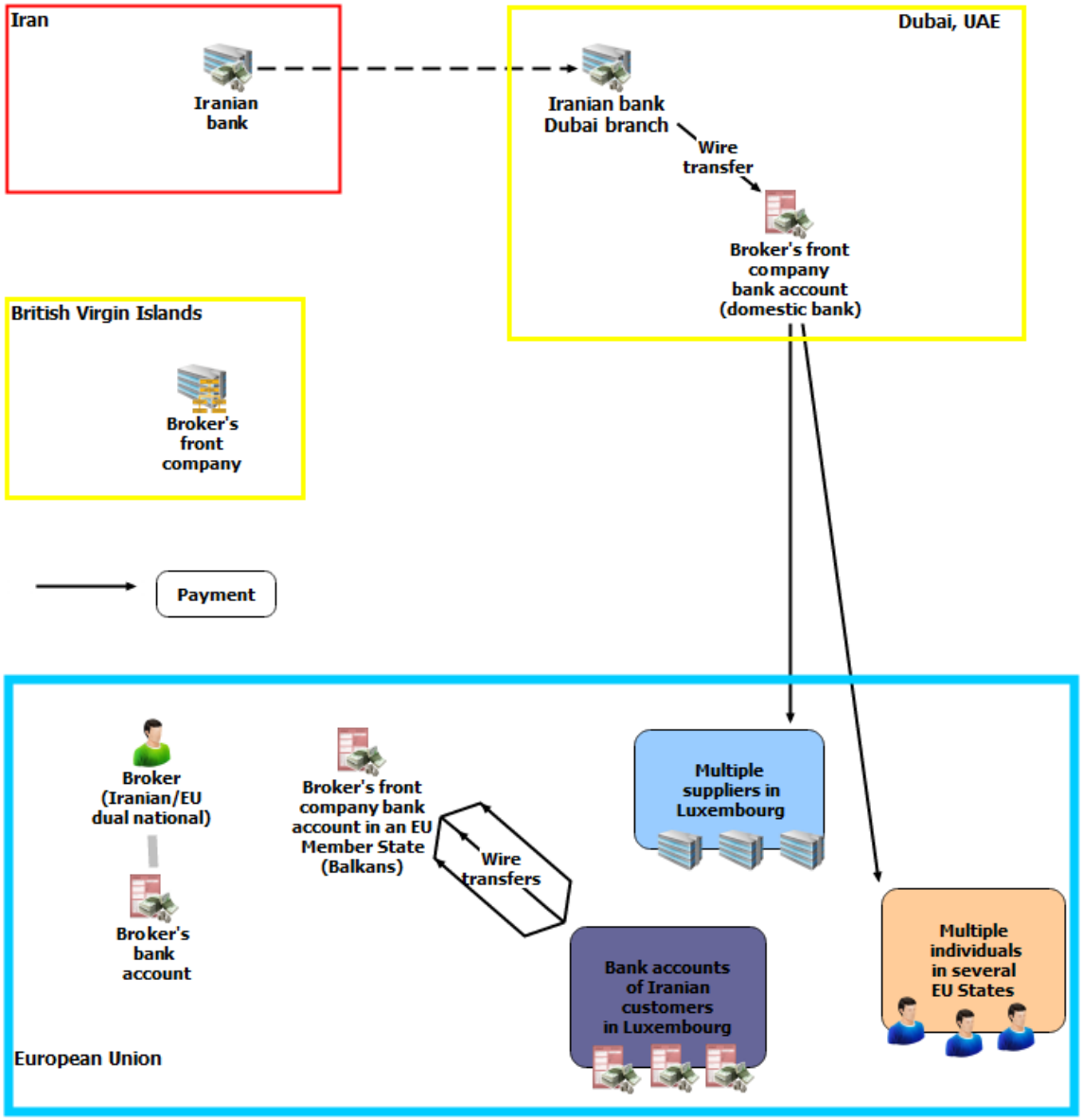


Figure 22. Financing of procurement from EU suppliers by a broker resident in EU and registered in the BVI

Key Points

- The broker, resident in the EU, registered in the BVI, was a dual national of the country of proliferation concern (Iran);
- His front company had bank accounts in the UAE and in the EU (in the Balkans);
- Funding originated with an Iranian bank in the UAE;
- Some of the funding channels apparently passed through bank accounts of private customers in the EU.

Case 21: Procurement of steel financed through bank in Europe (2010-2011)

The following is based on information provided by the Belgian Financial Intelligence Processing Unit (CTIF-CFI).[107]

In 2011, the bank account of a Belgian company A, a steel manufacturer set up at the end of the 1980s and managed by a Belgian national, received a transfer of nearly EUR 225,000 from an Iranian company B, selling products for industrial refrigeration (figure 23). Reference was made to the payment of an invoice. The transaction was carried out via bank X in Iran and bank Y in Western Europe (Germany).

In 2010, company A's account had already received a transfer of some EUR 130,000 from bank Y. This transfer also referred to an invoice but in this case the identity of the initial ordering party was unknown (the identity was not provided by the German bank).

Bank X was included in the consolidated list of persons and entities subject to restrictive measures against Iran set out in Council Regulation (EU) No 961/2010.

Banks X and Y were also included on the Office of Foreign Assets Control (OFAC) Specially Designated Nationals and Blocked Persons List with regard to Iran. These banks were said to be owned by or belonging to the Iranian authorities.

The Iranian company B was suspected of having taken part in building projects for the Iranian air force and navy. This company was also included on the OFAC sanctions list.

Belgian authorities concluded that these transactions could be linked to the financing of proliferation-sensitive nuclear activities or the development of nuclear weapon delivery systems.

[107] See footnote 97.

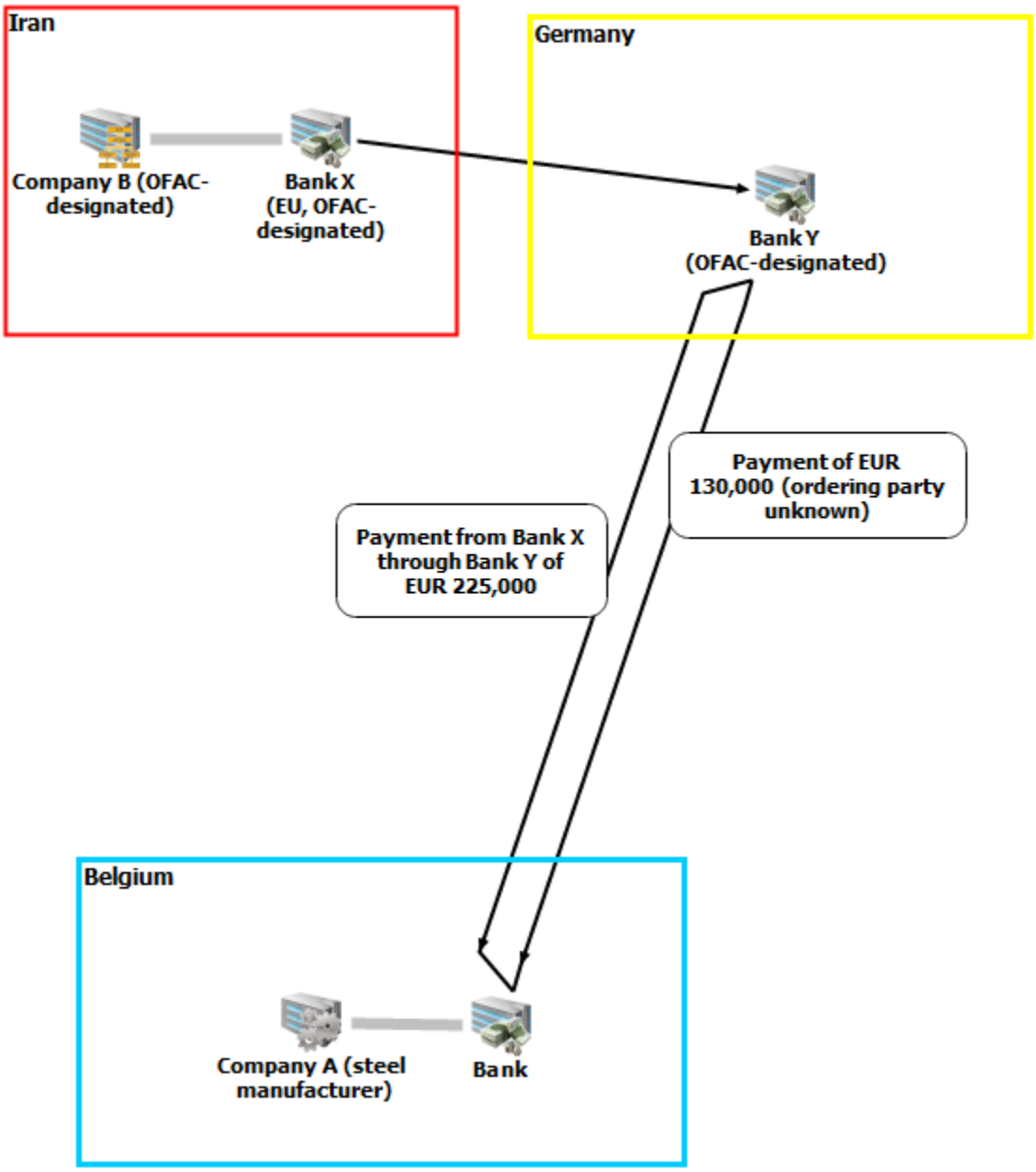


Figure 23. Channel for payments to a steel manufacturer involve designated bank

Key Points

- The transactions involved banks in Iran and Europe designated under different sanctions regimes;
- The steel manufacturer was an established company conducting transactions apparently consistent with its business.

Case 22: Financing of procurement of dual-use valves (2010-2011)[108]

Individual 1, a Swedish-Iranian dual national, managed a company, Petro Instrument HB, registered in 2009 by his wife and brother. The company acted as a procurer of technical equipment. Most of its customers were located in Iran.

Petro Instrument HB initially came to the attention of the authorities on the basis of STRs submitted by two Swedish banks. The reports noted payments to Petro Instrument from Iran, the first in late 2010, and the second in 2011. Investigation by the Swedish Financial Intelligence Unit revealed that Petro Instrument HB had no declared income and that withdrawals from the company's account were mostly in cash.

In 2010, Individual 1 arranged the procurement and shipment of a consignment of valves to a customer in Iran.

The valves, dual-use goods, were to be exported in violation of Swedish export controls.[109] Documentation accompanying the shipment declared it was not dual-use material, but Swedish technical experts established that the valves were in fact dual-use goods. Although manufactured for the petrochemical industry, they could also be used in uranium gas centrifuge enrichments plants (and for this reason were prohibited for transfer to Iran).

Although the air waybill and customs declaration named Sharjah in the UAE as the shipment's final destination, on the day of shipment the air waybill was changed to record the final destination as Tehran. Swedish authorities were not informed of the change.

Swedish authorities, who were already investigating Individual 1, intercepted the shipment before it left the country. A search of Individual 1's office and home by the authorities revealed several examples of export-related declarations and certificates stating that exported goods would not be used for production of nuclear weapons.

Investigation by the authorities determined that Individual 1 had an irregular employment history and no specialized training or knowledge in the engineering equipment he was seeking to procure.[110] He pre-paid most of the shipments to Iran. Initially, he was reimbursed by payments from Iran via a money exchange company in Sweden; later, he was paid through cross border wire-transfers to a Swedish bank account. He received a commission.

He claimed that while on vacation in Dubai he was approached by an Iranian national who suggested he establish a company in Sweden in order to procure items on behalf of Iranian entities.

The authorities determined that the language found on many of the documents discovered in Individual 4's computer during the search of Individual 1's office could be

---

[108] This case was Case No 5 in the Interim Report published 5 February 2017.
[109] Swedish export control regulations based on Regulation (EU) No. 961/2010 relating to Iran.
[110] Paragraph 23, UN Panel on Iran Final Report June 2013 (S/2013/331).

found using Internet search engines, and included language taken from the website of the government's non-proliferation office.

Key Points

- The successful investigation of this case by Swedish authorities was triggered by two banks identifying suspicious transactions and submitting STRs;
- The individual involved was connected to the country under sanctions; he had an irregular employment history and no specialized training or knowledge in the engineering equipment he was seeking to procure;
- His company's financial profile was unusual (no declared income, withdrawals from the bank account in cash);
- Export documentation was falsified.

Case 23: Procurement from US involving companies in east and South East Asia (2010-2015)

The following is based on information contained in US court documents.[111]

The Faratel Co, based in Tehran, was owned and managed by Individual A, a US person, and others. Faratel was involved in procurement of electronics and the design of uninterruptible power supplies. Its customers included the Iranian Ministry of Defence, the Atomic Energy Organization of Iran and the Iranian Centrifuge Technology Company (TESA). Individual A also owned and managed with others a company based in Texas, USA, Smart Power Systems Inc.

Individual B was a manager in the Hosoda Taiwan Co Ltd, a trading company based in Taipei, Taiwan. Individual C operated Golsad Istanbul Trading Ltd, a shipping company based in Istanbul.

Individual A was warned by US authorities on several occasions between 1985 and 2012 about illegal trade activities, but instead of stopping such activities he used the knowledge he had gained to expand business with Iran. According to court documents, between 2010 and 2015 he illegally shipped about 28 million parts valued at about USD 24 million to Iran via Turkey and Taiwan (figure 24). No licenses were applied for. He apparently made millions of dollars profit from the trade.

Individual A and his associates financed these transactions through a variety of means. One such method was for Faratel to initiate payment to Golsad in Turkey; these would then be sent to Hosoda as payment for commodities sent to Faratel. Payments by Faratel in Iranian currency were converted by Golsad to Turkish Lira, Japanese Yen, US dollars and euros before being sent to Taiwan. Faratel then used other foreign companies to wire transfer funds to Singapore and Hong Kong, from where they were transferred to Individual A in Texas.[112]

Techniques used to conceal the transactions included:

- Using cut-out companies (such as Golsad in Turkey) when forwarding items from Taiwan (to avoid paperwork stating that Iran was the destination); these cut-out companies would then forward the items to Iran.
- Using personal emails for correspondence to avoid direct communications between Faratel and companies in Taiwan.
- Mixing export-controlled items with electronic components that were not controlled; mislabeling export-controlled items.
- Transferring funds in weekly amounts under USD 10,000 so as not to draw the

[111] Indictment 15CR204 filed 16 April 2015, United States District Court Southern District of Texas Houston Division.

[112] According to testimony in court, these companies included “third party food distribution companies”, “Why did the US Government give Barham Mechanic a Get-Out-Jail-Free card?” Leif Reigstad, 12 April 2016, The Houston Press.

attention of authorities.

The network was also used to import items to the US, without OFAC licenses.

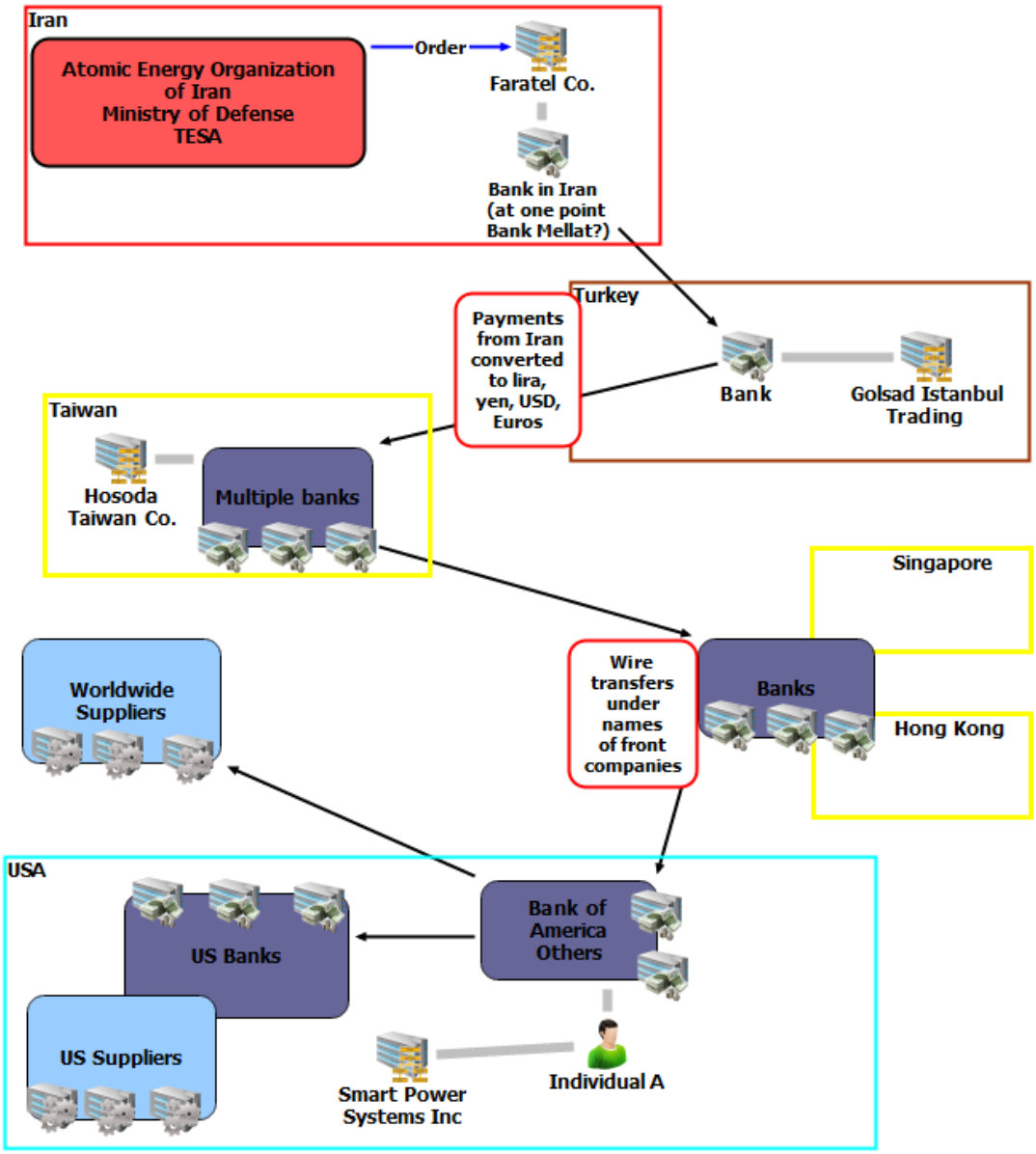


Figure 24. Financing procurement through multiple banks in multiple states. (Key: TESA = Iran Centrifuge Technology Company)

Key Points

- The network was financed by means of multiple banks and companies in multiple countries (including Taiwan, Turkey, Singapore and Hong Kong);
- Cash transfers were structured so as to remain below reporting limits;
- Transfers from Iran in Rials were converted in Turkey to foreign currencies for

transfer overseas (see similar procedures described in Cases 16 and 25);

- The goods involved were mislabeled, and written communications avoided reference to Iran;
- Shipments of controlled goods were mixed with non-controlled goods;
- The network also included companies that would not be subject to sanctions e.g. food distribution companies;
- The network was persistent – it continued to operate despite warnings from US authorities.

Case 24: Procurement network based on control of a bank (2011)

The following is based on information provided by a governmental source.

JSC Investbank in Georgia was set up in 2003. In 2011 the Board was reorganized and three Iranian citizens – Houshang Farsoudeh, Houshang Hosseinpour and Pourya Nayebi – were appointed members although their names did not appear in the bank's formal statutes.[113]

On 6 February 2014, the three Iranians were designated by US Department of Treasury. The Treasury press release at the time stated that:[114]

> …in 2011, they acquired the majority shares in a licensed Georgian bank with direct correspondent ties to other international financial institutions through a Liechtenstein-based foundation they control. They then used the Georgian bank to facilitate transactions worth the equivalent of tens of millions of U.S. dollars for multiple designated Iranian banks, including Bank Melli, Mir Business Bank, Bank Saderat, and Bank Tejarat.
>
> Treasury is also imposing sanctions on eight companies … including: Caucasus Energy (Georgia), [and] KSN Foundation (Liechtenstein)… KSN Foundation was used to disguise the control of the Georgian bank by Nayebi, Hosseinpour, and Farsoudeh…

According to the governmental source, the Iranians used their presence on the Board to establish a network of companies in Georgia involved in activities including transport, metallurgy, money exchanges and trade in precious metals. They relied on extensive networks of commercial financial and maritime structures set up prior to 2011, in New Zealand, Canada, UAE, Turkey and Switzerland (figure 25).

According to the governmental source, in autumn 2011, JSC Investbank purchased a metallurgical manufacturer, Company A, and Individuals A and B were appointed to head the company. The main shareholders of Company A were two Georgian companies, Caucasus Energy Ltd and Company B. Caucasus Energy Ltd was founded by Individual A.

According to the governmental source, Company B and Caucasus Energy Ltd appeared to be front companies set up for the sole purpose of transferring funds to the Company A account at JSC Investbank. Several companies associated with JSC Investbank Directors maintained regular contact with an overseas company, Company C, of which Individual A was a director. It appeared that Company C played a procurement role in the proliferation network that was funded at least in part by JSC Investbank.

The US Treasury actions significantly disrupted the network's activities.

---

[113] The three Iranians acquired 70% shares in the bank (Civil.Ge of 7 Feb 2014, http://www.civil.ge/eng/article.php? id=26923).

[114] https://www.treasury.gov/press-center/press-releases/Pages/jl2287.aspx.

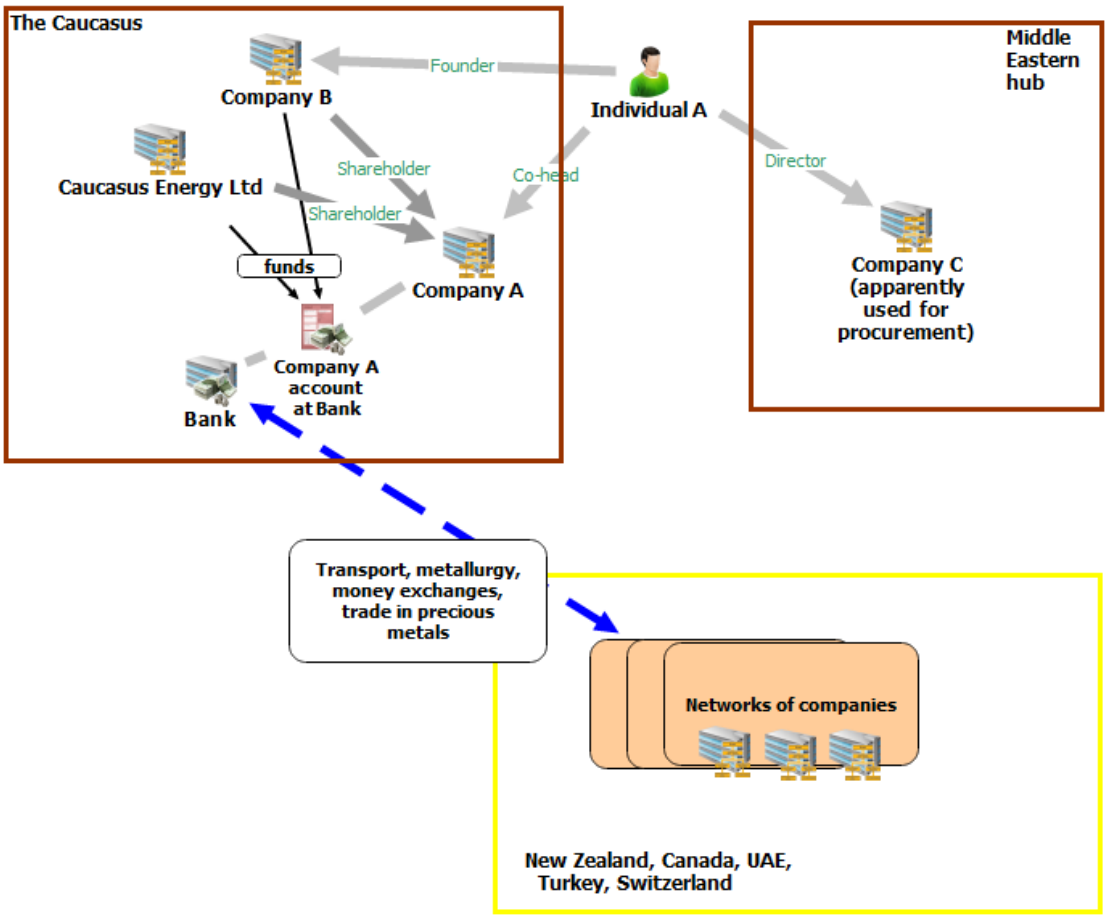


Figure 25. Procurement network based in the Caucasus

Key Points

- A bank appeared to play a central role in the financing of this procurement network;
- The network appeared in part to be self-financing, in a way perhaps similar to some DPRK networks (see for example Cases 6 and 8 above);
- The network made use of both newly-created entities and elements of existing networks overseas.

Case 25: Procurement by a car salesman (2012)

The following is based on information provided by Norwegian authorities.

An Iranian businessman living in Norway managed a small used car business. This involved some, but limited, exports overseas including to Iran. He had family and business contacts in Iran.

In 2012 he contacted a Norwegian company that supplied large, high-quality specialized diesel engines with a broad range of applications. The engines were produced in another European country and were available for sale in many countries. One configuration of a marine model of this engine was highly applicable in high-speed patrol craft, MTBs etc.

The businessman said he acted as a broker on behalf of a company in Georgia. He said he wanted a small number of diesel engines to be used in locomotives. During subsequent negotiations he increased the number of engines he wanted and changed the specifications to marine models. The businessman lacked knowledge of the products he was interested in and seemed to rely on information on the company´s website. This was unusual as these products as a rule are made to a customer's specifications.

The size of the order increased from approximately EUR 1,500 to approximately EUR 2 million. The Norwegian company did not sell any products to the businessman.

Norwegian authorities determined that the businessman was also ordering high tech dual use electrical equipment, suitable for both civilian and military air operations, and specialized rubber valves and other products from Norwegian and other European suppliers (figure 26). Some of these were to be exported to a company in Turkey. Norwegian authorities established that this company was under full control of an Iranian company. Further it was determined that all orders the businessman placed were actually on behalf of Iranian end-users; one of these was the Iranian Ministry of Defence and Armed Force Logistics (MODAFL).[115]

The businessman travelled frequently to Iran, and he brought cash with him back from Iran. The money was declared to customs and each sum was within the limits of the regulations. On one occasion he returned from Iran and declared an amount of cash, and the next day he transferred an almost identical sum of money from his bank account to a European supplier of dual use goods. The total sum of declared cash money within two years was enough to cover most of his orders, but would not cover any orders related to the diesel engines.

[115] MODAFL, which controls the organization responsible for Iran's ballistic missile research and production, was designated by US Treasury on 25 Oct 2007 and by the EU on 23 June 2008 (Council Decision Implementing Article 7(2) of Regulation (EC) No 423/2007 Concerning Restrictive Measures against Iran).

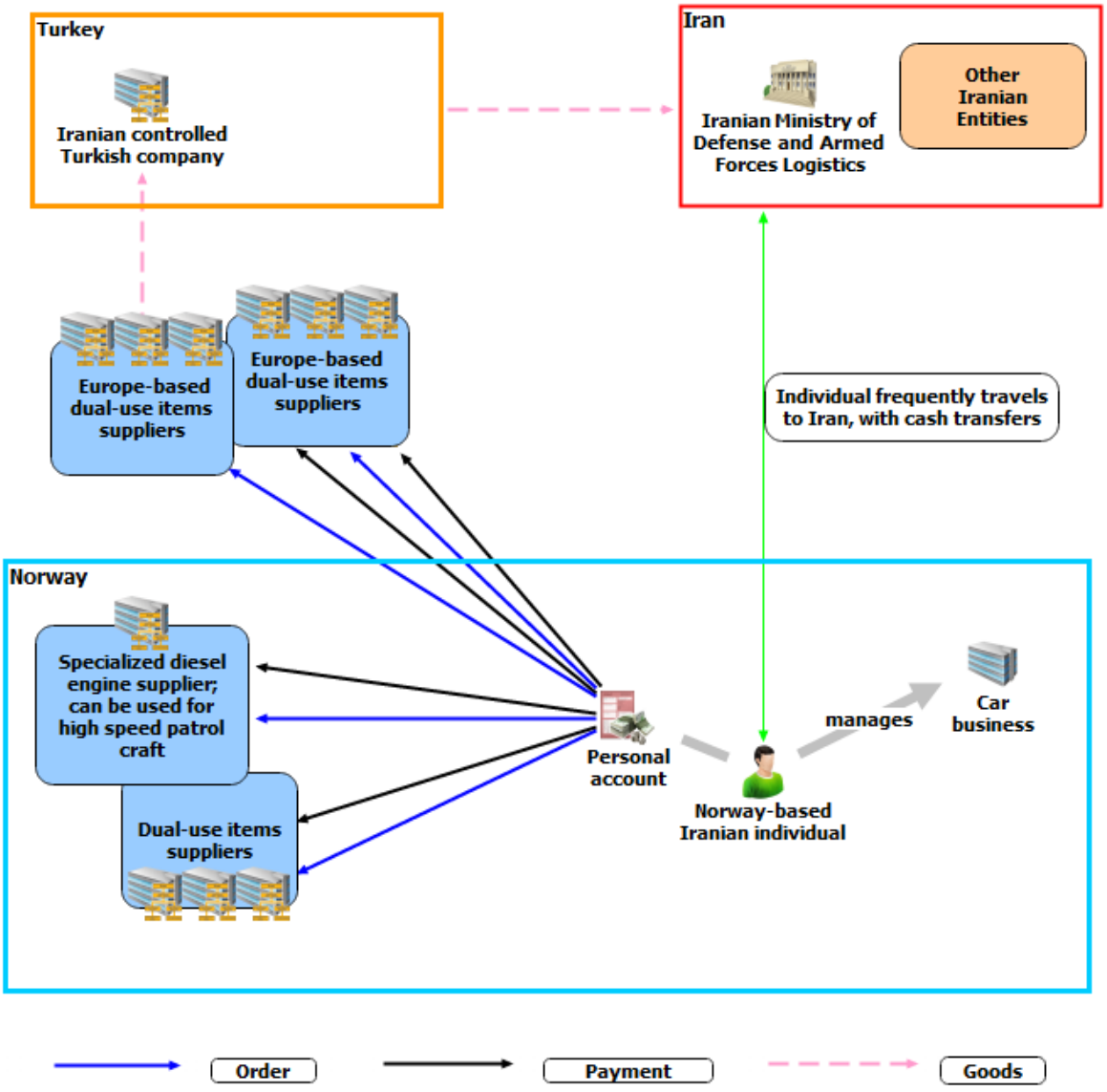


Figure 26. Procurement of dual-use goods and other materials for front companies acting on behalf of Iran

Key Points

- The businessman involved managed a small business and was connected with the country of proliferation concern (Iran);
- His procurement activities were inconsistent with his normal business;
- The businessman transported cash from Iran, and apparently used this for procurement, including of dual-use goods.

Case 26: Multiple banks involved in financing procurement by a small trading company in Europe (2011)

Information supplied by the Customs Administration of the Netherlands

In 2011 a Netherlands company attempted to export a shipment of Viton "O" rings to Iran by courier. The shipment was intercepted by Netherlands Customs. The items required a license for export but no license had been applied for. Investigations by the authorities revealed that the company concerned was a small Dutch trading company that had been set up in 1997 by an Iranian living in Germany, close to the Dutch border. According to Chamber of Commerce databases the company was a wholesaler trading ferrometals. The company accounts were poorly organized. The authorities confiscated the "O" rings and sent a warning letter to the company.

A year later Dutch authorities received an export declaration from the same company for a shipment to a consignee in Tehran, company A, of materials described as "equipment for glass production" (figure 27). The shipment was stopped and found to comprise 22 turbo vacuum molecular pumps manufactured and supplied by a company in another EU State, valued at EUR 232,500.00. These pumps were listed under EU sanctions regulations in force at the time as being of potential use in Iran's nuclear program. The company had made no attempt to obtain an export license, and Dutch authorities carried out further investigations of the company.

These investigations showed that, as the previous year, the trading company's accounts were incomplete. Although on paper it appeared that the company carried out a lot of business, in fact little of this was substantive and the company appeared to have no other business in the Netherlands. The authorities found a number of fake invoices. The authorities also noted that the owner often used a Dutch or German sounding name on emails rather than his real, Iranian name.

The trading company had told the supplier in the other EU State that the vacuum pumps were destined for a new glass company in Turkey, but according to documentation accompanying the shipment the consignee was a company in Tehran, company A. Furthermore, investigations revealed an email from another company in Tehran, company B, asking the trading company to change the name of the consignee from company B to company A. Further investigations showed that company B was a front company for the Iranian nuclear program.

In order to finance the vacuum pump deal, the trading company had received five payments by wire transfer into an account at a local Dutch bank from companies based overseas during a four-month period in 2011. The authorities noted that in addition to the attempted export of these pumps to Iran without a license, the trading company had never applied for a license to receive these payments as required by EU regulations in force at the time.[116]

[116] EU Regulations (961/2010) in force at the time required a license for financial transactions involving

Prior to shipment of the vacuum pumps to Iran in May 2012, the trading company paid the supplier in installments over a five-month period in 2011.

The trading company received and originated payments according to the schedule in Table 4.

Iran larger that EUR 40,000, so the company should have applied for a license for three of the five payments, and notified the authorities of the other two payments.

Table 4: Schedule of payments received and originated by the trading company in connection with shipment of vacuum pumps to Iran.

Date	Payment received by trading company (all different) from:	Amount (€)	Description attached to payment	Action by trading company
March 2011	Turkey	36,185.00	Invoice No…	
March 2011				Payment to supplier
11 April 2011	UAE	44,926.00	Business transaction	
14 April 2011	Turkey	25,000.00		
14 April 2011	Jordan	55,480.00	Purchase	
15 April 2011				Payment to supplier
2 June 2011	Turkey	68,220.00	Based on First Glass	
12 July 2011				Payment to supplier
May 2012				Attempted export of vacuum pumps

Investigations of these five companies showed that they did not all have a website. They were presumably set up specifically to finance this deal (and perhaps other deals elsewhere).

Although the total cost of the vacuum pumps was EUR 232,500, a total of about EUR 239,800 was paid into the trading company's banks account, suggesting that the company made a profit of about EUR 7,300 on the deal.

Following investigations by the authorities, the bank closed the trading company's account. The bank had no records of additional transactions involving the five entities.

The pumps were confiscated and sold into the local market by Netherlands authorities. The proceeds were used to settle a tax bill owed by the company.

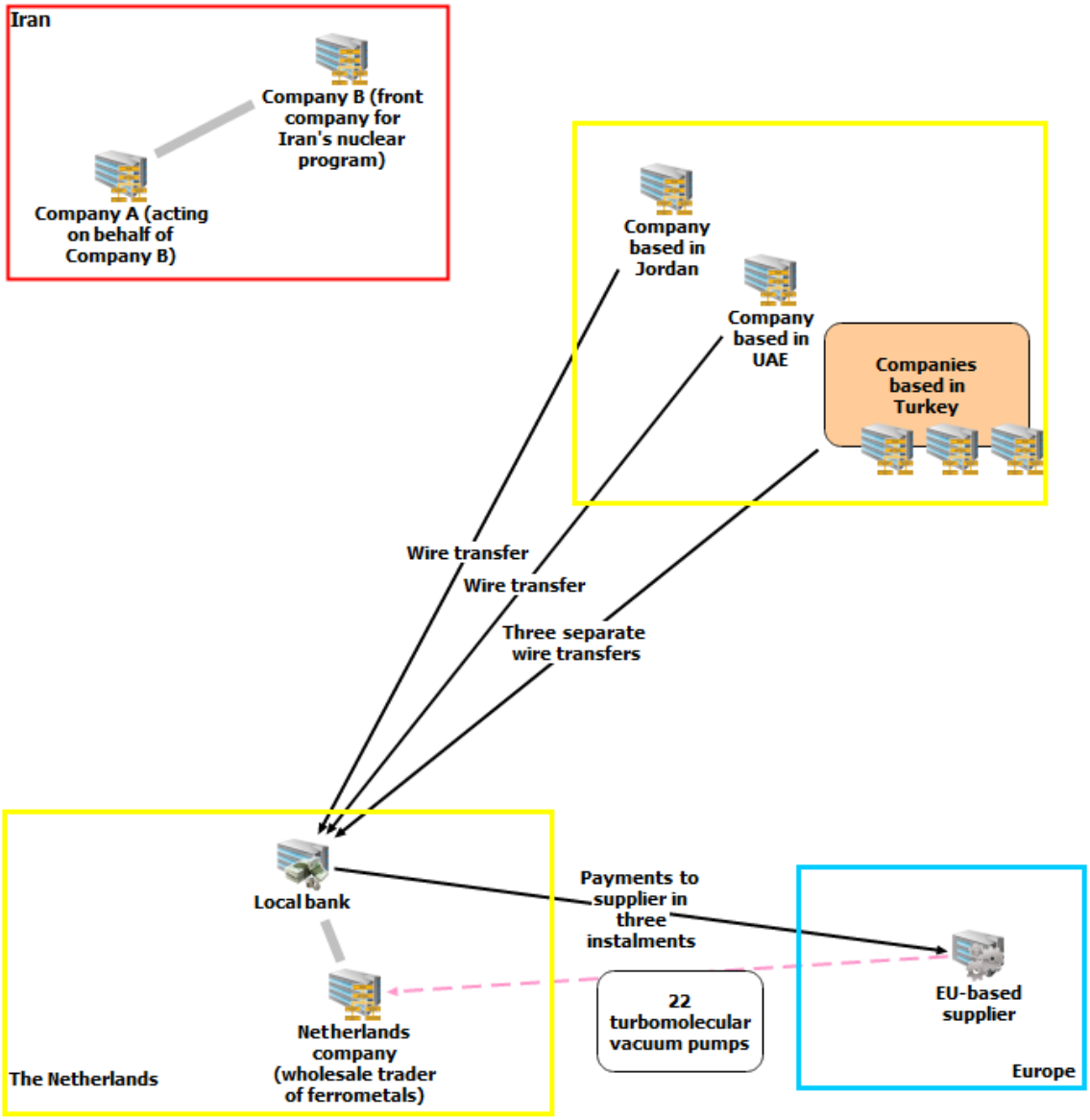


Figure 27. Multiple trading companies overseas used to finance procurement of vacuum pumps

Key Points

- A dual national (EU/Iranian) was involved, running a small trading company ostensibly dealing in ferrometals, but that appeared to do little genuine business;
- Separate payments from the different companies based in different countries may have reflected the preferences of the companies in Tehran; they may also have been intended to divert attention from the large size of the total sums involved;
- At least some of these companies lacked a website, suggesting they were shell companies set up simply to transfer funds;
- Two of the countries in which these companies were based (Turkey, UAE) are well known as countries of diversion concern, or as channels to circumvent sanctions; Jordan perhaps less so;
- The vague and generalized descriptions attached to the payments were probably also intended to avoid them attracting the attention of the recipient Dutch bank;
- The case illustrates that investigations of goods and materials carried out by Customs authorities can throw light on FoP.

Case 27: FoP through banks in South East Asia (2012)

The following is based on information from a governmental source. The source stated that the transaction described below had been implemented at least in part, but it had no confirmation that the transactions had all been completed.

A designated entity in Iran issued a purchase order in 2012 for items required by ballistic missile guidance systems (prohibited by sanctions for procurement by Iran) through a front company set up for the purpose, B (figure 28); the order was processed by an intermediary, a genuine company, C. Company C transferred the purchase order to Individual A, a businessman trusted by officials at the designated entity. He was not designated and therefore able to travel.

Individual A processed the purchase order through Company E, a company that trades in foodstuffs set up by Iran in a state in southeast Asia, State A. Company E transferred the purchase order in turn to F, a shell company set up by Iran in another state in southeast Asia, State B; This shell company transferred the purchase order to a manufacturer in a state in Asia, State C.

The financing network operated through Company D, a genuine Iranian company dealing in foodstuffs, as follows: Company C set up a financial agreement with Company D regarding payment for the items. Individual A, with an account at Bank A, a bank designated under UN sanctions, provided additional financial support in the form of a check guarantee from the Bank.

Company D held a bank account at a second Iranian bank, Bank B, not designated by the United Nations. Company D in turn arranged for a bank guarantee to be issued by Bank B. This bank guarantee was in turn transferred to Bank C in State A, and to Bank D in State B. There, the bank guarantee was made available to the front company F dealing with the manufacturer.

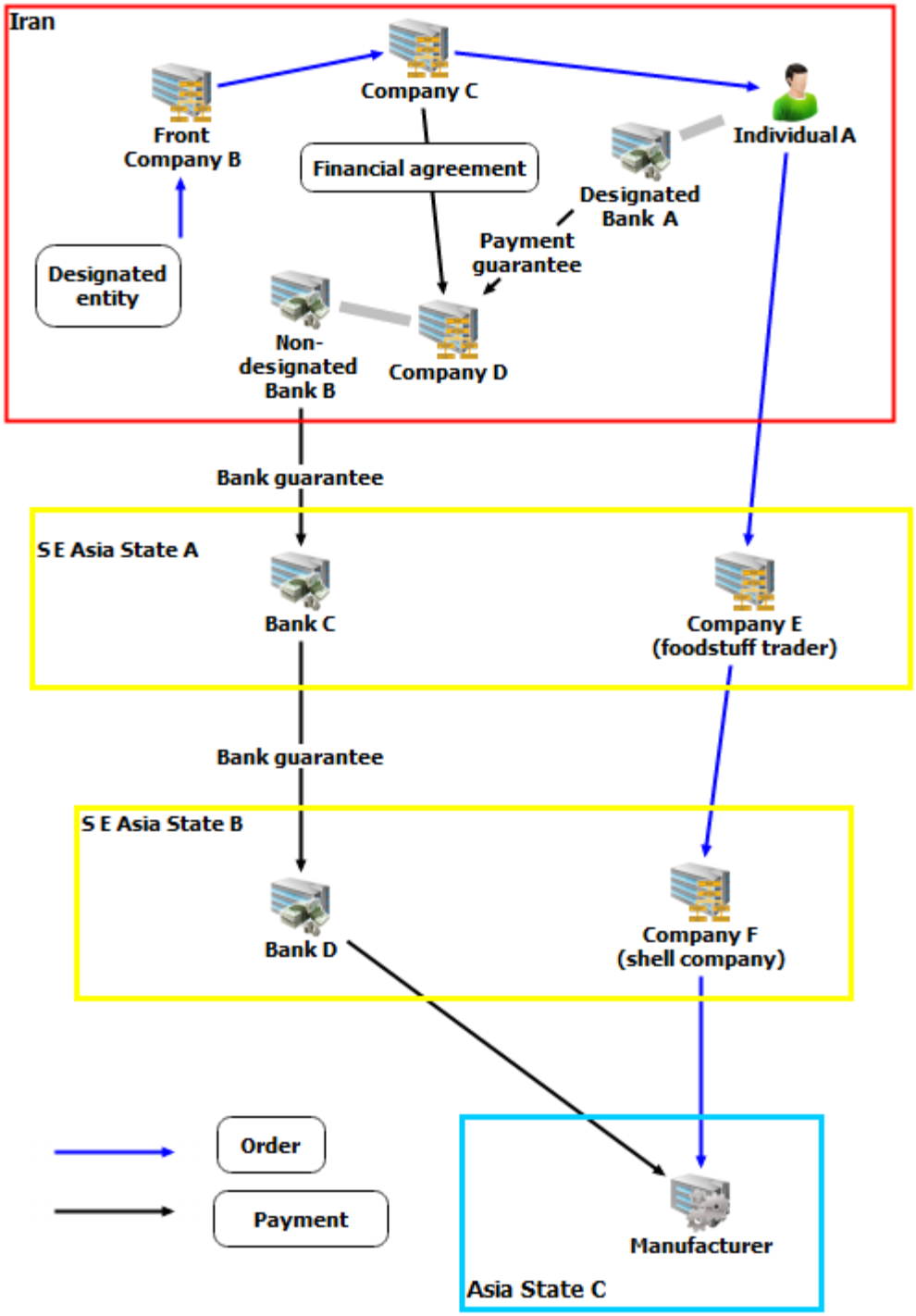


Figure 28. Procurement and financing networks based on states in South East Asia

Key Points

- The network of companies inside Iran was presumably intended to hide the role of designated entities in the ordering and financing of goods and materials. It would have been difficult for a foreign bank to detect the involvement of designated

entities;

- A non-designated individual played a key role in transferring the purchase order and in securing a payment guarantee through a designated bank;
- The network set up outside Iran consisted of existing companies and companies created by Iran for the purpose;
- Two foodstuffs traders were involved, one in the channel used to process the purchase order and the second in the channel used for financing the order;
- Financial channels in South East Asia are used for circumvention of sanctions by both Iran and DPRK.

Case 28: Procurement of materials for a biological laboratory (2012)

The following is based on information provided by Norwegian authorities.

An Iranian businessman living in Norway worked full-time in a travel agency that did some business with Iran. He was also the sole proprietor of a small import and export company that did very little business. The company address was his home address.

In 2012, the businessman contacted several suppliers of laboratory materials in Norway and a few in other European countries (figure 29). He ordered a broad range of products, i.e. a specialized vacuumer, growth media for bacteria, freeze-dried TB strains, biological analytical reference material, products used in molecular microbiology and other related supplies for the handling, analysis and processing of materials in a biological laboratory.

The businessman did not give the suppliers any information on the end use of these products. Some of them were regulated for export to Iran, others were not. Several of the companies alerted the authorities to the activities of the businessman. One of the companies notified the authorities that one of the orders was larger in size than needed by most national laboratories.

The Norwegian authorities established that the sponsor for this procurement was the Pasteur Institute of Iran. The businessman took active steps to hide this fact from the suppliers.[117]

The products the businessman was able to buy were paid from his personal bank account. The total amount needed to pay for the few products he was able to buy was not substantial. However, if the suppliers had sold him all the products he ordered, the sums would have been much larger, exceeding what he would have been able to pay based on his salary and the modest income of his small business. It is not known how those transactions would have been funded.

It could be noted that the Norwegian company reacted to the approach and alerted the relevant authorities in response to outreach previously conducted by the authorities, including The Norwegian Police Security Service (PST), to alert businesses to the risk of proliferation activities.

[117] The Pasteur Institute was listed in the Japanese Government's List of Foreign Users of Concern dated 22 March 2002 (e.g. http://learnexportcompliance.bluekeyblogs.com/2002/03/30/are-you-using-the-japanese-government%E2%80%99s-list-of-foreign-end-users-of-concern/; the UK Government's Iran List of end-users of potential concern of 15 August 2012 (http://webarchive.nationalarchives.gov.uk/20121015160307/http://www.bis.gov.uk/assets/biscore/eco/docs/iran-list.pdf); and included in the Canadian Government's Regulations Amending the Special Economic Measures (Iran) Regulations of 4 February 2016.

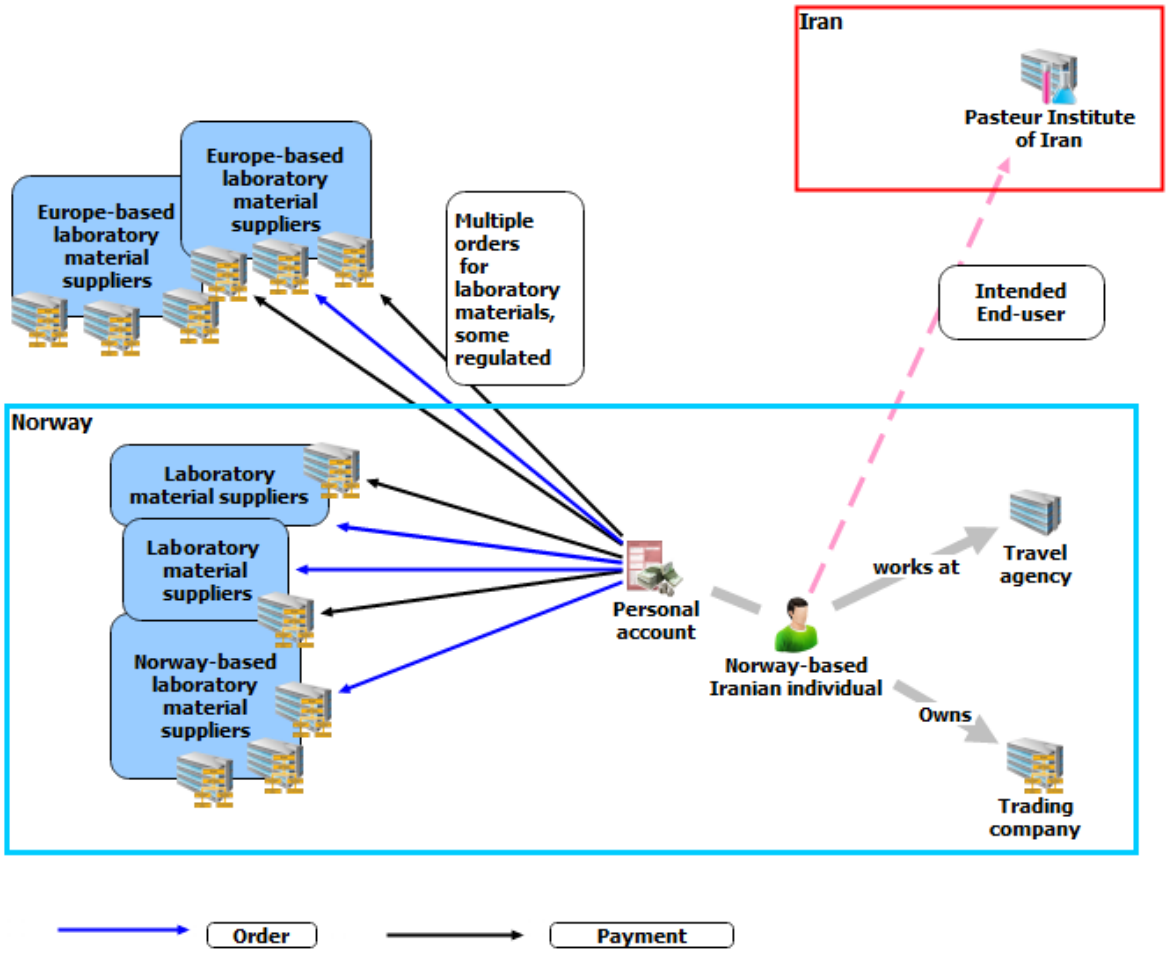


Figure 29. Use of personal banking account to procure materials for a biolab

Key Points

- The businessman was connected with the country under sanctions (Iran) and was conducting procurement activities inconsistent with his normal business;
- He used his personal bank account to conduct trade.

Case 29: A probable sanctions circumvention scheme detected by monitoring for suspicious transactions (1) (probably 2012-2013)[118]

A trading company was set up by a foreign national in a country in the Middle East.[119] A series of accounts on behalf of the company were opened at a branch of an international bank in the State concerned. These accounts were denominated in local currency, euros, US dollars, and other foreign currencies.

The international bank monitored transactions through the trading company's account in accordance with its standard practices. This monitoring revealed that the trading company received funds into its local currency account from only one source. This source was a second company, set up by another foreign national. These local currency funds were then quickly switched into foreign currencies and transferred overseas from the company's foreign currency accounts (figure 30).

This activity did not appear consistent with a trading company's normal pattern of financial transactions. The bank investigated, and discovered that the owners of both companies had links to Iran. The bank suspected the funds originated in Iran and that the trading company's bank accounts were being used to transfer the funds into the global financial system.

[118] This case was Case No 8 in the Interim Report published 5 February 2017.
[119] Annex V of UN Panel on Iran Final Report 2014 (S/2014/394).

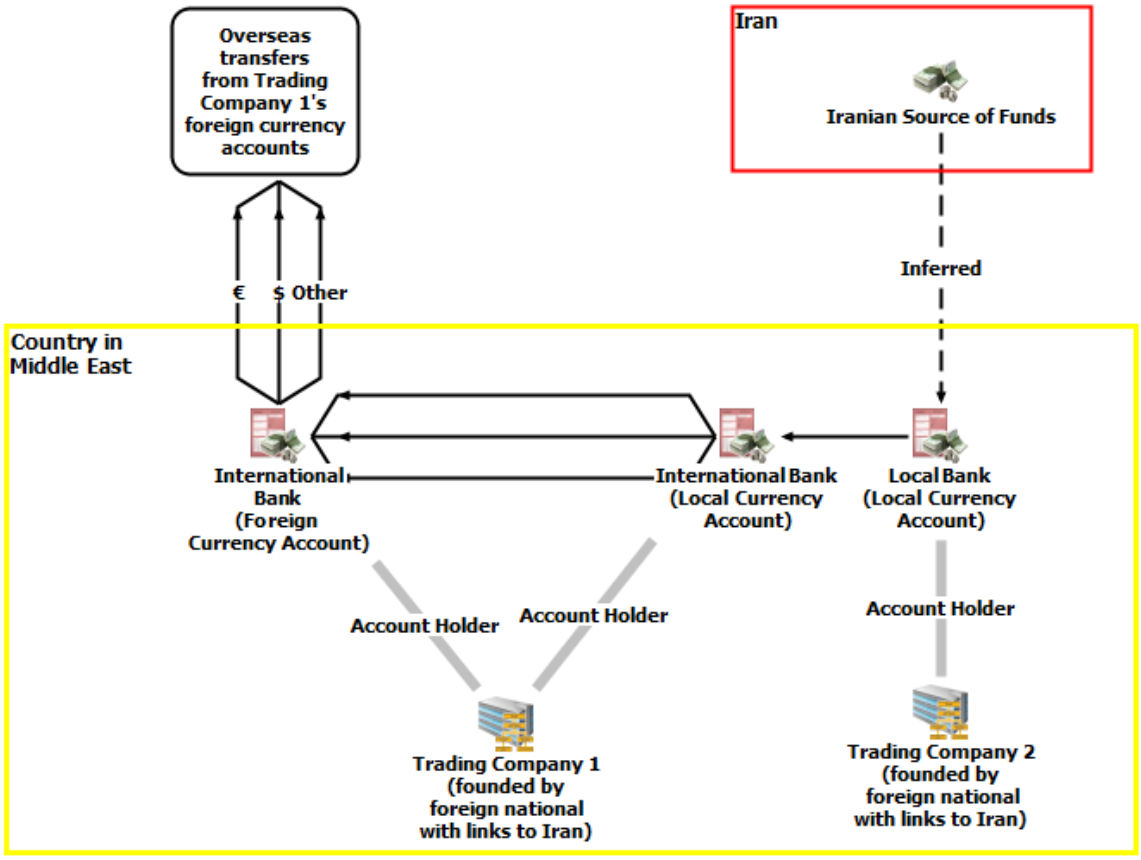


Figure 30. Mechanism for transferring Iranian funds into the international financial system

Key Points

- This apparent attempt to circumvent financial sanctions was detected by the bank's monitoring of suspicious indicators related to money laundering;
- The companies involved were linked to the sanctioned country;
- The policy of the bank was to withdraw from business connected to Iran. Thus no further data are available to determine whether the scheme involved FoP.

Case 30: A probable sanctions circumvention scheme detected by monitoring for suspicious transactions (2) (probably 2012-2013)[120]

A trading company was set up by a foreign national in the Middle East and a company account opened at an international bank in the state concerned.[121] The international bank monitored transactions through the trading company's account in accordance with its standard practices. This monitoring revealed a high turnover of funds, and the bank suspected money laundering was taking place.

Investigations by the bank showed that the foreign national's stated employment was as a member of staff in a second company. This second company had the same telephone number as the trading company.

Further investigation revealed that this telephone number was the same as that belonging to two further companies previously identified by the bank as having Iranian shareholders and being involved in Iranian business (see figure 31). The bank therefore suspected the trading company was being used as a front for Iranian business.

[120] This case was Case No 9 in the Interim Report published 5 February 2017.
[121] Annex V of UN Panel on Iran Final Report 2014 (S/2014/394).

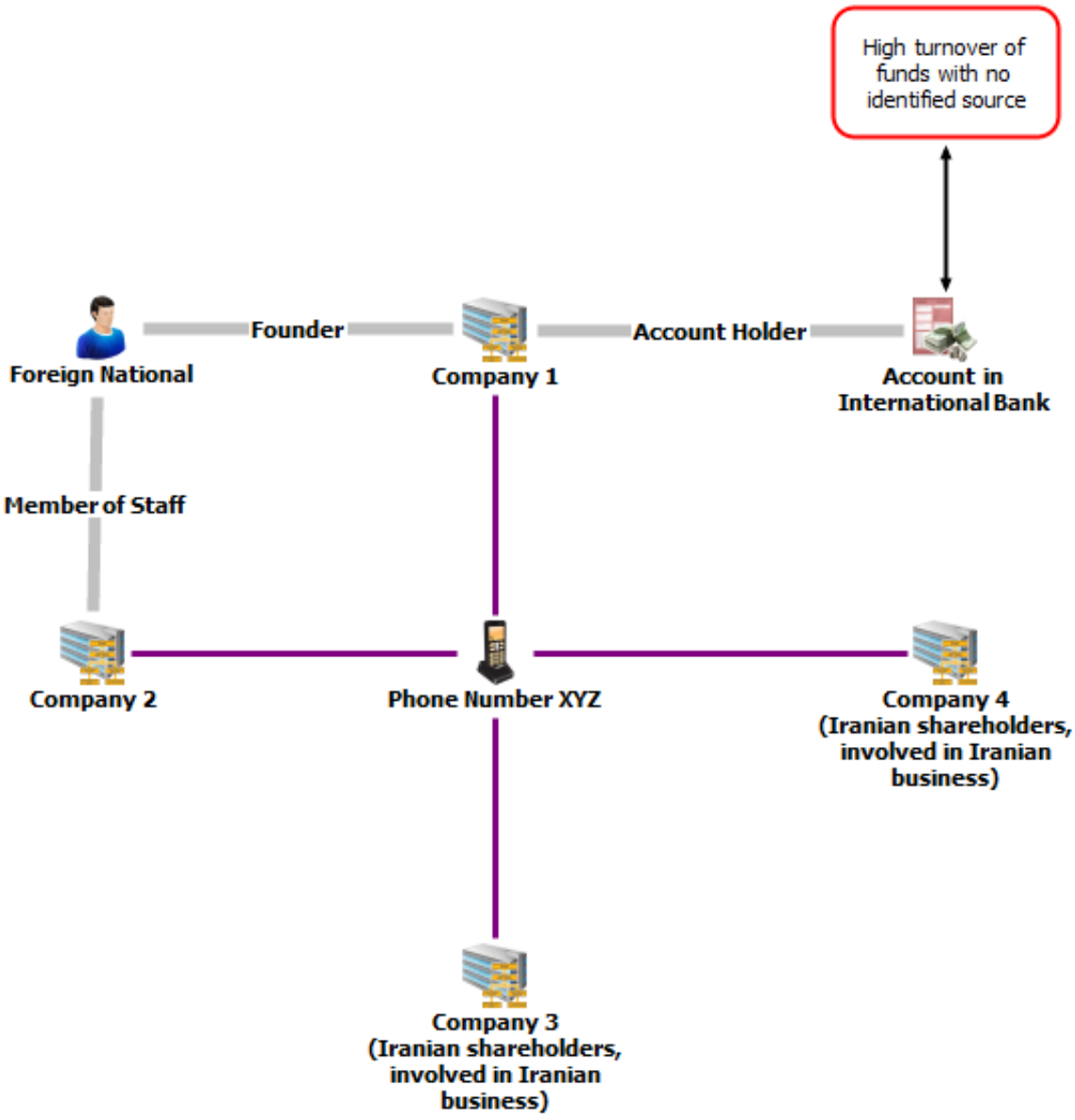


Figure 31. Common telephone numbers link companies in a suspected sanctions circumvention scheme

Key Points

- This apparent attempt to circumvent financial sanctions was detected by monitoring suspicious indicators related to ML;
- The companies involved were linked to the country under sanctions;
- The policy of the bank was to withdraw from business connected to Iran. Thus no further data are available to determine whether the scheme involved FoP.

Case 31: A probable sanctions circumvention scheme detected by monitoring for suspicious transactions (3) (probably 2012-2103)[122]

A company was set up in a Middle Eastern state by a national of the state concerned, in partnership with a foreign national as a minority shareholder.[123]

An account was opened on behalf of the company at an international bank in the state concerned.

Monitoring by the international bank of transactions through the trading company's account revealed that multiple large payments were being made from this account to several companies at the same address in a European state. Multiple large payments were also being made to a second set of companies sharing the same address in a second state in Europe (see figure 32).

The bank identified this pattern of transactions as possible ML. It carried out further investigation that revealed that the national of the state in the Middle East also managed another company that did business with Iran.

[122] This case was Case No 10 in the Interim Report published 5 February 2017.
[123] Annex V of UN Panel on Iran Final Report 2014 (S/2014/394).

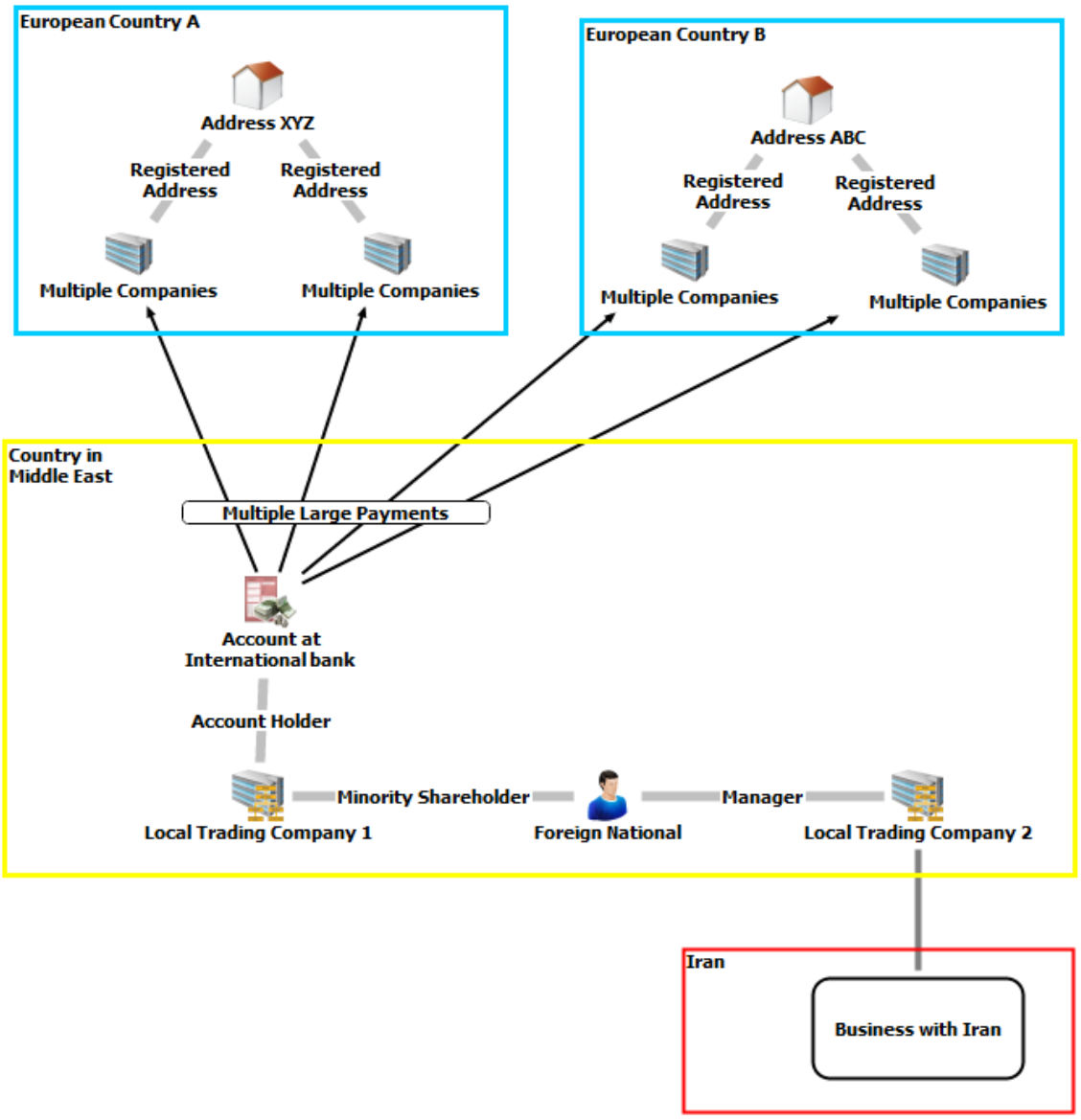


Figure 32. Suspected scheme to transfer funds from Iran to companies in Europe

Key Points

- This apparent attempt to circumvent financial sanctions was detected by monitoring suspicious indicators related to ML;
- The companies involved were linked to the sanctioned country;
- The policy of the bank was to withdraw from business connected to Iran. Thus no further data are available to determine whether the scheme involved FoP.

Case 32: Attempt to circumvent sanctions by use of a fake address (probably 2012-2013)[124]

A financial institution was asked to process a payment to a company in a state neighboring Iran.[125] The policy of the financial institution was to conduct enhanced due diligence where companies in this particular state were concerned. As a result this company (the beneficiary of the payment) was found to be located in Iran. The address in the neighboring state was fake (see figure 33).

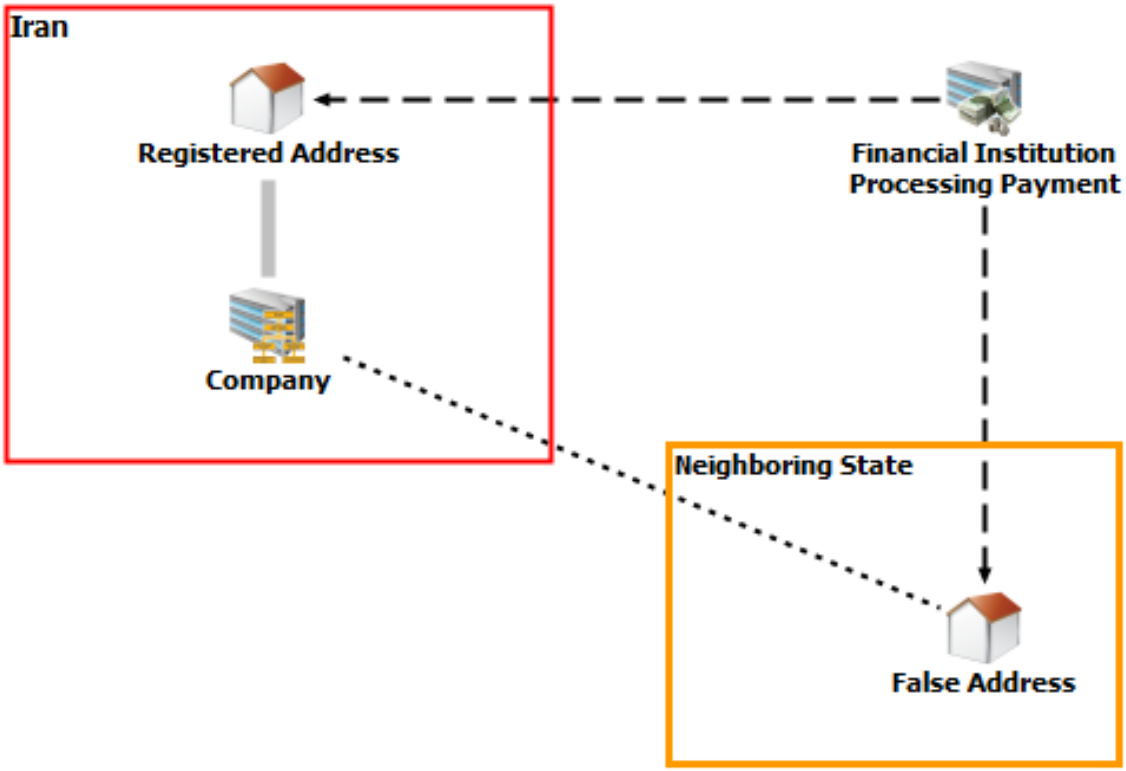


Figure 33. Sanctions circumvention using a fake address

Key Points

- The financial institution's due diligence procedures detected this apparent attempt to circumvent financial sanctions;
- The fake company address was located in a country neighboring Iran.

[124] This case was Case No 11 in the Interim Report published 5 February 2017.
[125] Annex V of UN Panel on Iran Final Report 2014 (S/2014/394).

Case 33: Beneficiary of a letter of credit acts as a front company to circumvent sanctions (probably 2012-2013)[126]

A financial institution was asked to process an import letter of credit covering a shipment of goods.[127] The goods originated in State A, in South Asia, and were ostensibly to be shipped from State B, neighboring Iran, to State C in North Africa.

The financial institution investigated the letter of credit, and discovered that the shipment was conducted by a third company, which was Iranian. The beneficiary of the credit letter in State B neighboring Iran was acting as front company to the Iranian company, the actual beneficial owner, based on information in the letter of credit (see Figure 34).

[126] This case was Case No 12 in the Interim Report published 5 February 2017.
[127] Annex V of UN Panel on Iran Final Report 2014 (S/2014/394).

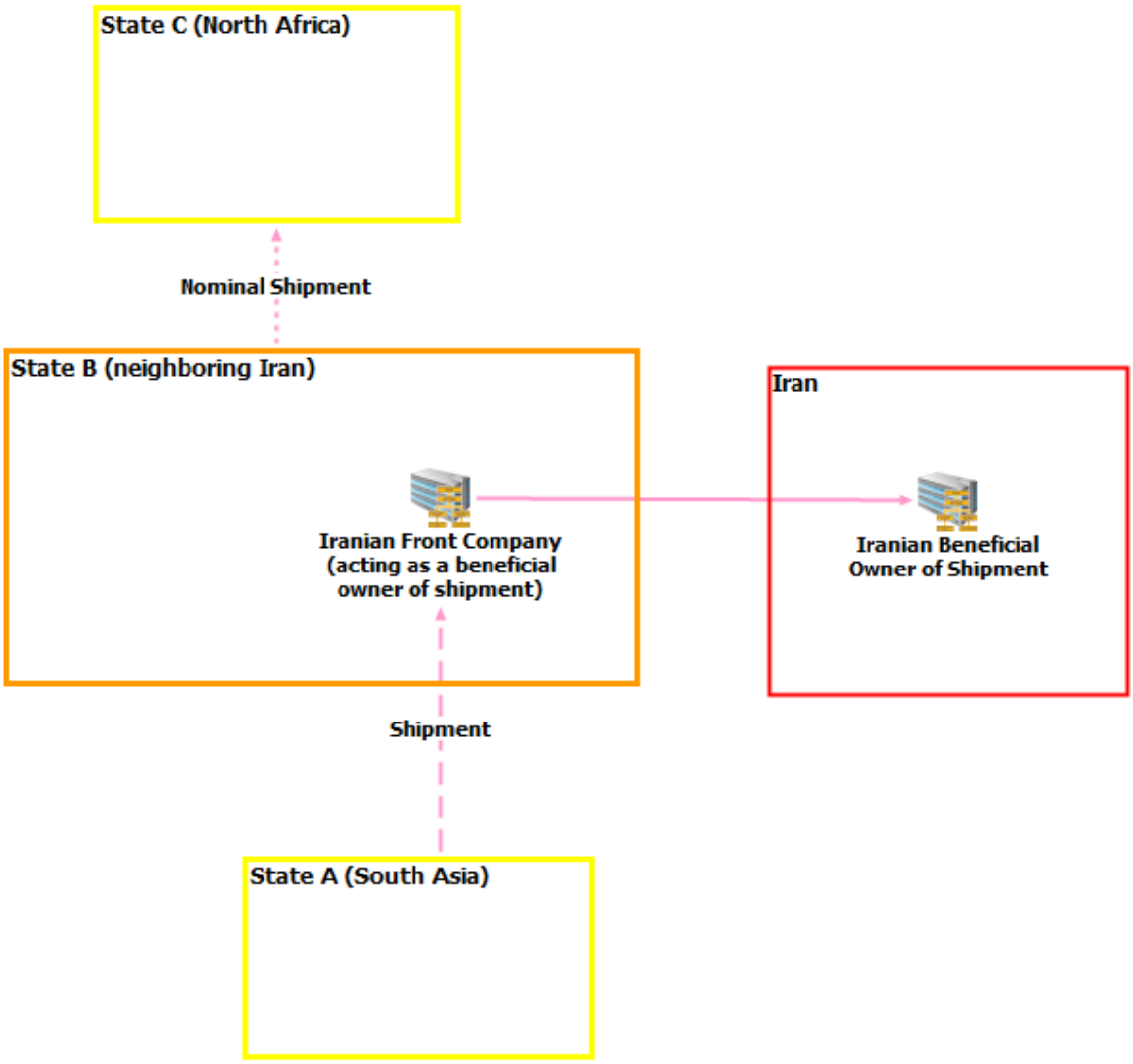


Figure 34. Sanctions circumvention by a front company based in a State neighboring Iran

Key Points

- This apparent scheme to circumvent financial sanctions was detected by application of due diligence procedures to trade financing schemes involving states which neighbor Iran;
- Checks on the letter of credit documentation extended to sanctions risk, as well as credit risk.

Case 34: Sanctions circumvention involving a shipment to a State neighboring Iran (probably 2012-2013)[128]

An international financial institution was asked to process transactions covering goods shipped from a State A in North Africa to a State B neighboring Iran.[129] A review of related shipping documents by the financial institution in accordance with its policies revealed that the goods were in fact in transit to Iran (see figure 35).

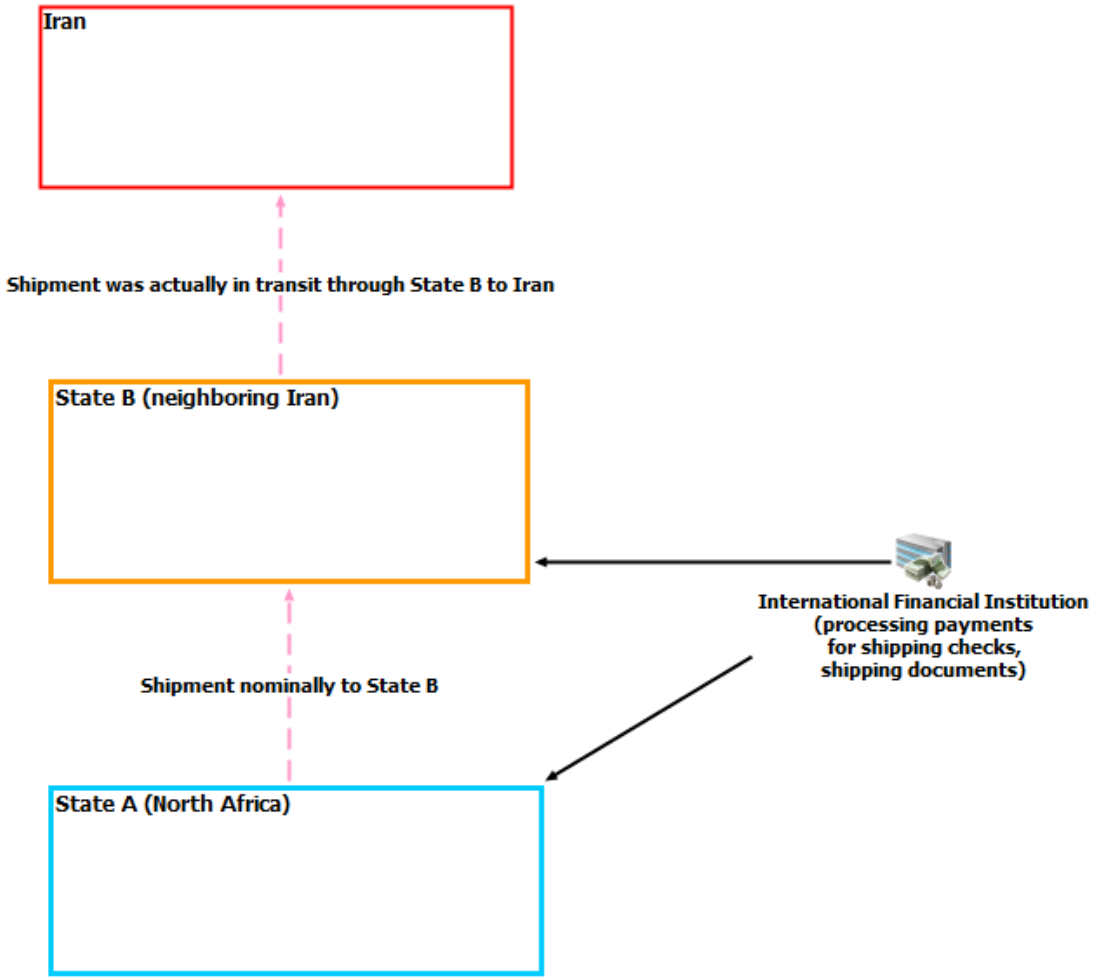


Figure 35. Sanctions circumvention through a State neighboring Iran

Key Points

- This apparent scheme to circumvent financial sanctions was detected by application of the bank's due diligence procedures to trade financing schemes involving States neighboring Iran.

[128] This case was Case No 13 in the Interim Report published 5 February 2017.
[129] Annex V of UN Panel on Iran Final Report 2014 (S/2014/394).

Case 35: Sanctions circumvention by a company acting as remittance agent (probably 2012-2013)[130]

A company in Iran, Company A, entered into an agreement with a company in a State in the Middle East, Company B, under which Company B agreed to accept or process payments on behalf of company A.[131] Company B had a bank account at a non-Iranian financial institution.

Company A informed its customers to direct their payments to Company B and informed beneficiaries to expect payments from Company B's bank (see figure 36).

It is not known how Company B and Company A in Iran settled their financial liabilities.

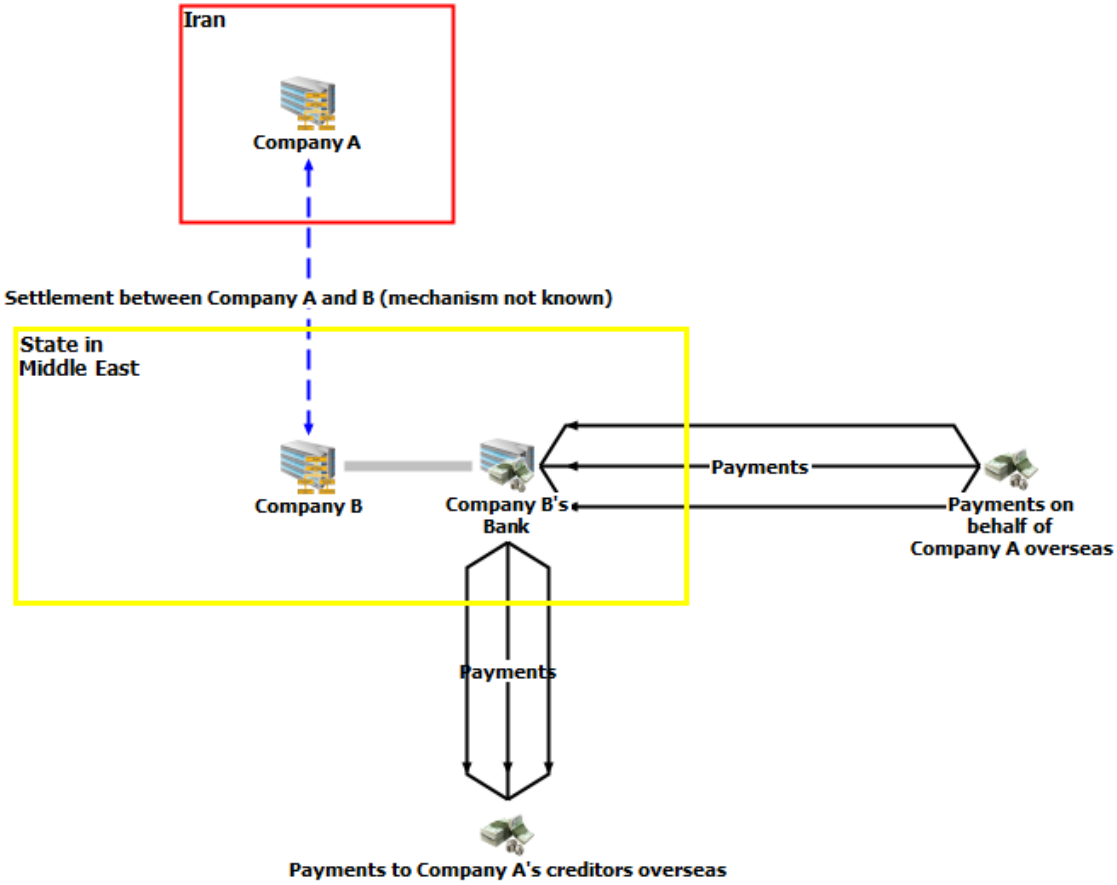


Figure 36. Sanctions circumvention by company acting as remittance agent

Key Points

- Monitoring by the bank presumably revealed that Company B's financial transactions were inconsistent with its expected financial profile.

[130] This case was Case No 14 in the Interim Report published 5 February 2017.
[131] Annex V of UN Panel on Iran Final Report 2014 (S/2014/394).

Case 36: Payment to company inside Iran is rejected and re-presented through a third company (probably 2012-2013)[132]

A non-Iranian company located outside Iran, Company A, tried to send a payment to a company inside Iran, Company B. The payment was sent to a specific account purportedly belonging to company B at a bank inside Iran. The payment was rejected by an international financial institution in the payment chain and a report filed with the authorities.

Company A then arranged a payment for a similar amount to a third company as beneficiary, Company C, located outside Iran. The number given for the beneficiary account number was the same account number as Company B (figure 37).

It is not known if or how this second attempted payment reached company B. Open source searches failed to reveal a connection between the Iranian Company B and Company C outside Iran.

[132] This case was Case No 16 in the Interim Report published 5 February 2017.

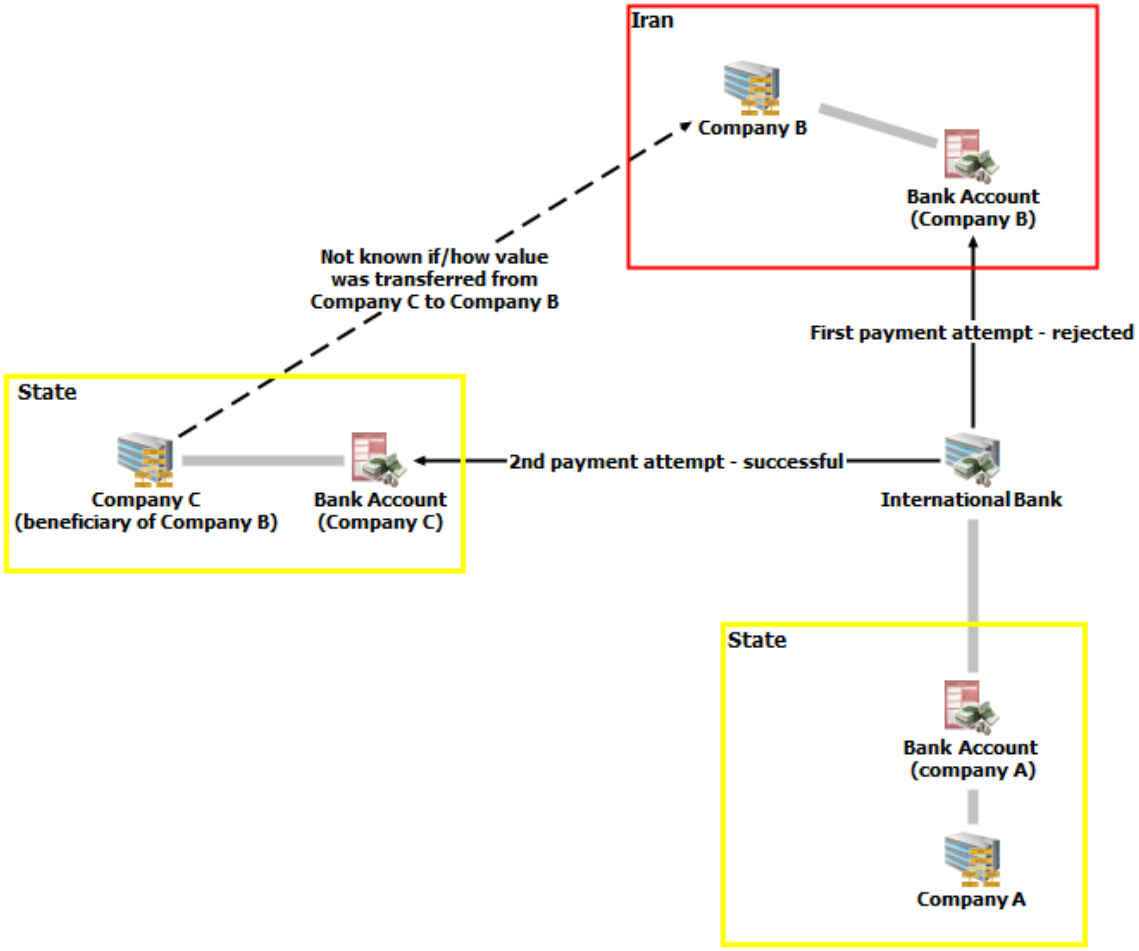


Figure 37. Repeated attempt to pay a company in Iran

Key Points

- A payment to a company inside Iran, initially rejected by an international bank, was represented to the bank, for a different payee outside Iran;
- The repeat transaction was identified because it contained a reference to an account number associated with the blocked transaction.

Case 37: Procurement of materials associated with extraction of uranium (2012-2014)

The following is based on information provided by the Belgian Financial Intelligence Processing Unit (CTIF-CFI).[133]

In the early 1980s, individual A, a Belgian/Iranian dual national, founded two Belgian companies, Company A and Company B. Individual A owned and managed Company A through Company B. These two companies imported and exported products, parts of machines and industrial equipment for the chemical and mining industry. Company A was known to have always traded with Iran, including with an entity designated under sanctions regimes for proliferation due to its activities linked to uranium mining (figure 38).

Company C, based in North Africa, was part of a local public company involved in mining phosphates, with Iran as one of its main customers. It traded regularly with Iran.

Company A received from 2012 to 2014 significant funds (via bills of exchange) for a total amount of approximately USD 1.5 million from Company C in North Africa. Company A performed large transfers to various companies in Asia justified by the payment of invoices, probably for the purchase of products (no further information available).

Iran was known to be interested in ways to extract concentrated uranium from phosphates in the context of its continuous search for uranium.

Shares of company B (the manager of company A) are and were held by an Iranian industrial company, part of an influential Iranian foundation (*Bonyad*). Commercial companies were commonly used as a cover by this foundation, and it was possible that that the transactions carried out by Company A could have been conducted on behalf of the foundation.

Based on these several elements, it appeared that Iran could be the final consignee of the products purchased by Company A from companies in Asia and sold to Company C and that these products could subsequently be used for the extraction of concentrated uranium.

Belgian authorities concluded that the transactions performed by Company A could potentially be linked to financing of proliferation-sensitive nuclear activities or the development of nuclear weapon delivery systems.

[133] See footnote 97.

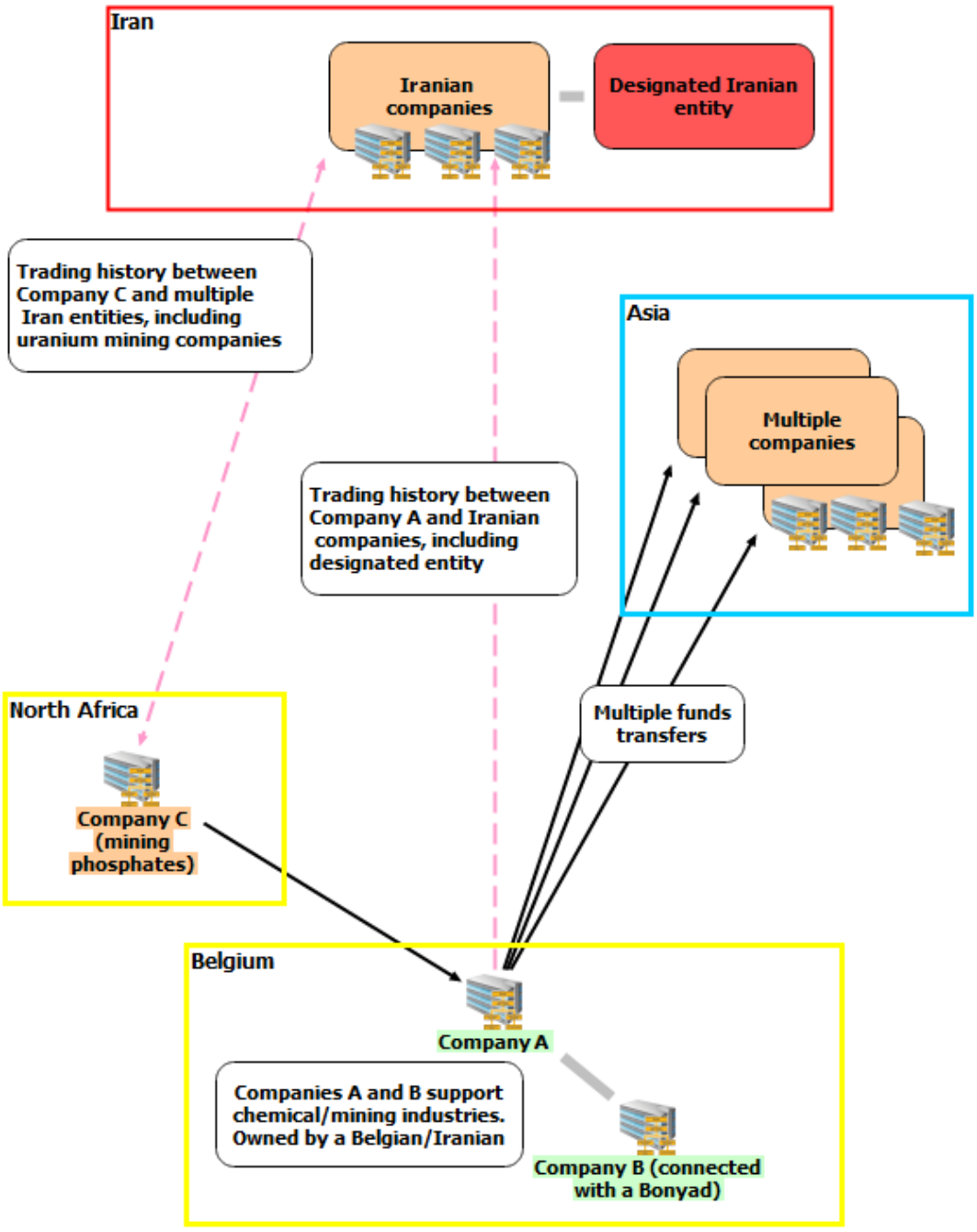


Figure 38. Network potentially to fund purchase of equipment from companies in Asia for transfer to Iran via North Africa

Key Points

- The Belgian trading company, well-established, was owned by a Belgian/Iranian dual national;
- The company appeared to be acting as a broker on behalf of Iranian entities; the suspected proliferation-sensitive activities were consistent with business.

Case 38: Procurement through an oil and gas network in the Middle East (2013)

The following is based on information provided by Spanish authorities.

In January 2013, Spanish authorities intercepted a shipment of valves that was being exported by a Spanish supplier to an oil field services company, Company A, in the UAE. They were intended to be transferred from there onto Iran. The valves were made of a corrosion resistant alloy and although export-related documentation suggested they were intended for the gas sector, the authorities judged they were also suitable for use in Iran's nuclear program. They were subject to export license under EU regulations in force at the time as dual-use goods. The total value of the valves involved was estimated at more than EUR 6 million.

Investigations by the authorities established that a network of companies had been set up to manage the operation (figure 39). Two Iranian nationals in the UAE, based in Company B, were in charge of the commercial transactions. They had links to the Iranian government. The destination of the valves in Iran was an oil and gas company, Company C.

The sales were invoiced to an energy company in the UAE, Company D. Funds for payment for the valves originated in the Oil Ministry of Iran and were channeled to Company D through two Iranian companies, Company E and Company F, linked to the two Iranian intermediaries in the UAE. The payment was initially channeled from Company D to the Spanish supplier through a Company G in Malaysia, but this did not work. The payment in the end was made through a company in Turkey, Company H, and a Turkish bank, Bank A.

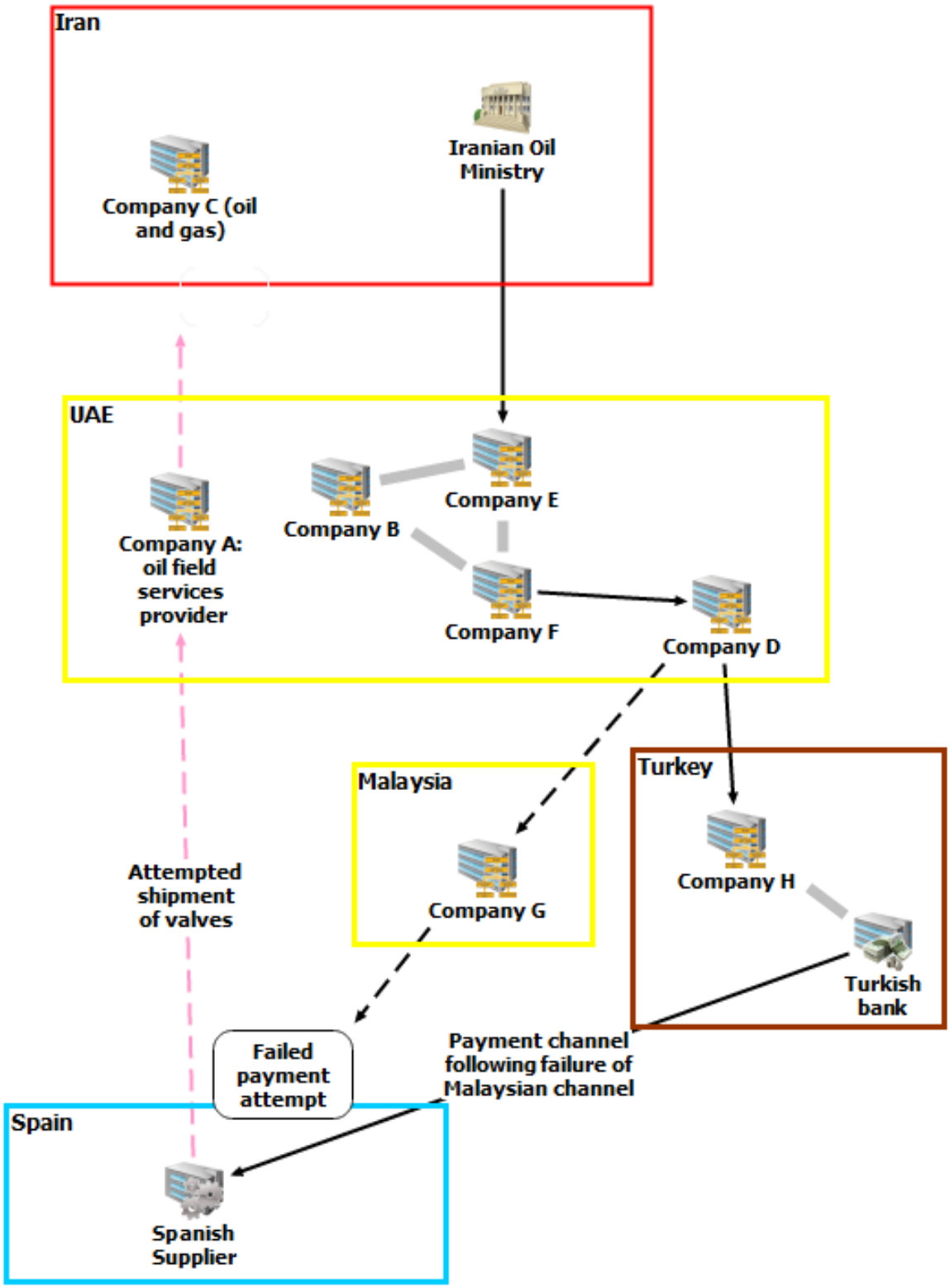


Figure 39. UAE-based network fails to finance procurement through Malaysia and does so through Turkey

Key Points

- The oil and gas sector was used as cover to procure equipment (corrosion-resistant valves) potentially of use in Iran's nuclear program;
- Complex networks of UAE-based companies, funded by the Iranian Oil Ministry, were set up to manage procurement;
- Different channels were used for supplies and payments;
- The network demonstrated resilience; following failure to transfer payment through a company in Malaysia, payment was made through a company in Turkey.

Case 39: Attempted procurement of gas turbines (2013)

The following is based on information provided by a governmental source

In February 2013, a front company for Iran's Defense Industries Organisation,[134] Company D, signed an agreement with three foreign intermediary companies for the purchase and shipment to Iran of four gas turbines. The three intermediaries were a company in a Middle Eastern hub, Company C, a company in a European country, Company F, and a company in a south Asia country, Company F (figure 40). The turbines were to be sourced from the European country. The order was worth about USD 43 million.

A pro-forma invoice for two of the turbines was subsequently transferred by Company F to a second company in the Middle Eastern hub, Company G. In August 2013, Company G transferred the invoice to Individual A, an Iranian national and director of Company C. Individual A was also a director of a company in the Caucasus, Company A, and he forwarded the invoice for payment to his co-director of Company A, Individual B, also an Iranian national.

In March 2014, Company G, on behalf of Company D in Iran, transferred the equivalent of about USD 540,000 from an account at an international bank in the European country to the account of Company E.

Later, Company B assigned two cheques in favor of Company E, drawn on the same international bank in the European country. The cheques were for the equivalent of USD 14,420,000 and USD 2,950,000. They were funded by wire transfers from Company A.

These payments to Company E totaled the equivalent of about USD 18 million.

At least one gas turbine was shipped from the European country to the Middle Eastern hub, and an attempt was made in April 2014 to ship this onward to Iran. Individual A made out a false customs declaration that the machinery was destined for a company in South East Asia. In fact Individual A intended to use another of his companies in the Middle Eastern hub to ship the machinery to front Company D. Authorities in the Middle Eastern hub detained the machinery and arrested Individual A. He was sentenced to 10 years imprisonment in April 2017.

Subsequent investigations revealed further details of the Iranian connections to this procurement network. The director of Company D was a former General in the Islamic Republic Guards Corps (IRGC), and one of the managers of Company F worked for the security office of the Iranian Ministry of Oil.

[134] Designated under then UN, EU and US sanctions on Iran.

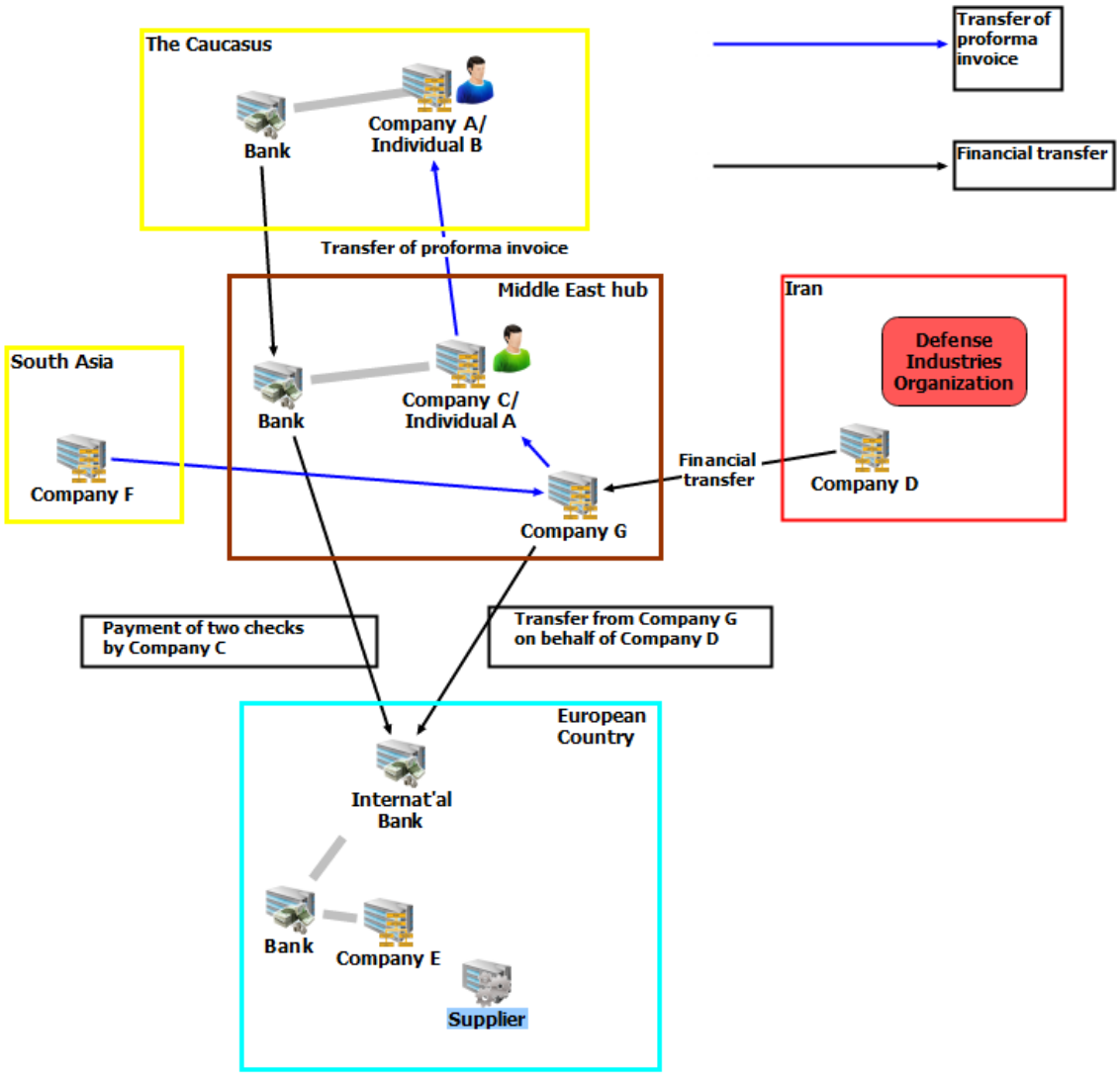


Figure 40. Financing of procurement of turbines from a European supplier

Key Points

- The procurement network extended to South Asia, Europe, the Caucasus and the Middle East;
- Procurement appears to have been financed partly by a network involving a bank in the Caucasus (see Case 22);
- Procurement also appears to have been partly financed by a transfer from a company in the Middle Eastern hub acting on behalf of a company in Iran (the transaction might have been similar to that described in other case studies, for example Case 31).

Case 40: A broker/intermediary plays a key role in a procurement network (2) (2013)[135]

According to documents[136] filed in connection with his arrest and conviction, in March and July 2013 Individual 1, CEO of a US-based company dealing in "special metal products,"[137] arranged two shipments of a metallic powder to a company in Turkey. These were then onward shipped to a company in Iran. The powder (a mix of cobalt and nickel), designed to protect surfaces against corrosion at high temperatures, could be used in aerospace, missile production and nuclear applications and required an OFAC license for export.

The first shipment was paid for by means of a wire transfer initiated by the Turkish company through a New York-based financial institution to a US-based account maintained by Individual 1. Individual 1 then paid the US-based supplier of the metallic powder by check (figure 41).

In July 2013, Individual 1 arranged a second shipment of powder to the Turkish company. On this occasion he paid the US supplier by means of a wire transfer through a New York-based financial institution. He subsequently invoiced the Turkish company for the sum plus a commission (about 9%).

According to court documents, on both occasions the Turkish company was described on export documentation as the end-user of the powder. In response to subsequent enquiries by US authorities, the Turkish company represented itself as an import business, including importing items used by medical industry customers to manufacture implants. The company claimed that the metallic powder was used for this purpose.

[135] This case was Case No 7 in the Interim Report published 5 February 2017.
[136] US District Court Eastern District of New York, Case 16M134, 18 Feb 2016.
[137] A naturalized US Citizen of Turkish descent and CEO of Global Metallurgy LLC, a small company based in, New York.

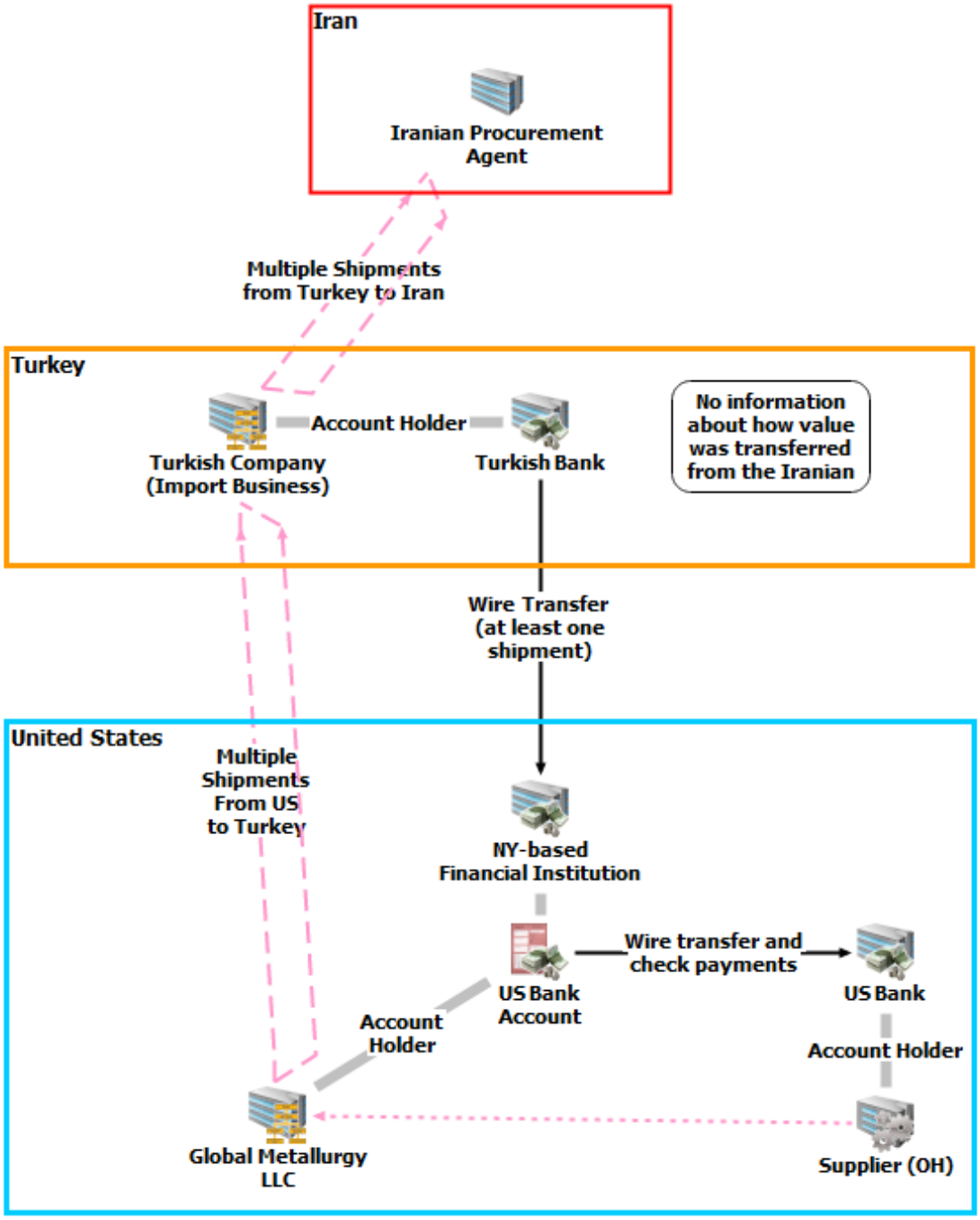


Figure 41. Procurement paid for by a transfer from a bank in Turkey

Key Points

- A small broker/intermediary company was involved; shipments concerned appear to have been consistent with the company's business profile;
- The owner of the company was connected with the state through which goods

were being diverted;

- Payments were made by wire transfers and by cheque;
- The metallic powder required a US export license but did not appear on lists maintained by the Nuclear Suppliers Group or other multilateral export control organizations.

Case 41: Cash used for procurement by small trading company in a rural area

The following is based on information provided by UK authorities.

A small company located in the UK carried out business by trading standard industrial metallurgical products. The company received requests from overseas customers, placed orders with domestic manufacturers and arranged export of the items concerned. Set up in the 1990s, the company was located in a rural area removed from major financial or industrial centers. The directors were nationals of the country in which the company was located. The company did not have any Iranian business.

Front companies in Turkey, UAE, Malaysia and China started to place orders for metallurgical goods, including dual-use goods. The company placed orders with manufacturers and arranged exports. Exported goods were sent to the UAE or other third countries from where it was believed the goods were transferred to Iran. Shipping documentation accompanying the goods typically recorded the names of Iranian banks as consignees.

When doing business with Iranian front companies, the company would sometimes require payment in cash in advance. These cash payments were generally each of the order of a few thousand pounds. It was not known how this cash was used to pay the manufacturers of metallurgical goods.

At one point it appeared that the company's Iranian customers were trying to influence how the company was run.

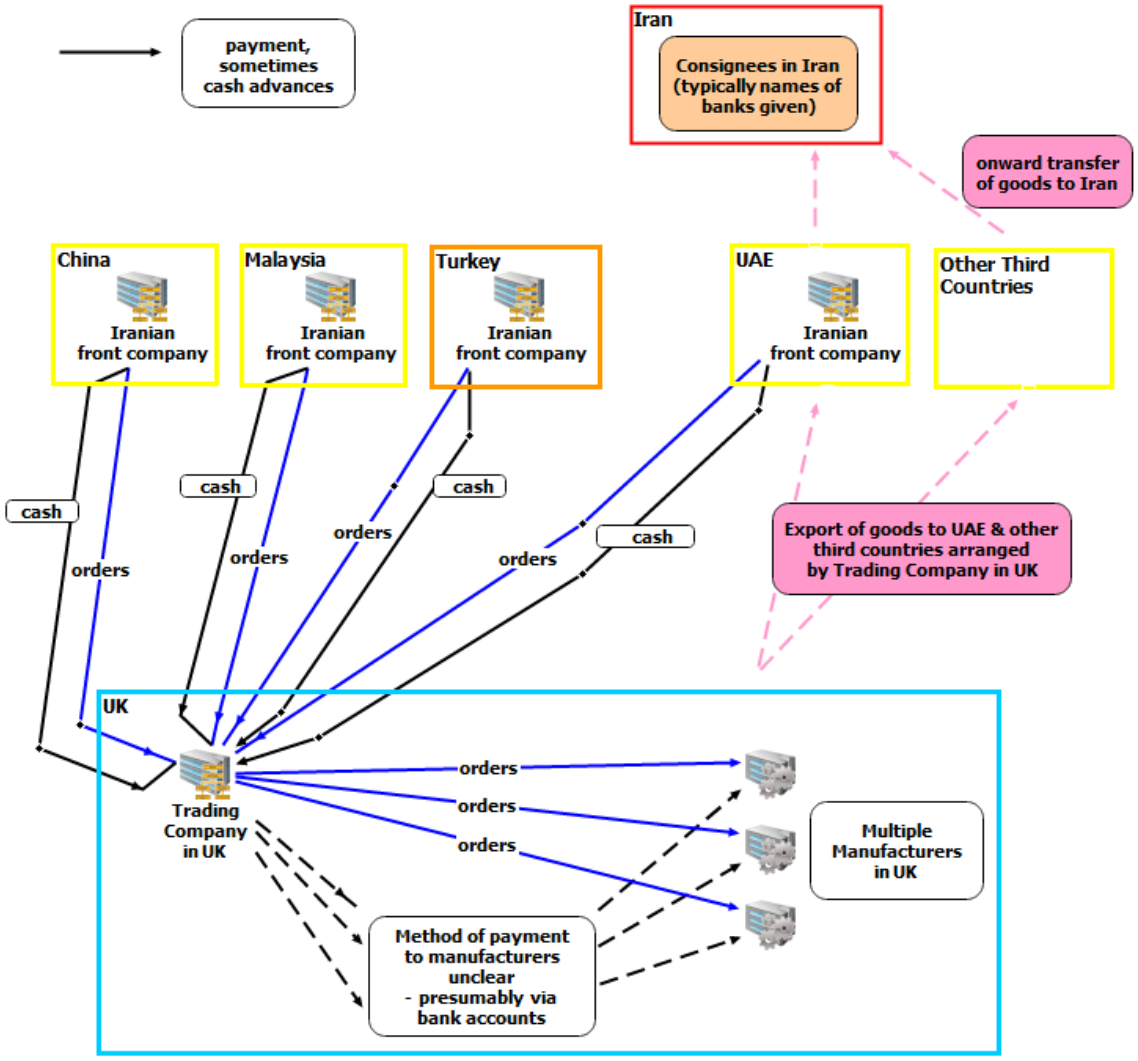


Figure 42. Trading company requires cash payments from Iranian front companies

Key Points

- The company on occasions required cash in advance; it is not clear how the cash was transferred to the UK; presumably the cash was credited to bank accounts and transferred to manufacturers;
- The company was located in a rural area, far from financial or industrial centers.

Case 42: Procurement financed through cash transfers in UAE (2015)

The following is based on information provided by the Belgian Financial Intelligence Processing Unit (CTIF-CFI).[138]

A Belgian individual X managed a telecommunications company, Company A based in Belgium. Company A was providing telecommunications services.

In 2015, Individual X wanted to deposit a total amount of EUR 32,000 (4 x EUR 8,000) in cash to company A's account at a Belgian bank in Belgium. It appeared that this account had already received two cash deposits for a total amount of EUR 18,000 some days before (Figure 43).

Individual X said that he had received the cash in the UAE from a business partner, a company based in Tehran, for the delivery by Company A of telecommunication material 'fiber to home' in order to set up network in seven large cities in Iran. Individual X submitted proof to the bank of payment from the Iranian company to Company A.

The bank refused to carry out the last transactions totaling EUR 32,000.

The Iranian business partner was part of an Iranian group, several subsidiaries of which were linked to Iranian nuclear and ballistic programs.

Belgian authorities were satisfied that the cash transactions had taken place in the UAE as described by Individual X and considered that this method of payment effectively bypassed financial restrictions and the embargo imposed by the European Union.

Belgian authorities also concluded that the transaction between the Iranian company and Company A could be linked to the financing of proliferation-sensitive nuclear activities or the development of nuclear weapon delivery systems.

[138] See footnote 97.

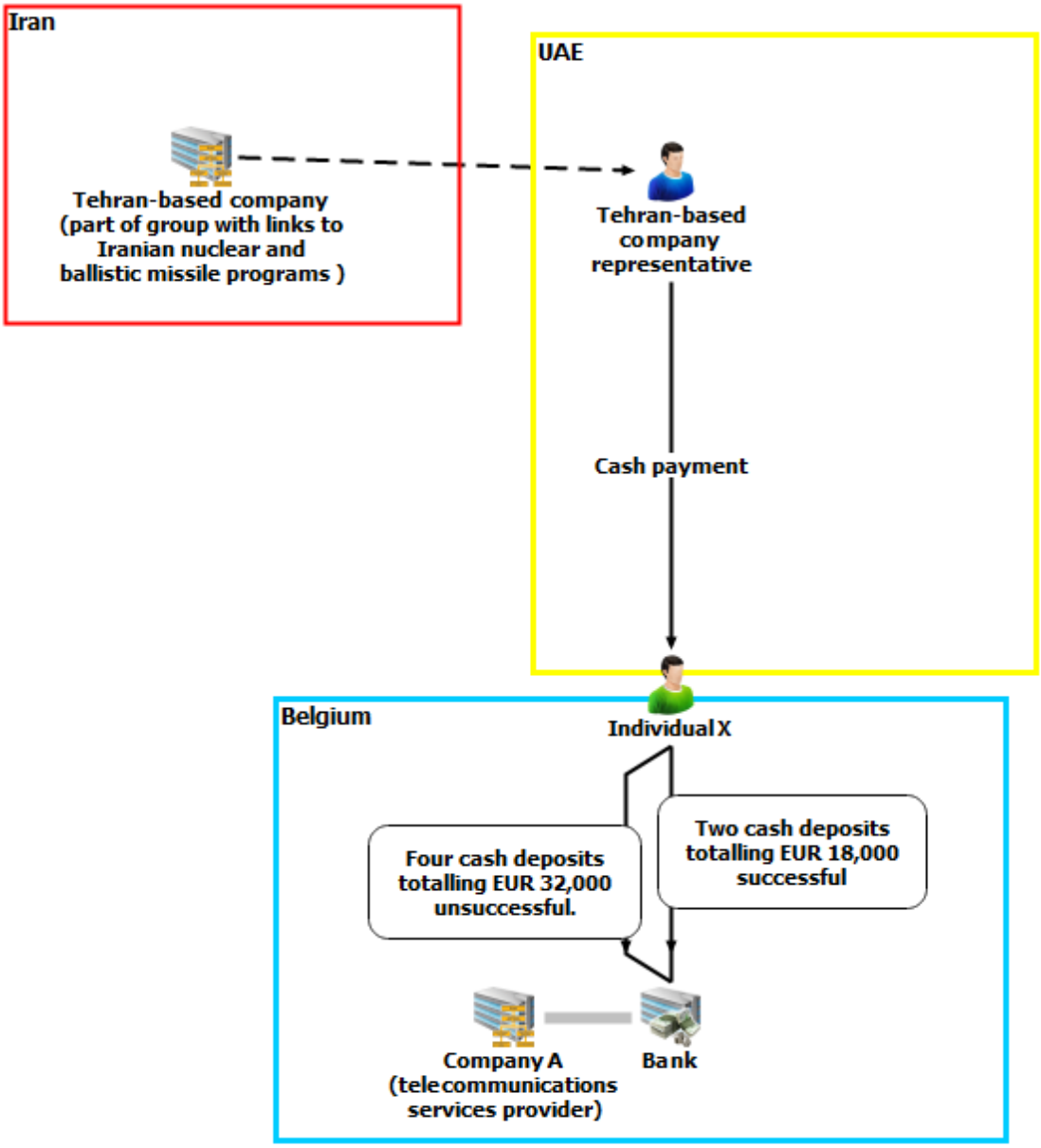


Figure 43. Belgian businessman paid in cash in the UAE for telecomms services in Iran

Key Points

- Payment of cash, possibly intended to circumvent financial sanctions on Iran;
- Cash transfers took place in the UAE;
- The Belgian bank involved appeared to be monitoring the businessman's accumulated cash deposits.

Case 43: Personal banking products used for procurement of items for potential use at universities in Iran (1) (2015-2016)

The following is based on information provided by a multinational bank, Bank A.

A customer of Bank A allowed his personal banking products to be used by a third party to buy chemicals which it is alleged that the third party then took with him to Iran and sold to universities (figure 44).

Upon reviewing the invoices, it turned out that three of the items purchased were listed on the UK Export Controls list.[139] There was no evidence of the appropriate export licenses being sought in advance. The payments made in respect of these invoices could therefore have been indirectly linked to export control violations.

[139] The three items were: Imidazole buffer substance ACS 1, Hellma liquid and Deuterium oxide.

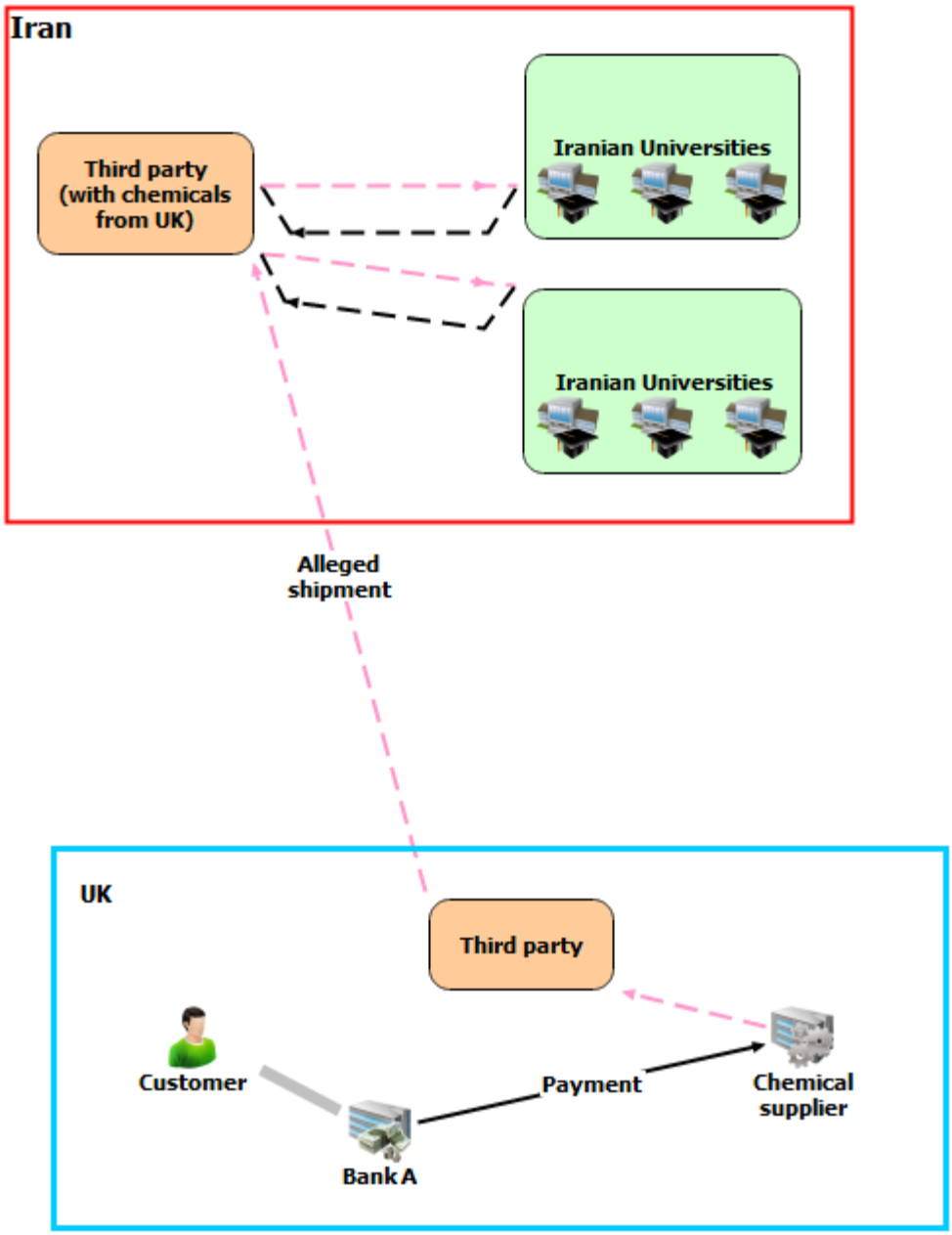


Figure 44. Chemicals for use in Iran purchased using personal banking products.

Key Points

- Personal banking products used to purchase an industrial product (chemicals);
- The involvement of universities in an apparent attempt to circumvent export licensing requirements.

Case 44: Personal banking products used for procurement of items for potential use at universities in Iran (2) (2015-2017)

The following is based on information provided by a multinational bank, Bank A.

A customer of the Bank used her personal banking products to purchase a turbine on behalf of a relative from a company based in New which manufactures and supplies photovoltaic and hydro solutions for the generation of electricity in remote areas. The turbine was due to be exported to Iran, but was intercepted by Customs in New Zealand due to a UN embargo, because the authorities believed that the hydraulic turbine could be used to make the drive for a centrifuge for uranium enrichment (figure 45).

The customer maintained that the good was a solar panel for her family home in Tehran. However, her relative was a university professor and said that the good was a "small water turbine" which was purchased for his own research activity. The turbine cost less than about USD 2,500.

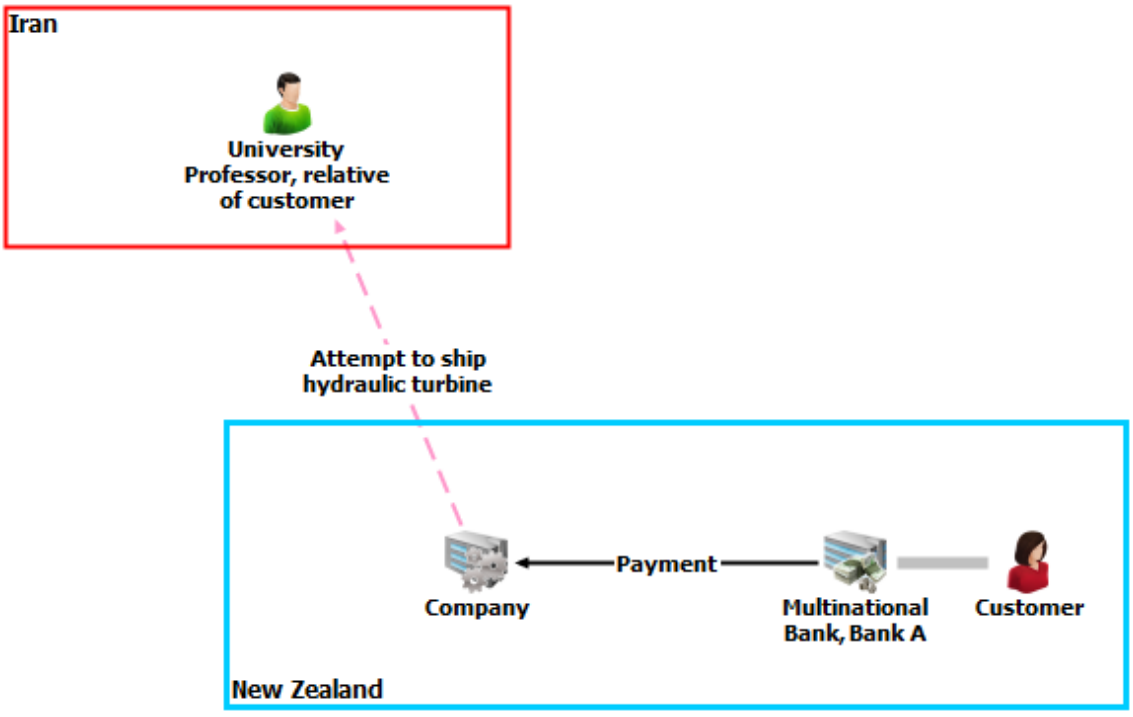


Figure 45. Purchase of turbine for use in Iran using personal banking products

Bank A's key takeaway: detection of these types of purchases (cases 43 and 44) is challenging due to the nature of the personal banking products, particularly where a merchant acquirer[140] is involved and the transaction is settled by another financial institution.

[140] A merchant acquirer is a bank or financial institution that processes credit or debit card payments on behalf of a merchant.

Key Points

- Personal banking products were used to purchase an industrial product;
- The explanations for the purchase were inconsistent;
- One of the explanations offered was university research.

Case 45: Financing of procurement using intra-company transfers (2016)

The following is based on information provided by the authorities of a European country.

A company in a European country (A) manufactured a specific metal of very high purity. The company was part of a large multinational commodity company with headquarters in another European country (B).

In 2016, the authorities of Country A were approached by the headquarters of the commodity company for a license to sell to Iran a very large amount of the metal produced in country A. All details of the orders were to be handled by the commodity company´s headquarters in country B. Payment would be made by means of intra-company transfer from the company´s headquarters in country B to the manufacturer in country A. Details of how the payment was to be transferred from the Iranian end-user to the company´s headquarters were not known to authorities in country A.

The product, although not controlled under export control lists, was suitable amongst other uses as a crucial component in highly specialized alloys such as maraging steel, Ti-DSS and Inconel. These alloys both have very high strength and very good corrosion-resistance properties and are extensively used within the aerospace field and for missile parts, as well as nuclear processing plants. The Iranian end-users of the product, although not designated under sanctions regimes, were known to be connected to Iran´s ballistic missile programs. Authorities in Country A refused a license for export to Iran on “catch-all” grounds.

The company’s headquarters in Country B then asked the authorities in Country A whether export from country A to Iran could take place through a third European country, Country C (figure 46). The authorities of country A refused permission and informed authorities in both country B and C.

Subsequent information suggested that the international commodity company eventually succeeded in collecting sufficient amounts of the metal from supplies it held in its warehouses in a number of different countries. The international commodity company then exported the metal to the given end-user in Iran. The product collected from its warehouses in different countries had been exported from Country A prior to the order from Iran.

Authorities in Country A commented that the proposed business model made it very difficult for the manufacturing company in Country A to carry out due diligence. The manufacturer had no or little insight into the end-user nor the source of funding. Countries with weak export controls might be more willing to license the deal than was Country A.

Key Points

- Intra-company financial transactions, in the form of ledger accounting

arrangements, might be a mechanism under some circumstances to circumvent requirements to declare or seek approval for international financial transactions involving sanctioned countries, in this case Iran.

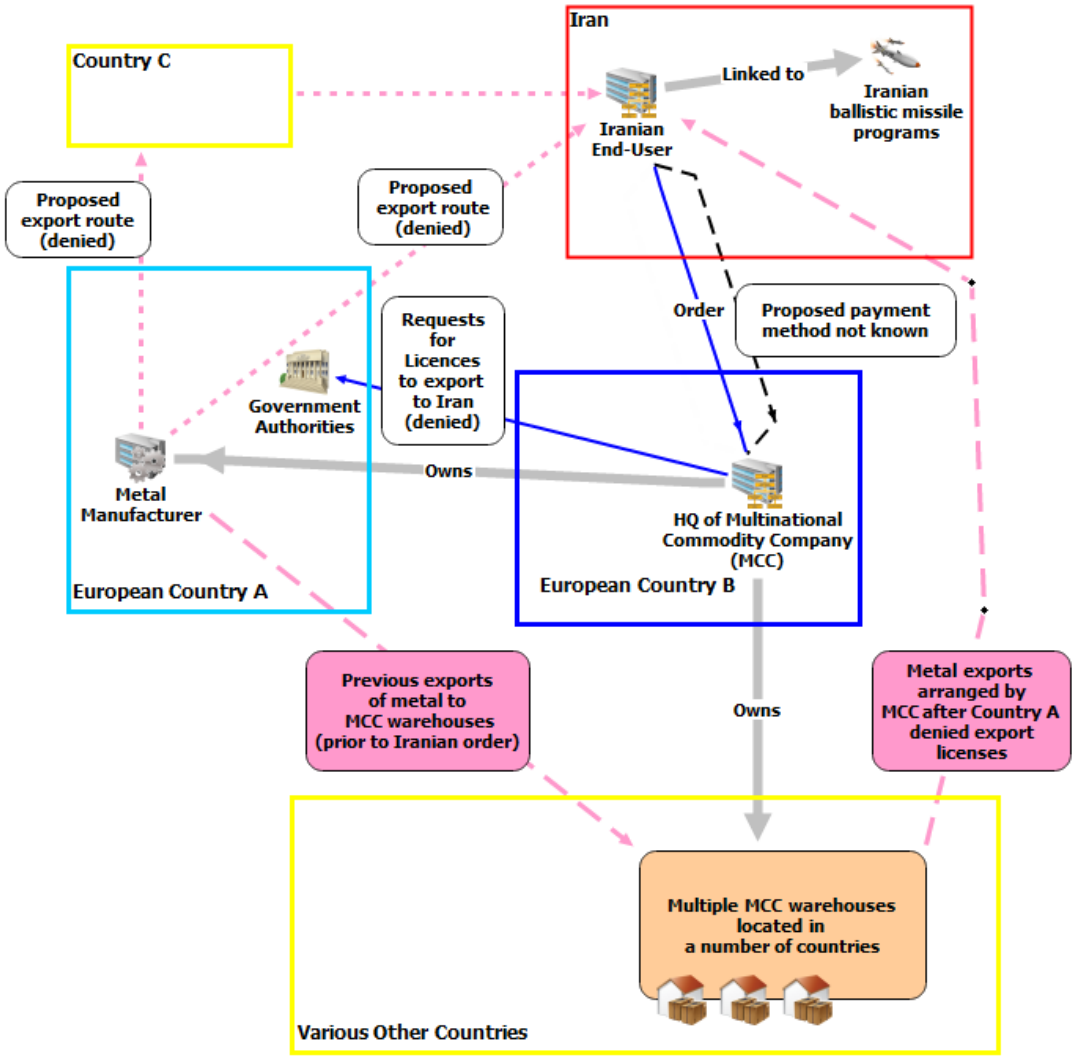


Figure 46. Procurement methodology of a multinational commodity company

Case 46: Common characteristics of financial networks

The following is based on the investigative experience of a multinational financial institution (2017).

The financial institution had found a number of common characteristics of financial networks which appeared connected to Iran.

The core companies (i.e. those companies that were central to and likely knowing participants in the sanctions evasion activity) traded with a more diffuse network located in many different countries. The type of connections between elements of the network included:

- Common PO box numbers (for example in the UAE);
- Common directors or other personnel;
- Activity apparently coordinated after a particular event, such as resubmission of a restructured payment by different companies after an initial payment from a company had been rejected;
- Websites of different companies set up by users based at a common IP address;
- Internet bank accounts set up by users based at common IP addresses.

Some of the companies in the network lacked a website or other internet presence. A number had Chinese or Iranian directors, some of whom possessed passports issued by St Kitts and Nevis. Some of the companies were involved in trade that appeared incongruent with their stated business (for example textile companies trading electronic goods). Some of the transactions appeared to correlate with activities of Iranian oil tankers.

The financial institution concluded that the activity observed was mainly linked to payments connected with exports of oil and petrochemicals by Iran to the Far East and China.

Pakistan

Case 47: Procurement for Pakistan's WMD programs through front companies in UAE (2006-2007).

The following is based on information contained in US court documents.

According to US court documents,[141] Individual A, a Pakistani-based national owned a trading company in Karachi, NewTech Global that did business with Pakistani government entities. Individual B was a Pakistani permanent resident of the US and owner of Computer Communications USA (CC-USA), incorporated in Maryland. He seemed to work primarily from home.

Between 2006 and 2007, Individual A received orders from Pakistani government entities, including restricted entities[142] and would direct Individual B to purchase items in the US to fulfill these orders (figure 47). Individual B then negotiated prices, placed orders and arranged shipping. He supplied shippers with false information about the nature of the items, their value and identity of the end-user.

Shipments to restricted entities in Pakistan were shipped initially to Dubai (companies used for this purpose included Bosfor Trading and Shairook Scarps USP (LLC)). Funds for the shipments were transferred by wire from Pakistan and Dubai to US-based bank accounts, including Individual B's personal account and CC-USA's account. Individual B used his personal account to pay manufactures and suppliers, and also third parties that he used to procure items. Payments to manufacturers and suppliers were also made using personal and business credit cards (see Table 5).

[141] United States of America v. Naeem Malik and Nadeem Akhtar, Indictment filed in the US District Court for the District of Maryland, case 10 CR 00103, 11 March 2010.

[142] Entities to which exports from the US would be subject to licenses. These included Pakistan's Space and Upper Atmosphere Research Commission (SUPARCO), Pakistan Atomic Energy Commission (PAEC) and its subordinate entity, Pakistan Institute for Nuclear and Science Technology, National Development Complex, all fuel reprocessing and enrichment facilities, uranium processing facilities, conversion and enrichment facilities, heavy water production facilities and co-located ammonia plants, and reactors and power plants. At the time the latter included the Chasma Nuclear Power Plant 1 (CNPP) and a research reactor maintained by the Pakistan Institute of Engineering and Applied Sciences (PIEAS).

Table 5: Payments arranged by Individual B in connection with procurement on behalf of Pakistani entities

Date	Amount (USD)	Method of payment	Items
May 2006	5,000	Payments from CC-USA's account to a bank account of a wireless company in Illinois	Dosimeters (model DMC-2000S)[143]
Jun 2006	10,000		
Jul 2006	30,350		
Sep 2006 (twice)	25,000		
May 2006	1,112.50	Payment from credit card of Individual B associate in California	Nuclear grade resins (NRW100)
June 2006	9,475		
Sep 2007	3031.59	Credit card payment from CC-USA account to a US company	Model 90 fixed coaxial attenuators
Jul 2007	9,487.50	Wire transfer from CC-USA account to a US company	Series 20M selector switches
Sep 2007	23,775.00	Cheque from CC-USA bank account to a US company	
Sep 2007	15,000.00	Payments to a US company	
Sep 2007	15,000.00		
Jul 2007	5,000.00	Payment to a US company in the name of a third party at a UK billing address.	MPC 9300 manual alpha-beta counting system
Jan 2008	28,750.00	Wire transfer from CC-USA bank account to a US company	
Jan 2008	3,050.00	Wire transfers from CC-USA bank account to a US company	3M abrasive sheets
Feb 2008	4,051.48		
2008	No info	No info	Model 2350-1 Data Logger, Model 44-10 Gamma Scintillation Detector, Model 44-94 Diamond Cluster Pancake (Detector), Model 44-38 Energy Compensated Detector

[143] These items required an export license, but no license applications were made.

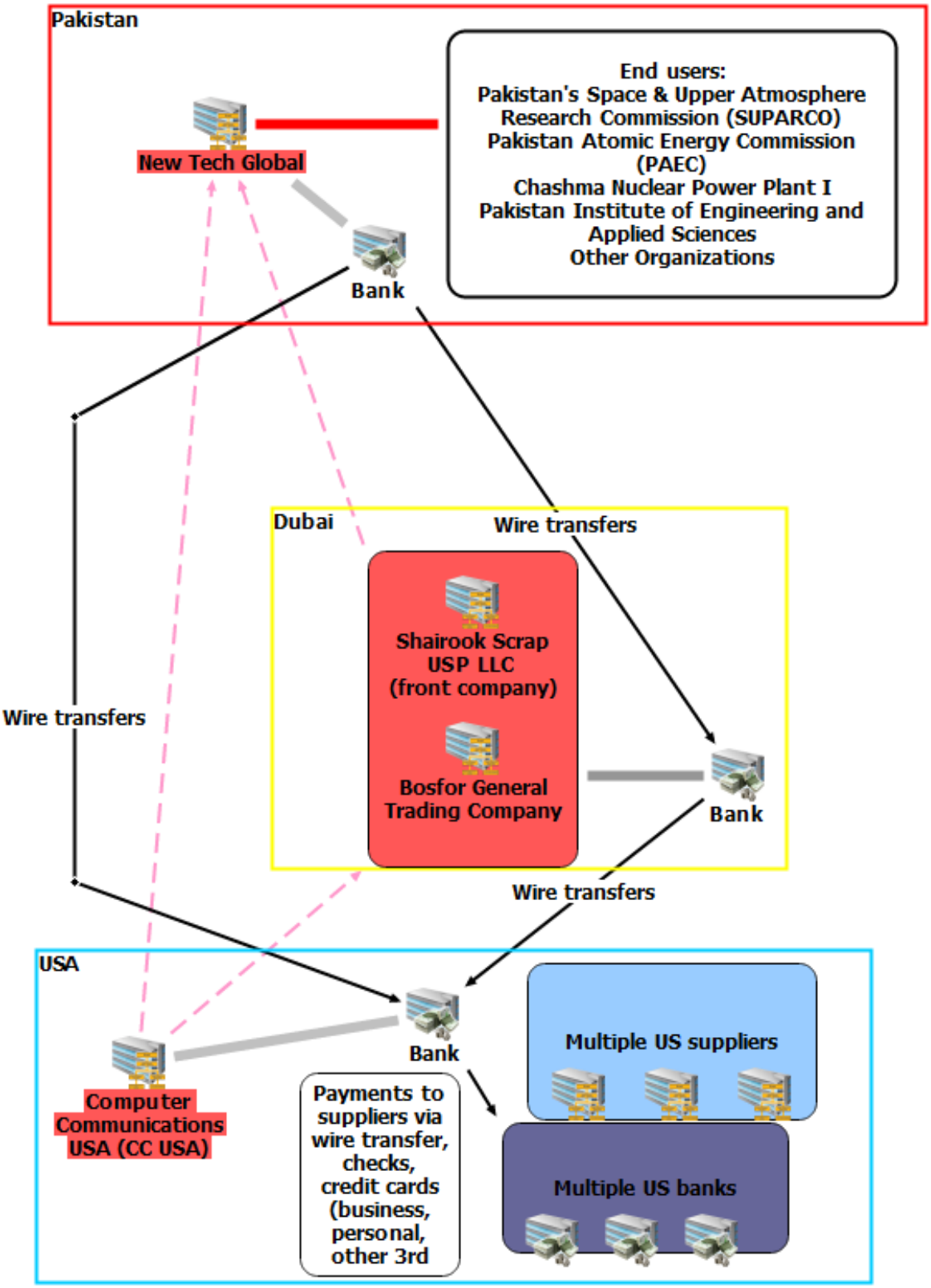


Figure 47. Procurement by Pakistan through front companies in UAE

Key Points

- The businessman was connected with the country of proliferation concern. The nuclear-related items he procured would not appear to be consistent with the business of his company (Computer Communications);
- Companies in the UAE were used both to transfer funds and as consignees for items subsequently transferred to Pakistan;
- Payment methods varied included wire transfers, credit cards and cheques, involving both business and personal accounts.

Case 48: Alleged procurement network operating from Pakistan (2009-2013)[144]

The following is based on information contained in US court documents.

According to an Indictment filed in 2014,[145] a US-based company, Optima Plus International LLC, exported a range of dual-use items to Pakistan between 2009 and 2013. The items were imported by a Pakistani company, Afro Asian International Pvt Ltd, and transferred to the Pakistan Atomic Energy Commission, PAEC (see figure 48). PAEC is listed on the US Department of Commerce restricted Entity List,[146] and many of the items transferred were subject to export licensing applications. According to the Indictment none was applied for.

In addition, according to the Indictment, Optima and Afro Asian colluded to mislead US authorities by falsifying invoices and shipping documents by mislabeling and undervaluing the items shipped to Pakistan.

The Indictment does not describe how Optima received payment from Afro Asian, nor how Afro Asian was reimbursed by PAEC. However, the case is of interest because as described several elements of this Pakistani network resemble networks described above connected with DPRK's, Syria's and Iran's proliferation programs. Financial institutions unknowingly involved in processing transactions connected with this network would likely have come across similar suspicious indicators.

[144] This case was Case No 18 in the Interim Report published 5 February 2017.

[145] 22 January 2014, US District Court for Middle District of Pennsylvania Case No 14 CR 29 US v. Shafqat Rana, Abdul Qadeer Rana, Shahzad Rana, Optima Plus International LLC, Afro Asian International Pvt Ltd The case has yet to come to court.

[146] PAEC is described on the Department of Commerce's restricted entity list as "…engaged in activities that could result in in increased risk of diversion of exported items to weapons of mass destruction programs, to nuclear proliferation activities…."

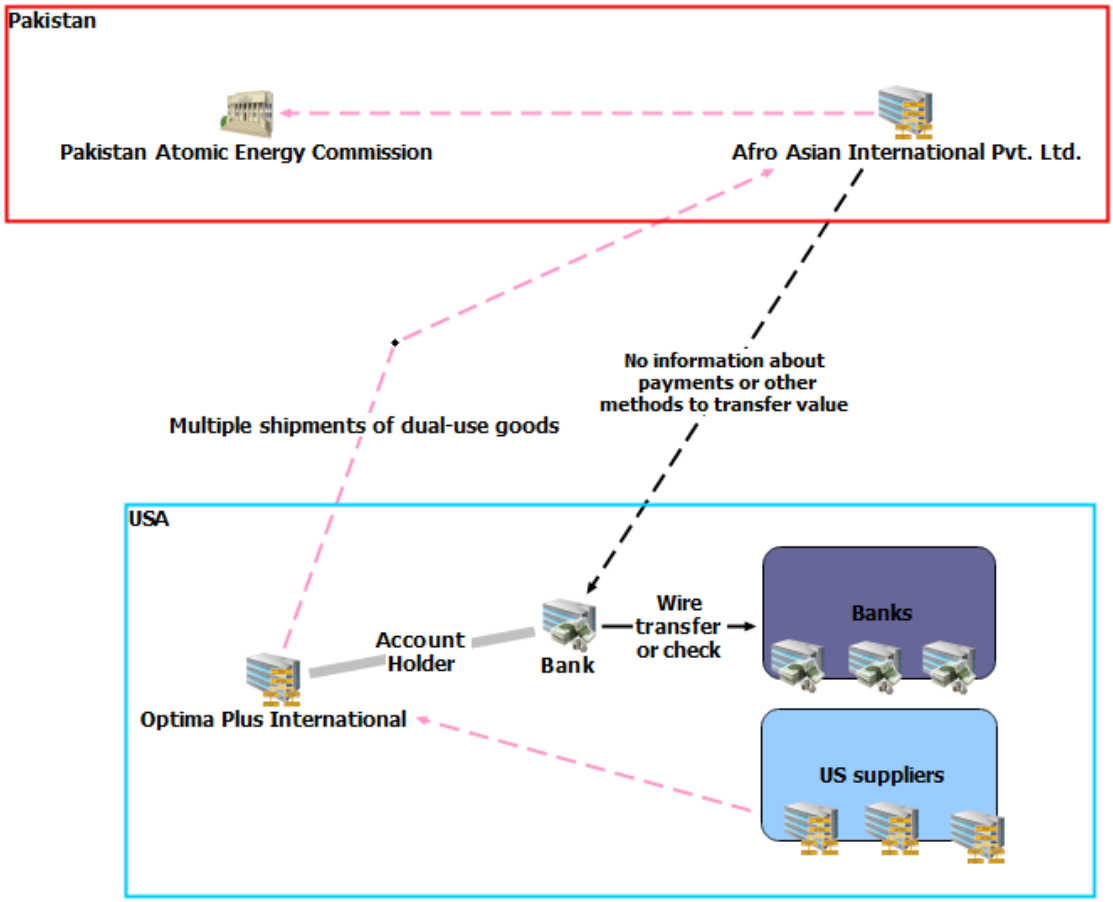


Figure 48. Alleged transfers of dual-use items to Pakistan

Key Points

- The exporting company based in the US appears to have been a small, privately owned broker/intermediary;
- The owner of the company was linked to the country whose proliferation program he was allegedly supplying;
- Documentation (such as shipping documentation and invoices) was falsified.

Cases in which the State involved in proliferation is not specified

Case 49: Following rejection, a procurement order is repeated by a second company in a different country (2006)

The following is based on information provided by Canadian Authorities.

Information analyzed by FINTRAC identified individuals and entities that were suspected of being involved in the procurement of technology in 2006 that could possibly be used for WMD programs. This case came to FINTRAC's attention through information shared by the FIU of a Country Z. Subsequent information was also obtained through media reporting after enforcement action was taken against the individuals involved in the scheme in Country Z.

Company A, located in Country Z, was a manufacturer of technology that could possibly be used in WMD programs. Company A received an order for technology that had nuclear and military applications from Individual 1, an employee of Company B in Country X. Company A turned down the order from Individual 1 on the grounds that export of the requested goods to Country X was legally prohibited for companies operating in Country Z, but within two days Company A received an order for identical technology from Individual 2, a Director of Company C in Canada (figure 49). Company C, a software engineering firm, had been in operation since the early 1980s.

Company A noticed that Company C was copying Individual 1 on a series of e-mail exchanges.

Company B was headed by Individual 3 who had also created Company C (he was listed as its former Director General). Individual 2 operated Company C on behalf of Individual 3.[147]

[147] Information available to FINTRAC indicated that Individual 2 held a Canadian passport. FINTRAC does not know if Individual 2 was a dual national. Individual 2's name and transaction activity indicated possible familial links to Country X.

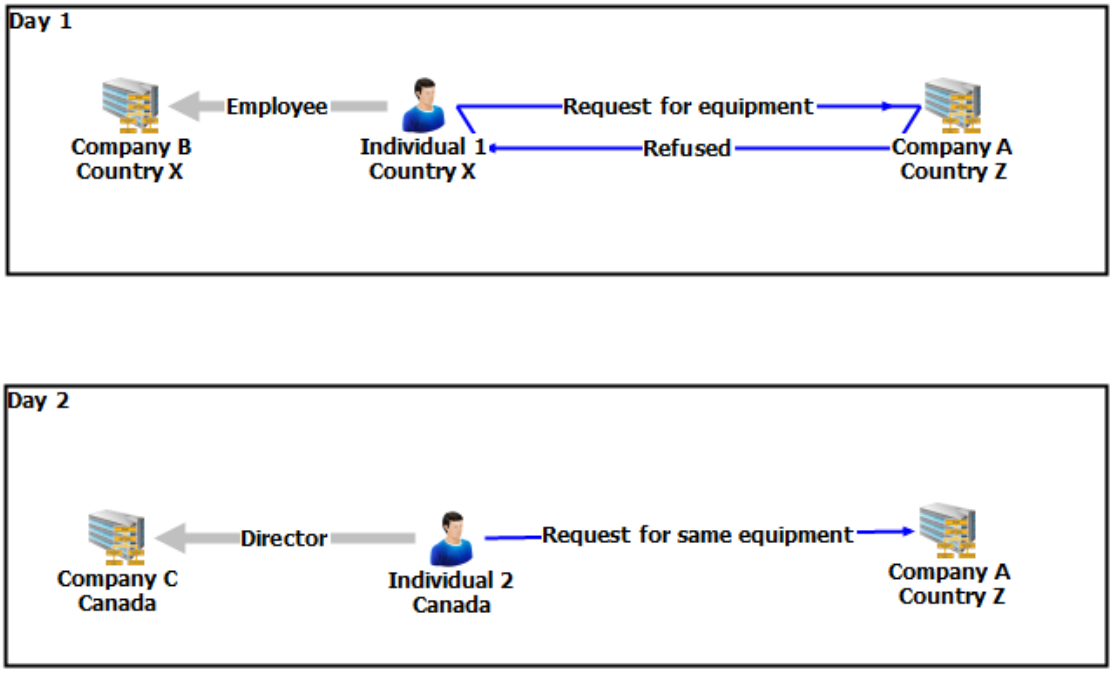


Figure 49. Following refusal by a manufacturer of an order from one country, an order for identical equipment was received by the manufacturer from another country (Source: Figure supplied by Canadian authorities)

Over a two-month period following the order from Individual 2 to Company A, Company B made a series of electronic funds transfers (EFTs) to Company C, totaling USD 100,000.[148] The individual EFTs were all at or above the CAD 10,000 threshold for a report to FINTRAC and as such there was no indication of structuring.

A few weeks later Company C made an EFT to Company A to cover an initial deposit on the order. This was followed a month later by an EFT covering the balance due on the order (figures 50, 51).

[148] It is not known whether Company C made a profit on the deal.

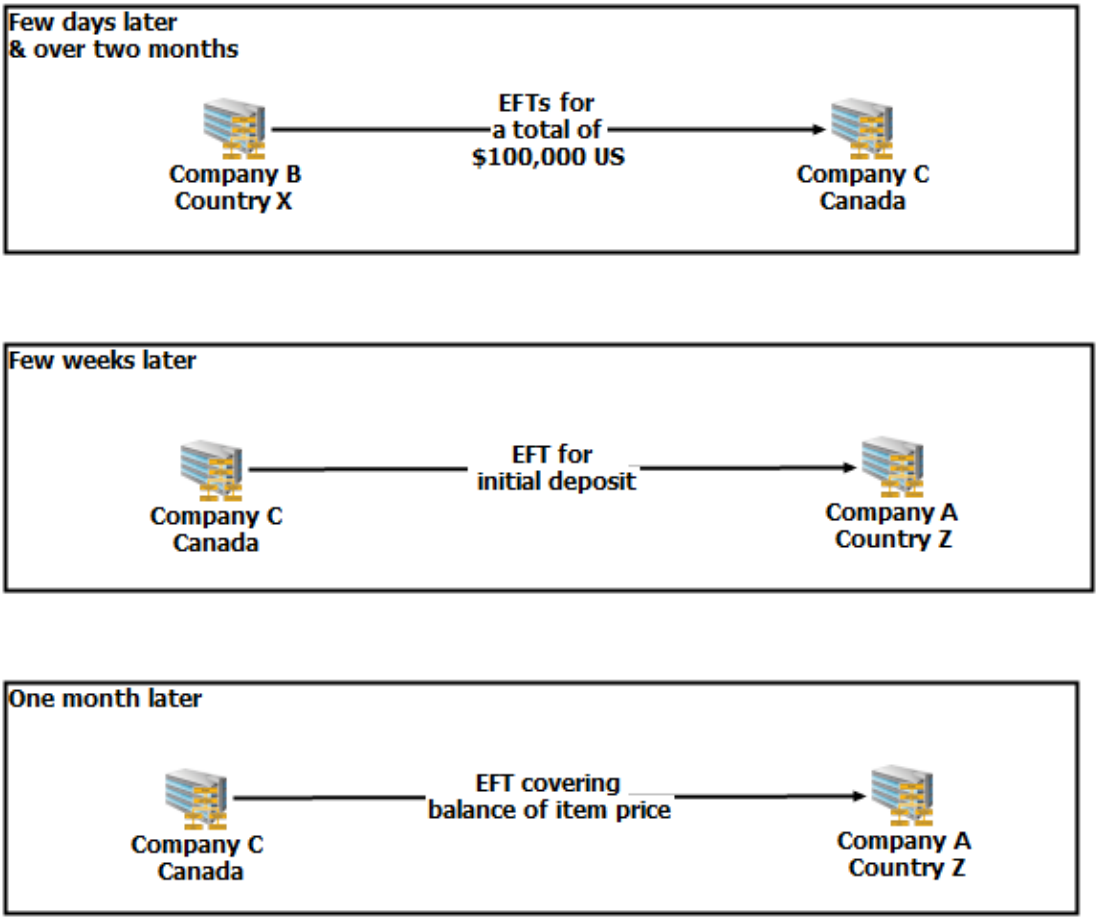


Figure 50. Funds are sent from the country that was refused the order to the country that was accepted, and funds transferred to the manufacturer (Source: Figure supplied by Canadian authorities)

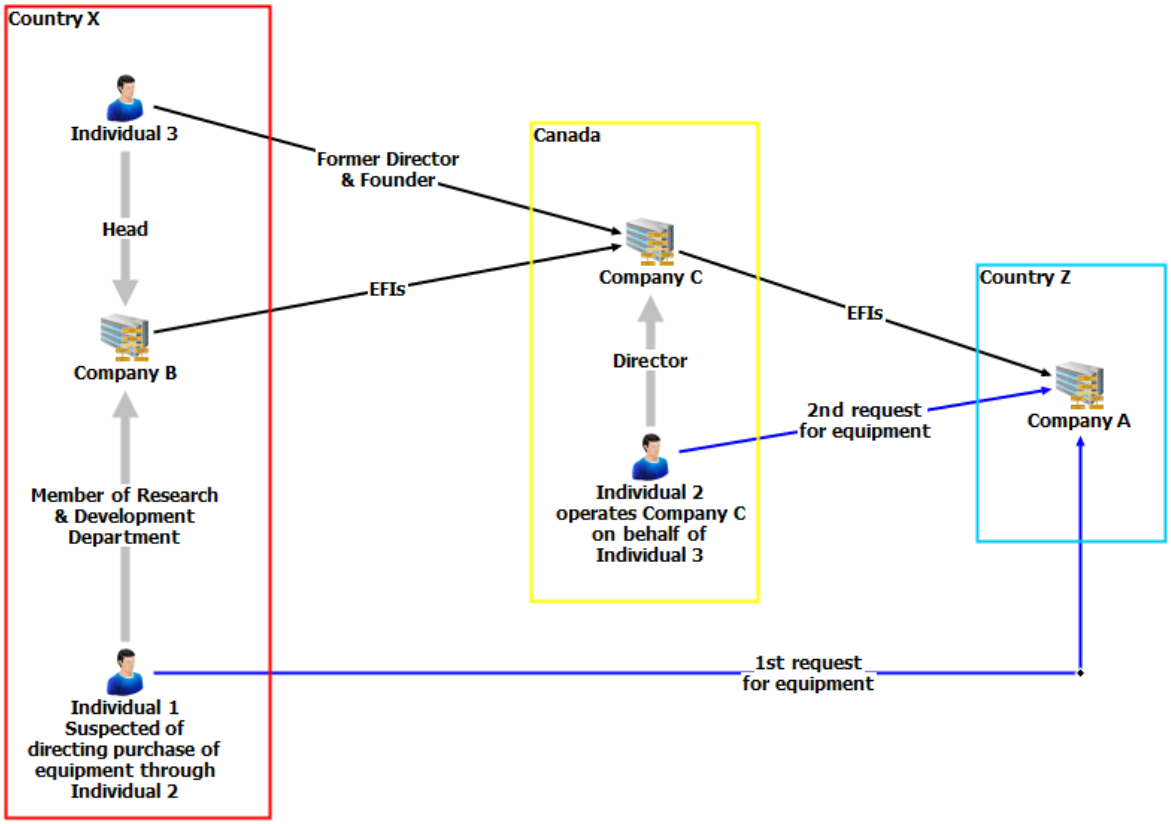


Figure 51. Summary of order and payment channels (Source: Figure supplied by Canadian authorities)

Key Points

- Following initial refusal by the supplier of an order by the first company, within two days the order was repeated by a second company in a different country;
- Although the second company was well-established, its business was not consistent with the technology it was trying to order;
- Funding for the purchase by the second company was supplied by the first company.

Case 50: Sale of US-manufactured carbon fiber to China financed through bank in Luxembourg (2007)

The following is based on information provided by Luxembourg authorities.

In November 2013, Individual 1, a businessman based in New York, USA, was sentenced to three months imprisonment, together with fines and penalties, for shipping high-grade carbon fiber to China without a license in 2007. He had mis-declared the final destination of the shipment on the export declaration form, and whether it required an export license.

According to the indictment filed by US prosecutors,[149] a co-conspirator based in Belgium (CC-1) ordered the carbon fiber from Individual 1, and on 17 May 2007 sent USD 100,883.86 by wire transfer from Luxembourg to Individual 1's US bank account (figure 52).

According to Luxembourg authorities, this was one of a series of transactions between CC-1 and Individual 1. CC-1, acting as the broker between the US supplier and the Chinese customer, initiated fund transfers to Individual 1 from an account he held at a Luxembourg bank, usually in the form of a single sum. The Chinese customer would wire the amounts due into CC-1's account. Bank account statements often indicated that transfers were linked to the sale of carbon fibers, or sometimes they indicated only an invoice number.

CC-1 made few attempts to hide the trade even though he was aware that he violated US law. Unless the bank had queried whether the specific type of carbon fiber that CC-1 wanted to pay for would need a US export license, it had no reason to suspect anything untoward either in the payments from CC-1 to Individual 1's bank in the US, nor the payments to CC-1's account from China.

Moreover, CC-1 made his transfers from a small local office of the Luxembourg bank, close to his house, and the clerk at the bank and CC-1 knew each other well. CC-1 cultivated his status as an experienced and distinguished businessman with important financial assets (a large house for private use, flats in France that he rented to other people) perhaps to encourage trust in the individual transactions.

[149] US District Court Southern District of New York, Case 1:12-00302, 19 April 2012.

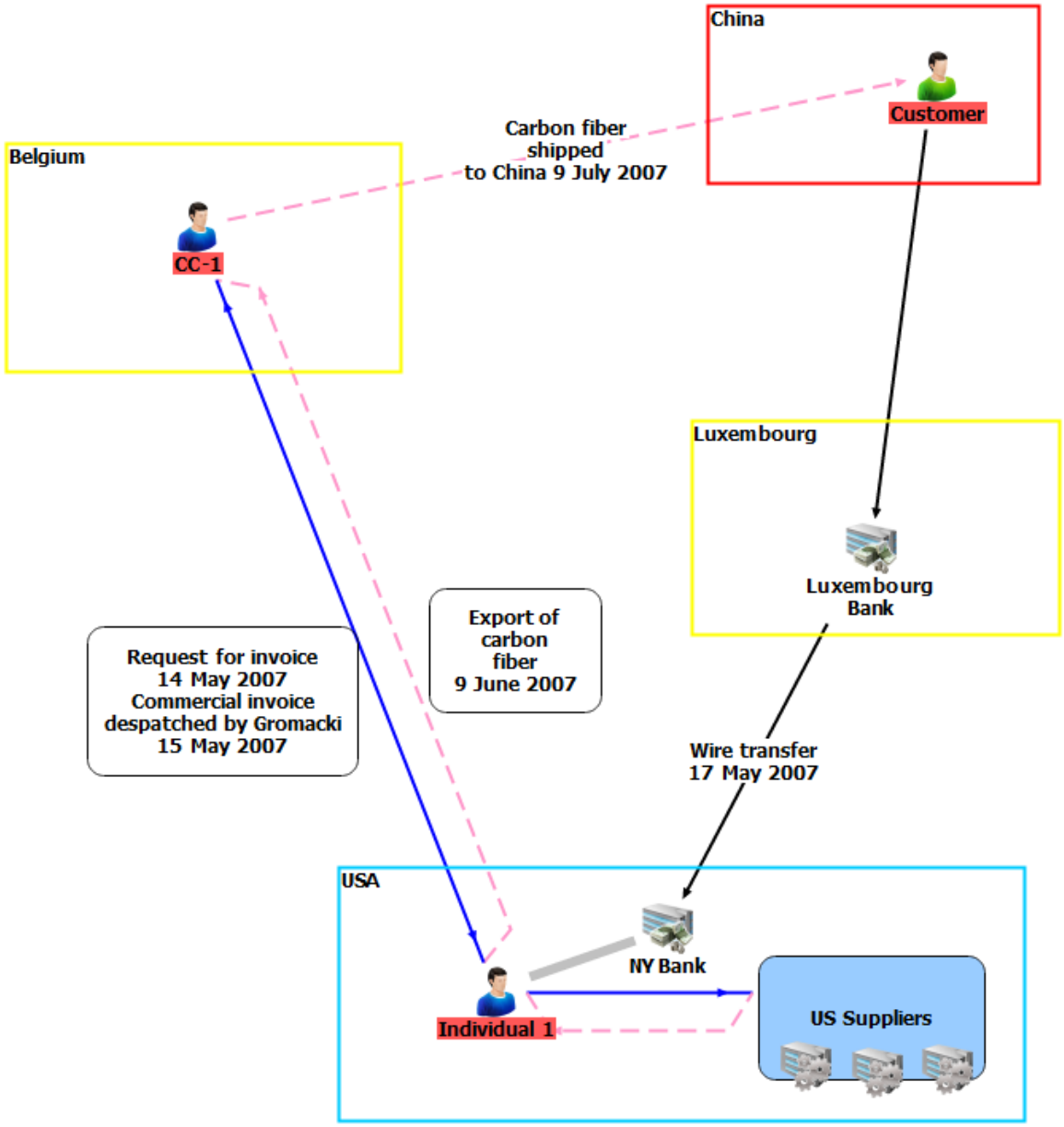


Figure 52. Payment for procurement by Chinese entity takes place through bank in Luxembourg

Key Points

- CC-1, a Belgian businessman, transacted this business through a small bank in a neighboring state, Luxembourg, possibly because he judged his business transactions with a Chinese entity would draw less attention there.

Case 51: European company possibly involved in diversion of goods to sanctioned entity (2009)

The following is based on information provided by Australian authorities. The Australian authorities cannot confirm that the transactions are connected to a designated entity and/or a proliferation financing offence.

In 2009, a company lodged an export declaration to export goods to a country in the Middle East. The named end user gave rise to concerns that the goods might be made available to an entity acting on behalf, or at the direction of, a designated entity in contravention of sanctions. Officials prevented the goods from being exported.

Subsequently, a company based in Europe (the purchaser of the goods) claimed there was an error on the shipping instructions and the goods were not in fact destined for the Middle Eastern country. The Government remained of the view that, given the initial shipping instructions and the company's previous export history, the material was intended for the Middle Eastern country, whether directly or indirectly, and that UNSC sanctions prohibited such supplies.

Case 52: Procurement possibly paid for by credit card (2012)

The following is based on information provided by Australian authorities. The Australian authorities cannot confirm that the transactions are connected to a designated entity and/or a proliferation financing offence.

In 2012, an Australia-based technology company sold technology to a South-East Asia based entity that was alleged in open sources to be a front for a company based in a country subject to sanctions (figure 53).

The payment for the technology itself likely occurred through a non-reportable method such as a credit card payment, possibly to circumvent AML/CTF reporting requirements. However, incidental payments (for freight charges) were made through two established banks. These were reported under AML/CTF obligations.

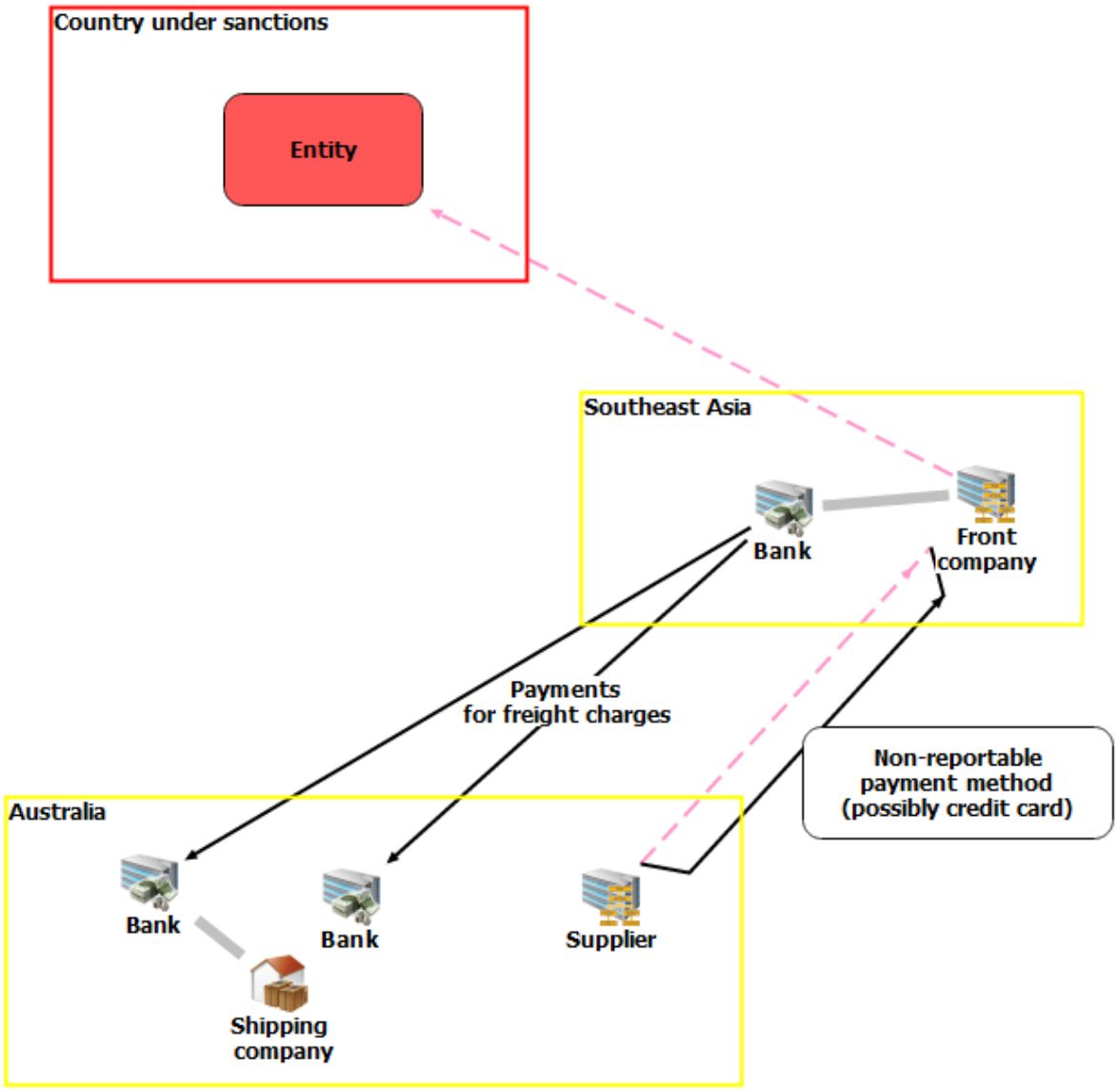


Figure 53. Payments for freight charges reveal possible shipment of concern

Key Points

- Payments for the technology itself were made through a non-reportable method (such as by credit card). Payments for shipping were reported, presumably because of the open source information regarding the front company.

Case 53: Payments for dual-use goods took place via shell companies and an Australian company (2012)

The following is based on information provided by Australian authorities. The Australian authorities cannot confirm that the transactions are connected to a designated entity and/or a proliferation financing offence.

In 2012, a private company registered in Australia received funds via telegraphic transfer from several limited liability companies incorporated in multiple Middle East jurisdictions (figure 54). It is likely the companies, some of which were based in free trade zones, were shell entities. Office holders of the Australian-based company had links to a sanctioned country. Once received by the Australian company, the funds were then remitted from Australia to industrial manufacturers in Europe and Asia, referencing payment for goods with dual use applications in the nuclear industry.

It is likely that the routing of payments via likely shell companies in third-party jurisdictions including Australia was an attempt to obscure the payment by an entity in the sanctioned country for the procurement of dual-use goods.

The payments from Australia were halted, the relevant bank discontinued business with the Australian-based company and Australia forwarded on the relevant information to like-minded countries for further investigation.

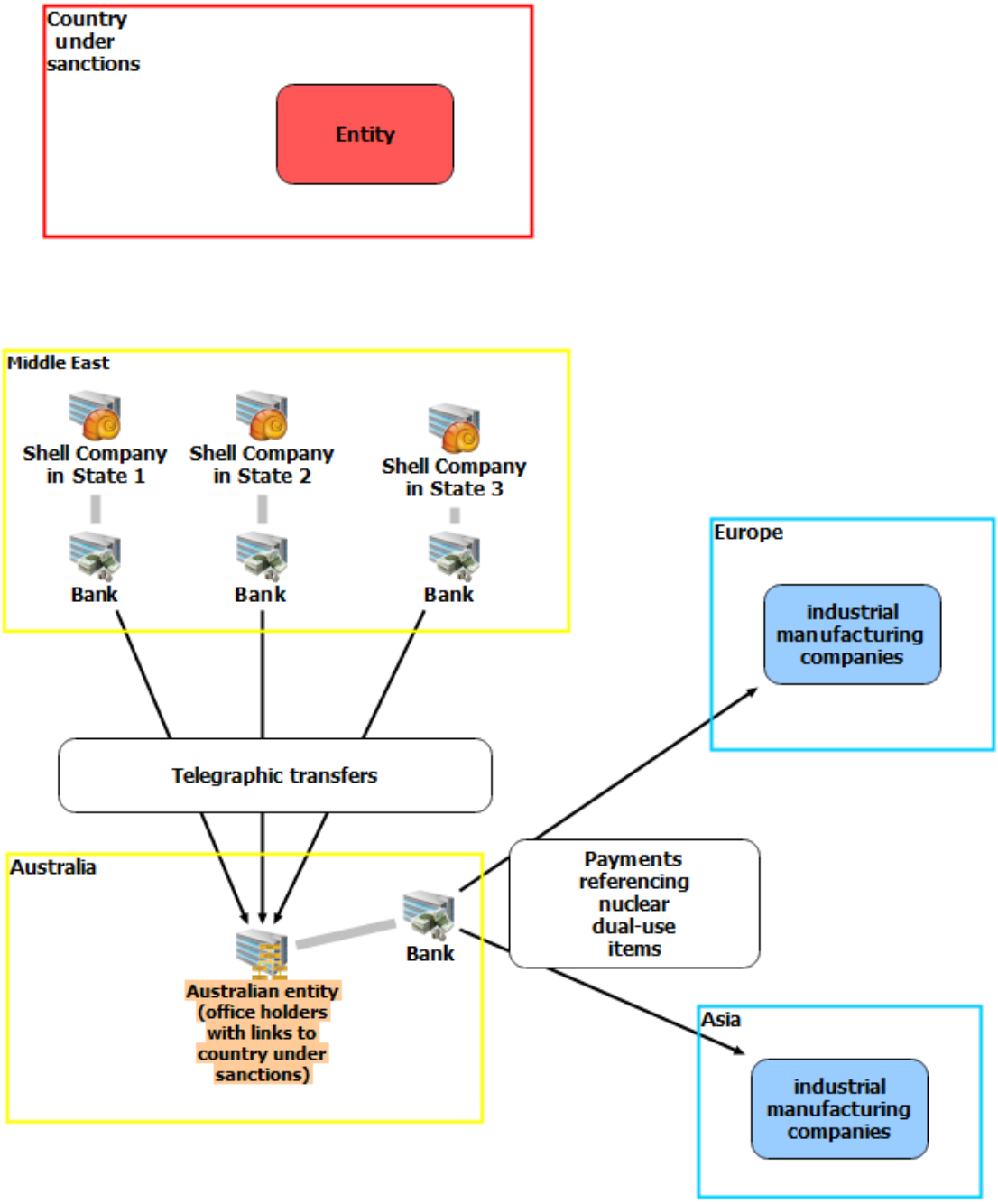


Figure 54. Suppliers in Europe and Asia funded via probable shell companies in the Middle East

Key Points

- Payments to manufacturers for dual-use goods were routed circuitously and channeled through shell companies and a company in Australia;
- The company in Australia acted as a money remittance business;
- The company office-holders had links to a sanctioned country.

Case 54: Financial transactions connected with mining deals allegedly channeled through third country (2013-2014)

The following is based on information provided by Australian authorities. The Australian authorities cannot confirm that the transactions are connected to a designated entity and/or a proliferation financing offence.

A number of Australia-based entities came to attention for possible sanctions contraventions as a result of media reports alleging involvement in mining deals in a country subject to sanctions between 2013 and 2014.

Open source reporting indicated that an Australia-based company announced a mining sub-license involving a company that may have been a designated entity.

The majority of transactions were allegedly channeled through a third country.

Case 55: Circumvention practiced by a professional firm (2017)

The following is based on information provided by Australian authorities. The Australian authorities cannot confirm that the transactions are connected to a designated entity and/or a proliferation financing offence.

In 2017, a professional firm sought to use its role as a professional facilitator to send funds to a company based in a country subject to sanctions via an Asia-based shell company (figure 55). The payment did not appear to relate to WMD proliferation or technology transfer; however, additional collection showed the professional firm sought to omit the ultimate beneficiary from funds transfer instructions at the request of the beneficiary.

The transaction was attempted through an established bank.

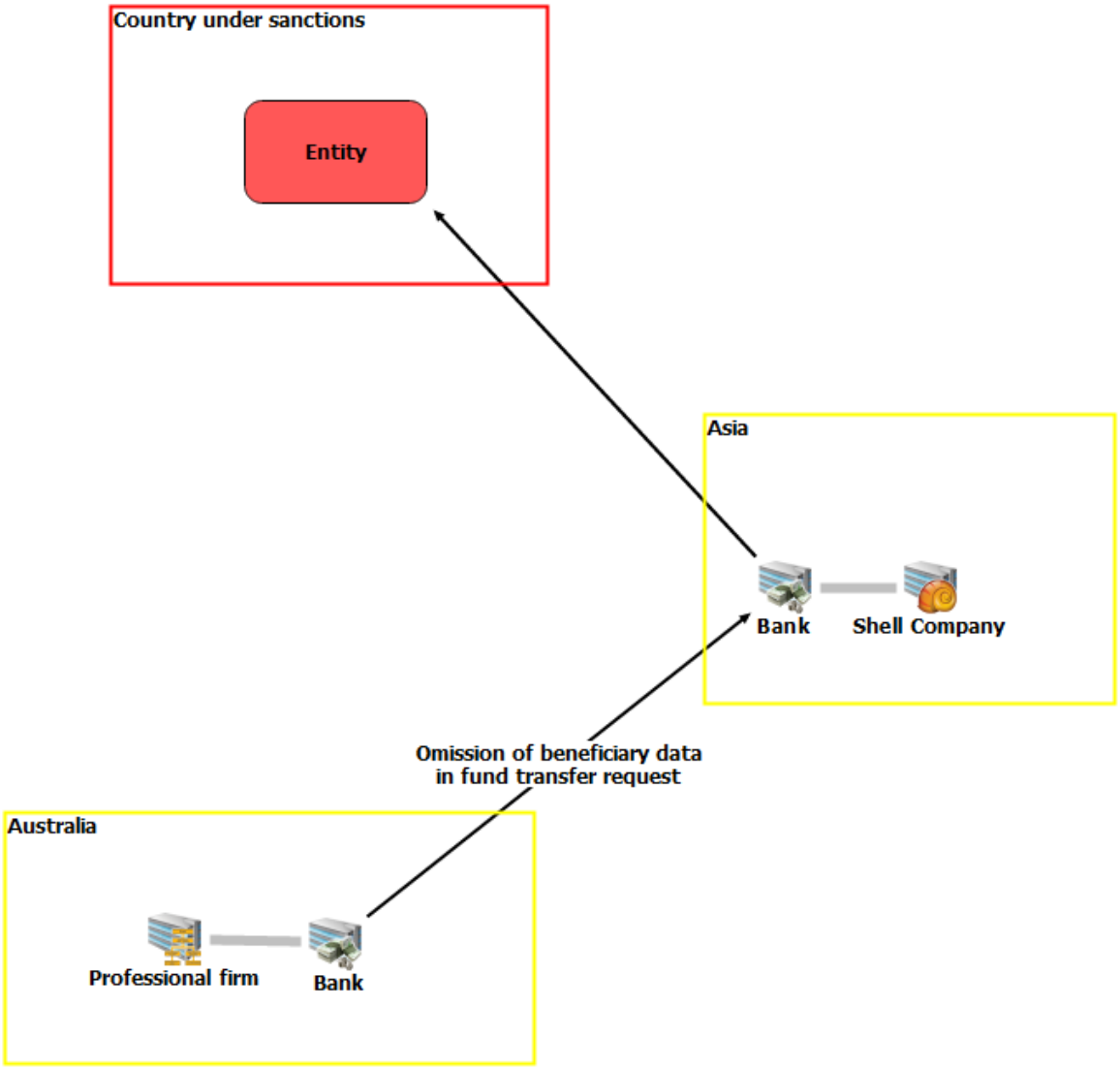


Figure 55. Beneficiary details removed from funds transfer request

Key Points

- The professional firm attempted to transfer payment through a shell company in Asia;
- Information about the beneficiary was removed from funds transfer instructions;
- On the basis of the information available it would appear that the bank reported the attempted transaction.

Circumvention of WMD-related Financial Sanctions

Case 56: Misappropriation of funds held by Central Bank of Iran overseas (1) (2011)

The following case is based on information contained in Republic of Korea (RoK) court documents and US court documents.

Following UN resolution 1929 (2010) of 9 June 1929, RoK imposed unilateral sanctions on Iran. In order to alleviate the impact on RoK companies trading with Iran, the authorities set up a trade finance arrangement. Purchases by RoK entities of Iranian commodities such as oil were paid by depositing Korean won into accounts belonging to the Central Bank of Iran (CBI) at two RoK state-run banks: Woori Bank and Industrial Bank of Korea (IBK).

Access to funds in these accounts was restricted and controlled: they could be used only to finance commerce with Iran approved by the RoK government and the Bank of Korea. The approval process included examination of relevant trade documentation.

According to a press statement issued by the Seoul Prosecutor's Office[150] a trading company, Company A, set up by a Korean-American (Individual A), applied in 2011 to import marble from Dubai for onward export to Company F Iran. On the basis of falsified documents Company A applied to the Bank of Korea for approval to finance the deal using the controlled funds in the CBI's accounts. Approval was granted and funds transferred to Company A, but instead of spending them on the marble trade Company A converted these funds to US dollars and remitted almost USD 1 billion them to a number of countries overseas. Individual A received a commission of about USD 10 million which was transferred to Company G in Anchorage, Alaska from where it was used for personal expenditures (figure 56).
It was not immediately clear whether this was an attempt to circumvent RoK's sanctions on Iran or a criminal scam. Individual A was convicted of violating RoK's foreign exchange trading act and given a two-year prison sentence.[151]

Further details of this case can be found in an affidavit subsequently filed in a US court in support of a property forfeiture application,[152] and in a later indictment charging Individual A with violations of US sanctions and money-laundering legislation.[153] In these documents, Company M in Dubai is named as MSL & Co Investment Trading (MSL Investment Dubai), an Iranian-controlled shell company, and Company F in Iran is

[150] Dated 24 January 2013 (http://www.spo.go.kr/seoul/notice/notice/notice01.jsp?mode=view&article_no=549099&pager.offset=0&search:search_val:search=%25C0%25CC%25B6%25F5&search:search_field1:equals1=A.etc_char5&search:search_key:search=article_title&search:search_val1:equals1=&board_no=116&stype=&info_id=&seq_id=).
[151] "South Korea reveals staggering $1 billion transfer fraud in Iranian money," Ju-Min Park, Reuters 25 January 2013.
[152] Affidavit of Sue Chambers in support of Verified Complaint, No. 3:14-cv-65 of 2 May 2014.
[153] United States District Court for the District of Alaska Case 3:16-cr-00142 of 14 Dec 2016.

Farsoodeh and Partnership Co, located on Kish Island, Iran. Company A in RoK is Anchore.

According to the US court documents, the scheme involved purported sales of Italian-origin marble and other construction materials, claimed to be finished by MSL & Co in the UAE, to Farsoodeh & Partnership on Kish Island. Documentation named KSI as the shipper and Farsoodeh Kish & Partnership Co, 3rd Flr, Sadaf Tower, Kish Island, Iran as the consignee. According to emails originating from Individual A, reproduced in US court documents, the scheme also involved fake or fraudulent documentation such as bills of lading, *pro forma* invoices and sell-and-purchase agreements.

According to US court documents, between 2011 and 2012, Individual A carried out at least some of these activities with three Iranians Pourya Nayebi, Houshang Hosseinpour, and Houshang Farsoudeh.[154] Nayebi was the owner of MSL & Co Investment Trading (MSL Dubai). He also owned Orchidea Gulf Trading, an Iranian front company based in the UAE designated by US authorities on 6 February 2014.

To support these activities, Individual A created a South Korean company, KSI Ejder Korean Inc in 2009. The name was changed to Anchore in 2011. He also created a number of additional companies including Dynamic First, AutoPex Corporation, Topex Corporation (established May 2011, name subsequently changed to Gem Art Corporation).

According to the US court documents, Individual A opened an account at IBK in the name of KSI in January 2011. Two days later, Bank Maskan, a commercial bank in Iran,[155] issued a payment order to the CBI account at IBK to transfer funds to KSI's new account, followed by a second payment order a day later. Bank Saman in Iran also issued a payment order.

According to the US court documents, between January 2011 and April 2014 Individual A transferred Iranian funds converted to dollars or euros to 50 different persons and companies around the world in more than 10 countries (see Table 6). There was no logical business behind these transactions.

[154] These three were designated by the U.S. Department of Treasury, in 2014 because they "established companies and financial institutions in multiple countries, and have used these companies to facilitate deceptive transactions for or on behalf of persons subject to U.S. sanctions concerning Iran."
[155] Designated by OFAC, US Treasury, between 16 June 2010 and 16 January 2016.

Table 6: Funds transferred overseas by Company A between January 2011 and April 2014.

Approximate sum (USD)	Recipients
862m	Orchidea Gulf Trading, UAE (February – July 2011)
994m	Five other companies in the UAE
10m	20 individuals and four companies in the US
670k	Three companies in Italy (payment in EUR)
430k	Six companies in Germany (payment in EUR)
330k	Two companies in Switzerland (payment in EUR)
140k	One company in Austria (payment in EUR)
80k	One individual and one company in France (payment in EUR)
46k	One company in the Netherlands (payment in EUR)
40k	One individual and one company in Canada
30k	Two individuals in Bahrain

US court documentation contains no information regarding the ultimate use of these funds. Many of the countries to which funds were sent feature in other case studies in this report, and it is possible that some of the funds that were misappropriated here were used for financing proliferation.

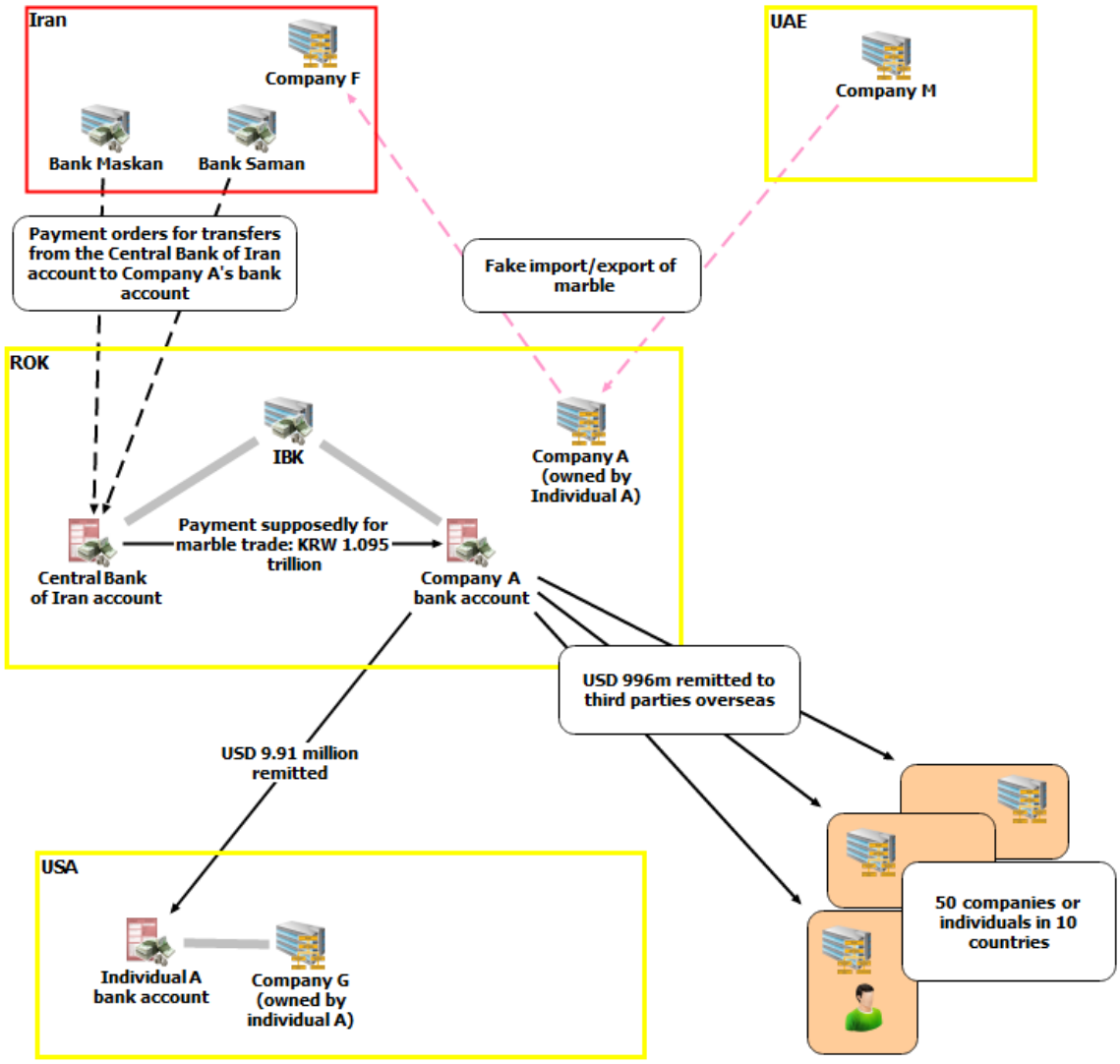


Figure 56. Funds belonging to the Central Bank of Iran are misappropriated and sent overseas (Key: IBK = Industrial Bank of Korea)

Key Points

- The three Iranians named in the US court documents are identical to those involved in Case 24. It is possible that these two cases are linked although there is insufficient information in the court documents to establish this;
- The end-users of the misappropriated funds are not known. Many of the countries to which funds were sent feature in other case studies in this report.

Case 57: Misappropriation of funds held by Central Bank of Iran overseas (2) (2011)

The following is based on information in open source media reporting.

Following US and EU financial sanctions on Iran, Indian authorities set up an arrangement in 2012 under which partial payments in rupees for Iranian oil imports were deposited into accounts held by the Central Bank of Iran (CBI) at UCO Bank Ltd.[156] Indian exporters to Iran could claim rupee payments from UCO Bank against letters of credit opened by certain Iranian private banks (i.e. a form of trade finance).[157]

According to early 2015 media reports, substantial sums held in these CBI accounts were subsequently paid out for exports of goods to Iran, although the exports never took place.[158] In early 2014, eight foreign nationals (seven from Iran and one from Azerbaijan) entered India on student visas and set up to 80 fake companies. These shell companies presented invoices and received advance payments against the future exports. Sums of at least USD 150 million (rupee equivalent) were received by the shell companies from the CBI accounts at UCO Bank and then transferred to certain entities in Hong Kong, Dubai and Iran (figure 57). Under the rules, advances for exports should have been covered within a year by proof that an actual export was made.

According to media reporting, investigations of accounts of some of the shell companies showed that when advance payments for future exports were received into these accounts they were immediately transferred (see Table 7).[159]

[156] Times of India 25 January 2013.

[157] The Iranian banks were Bank Parsian, Saman Bank, Pasargad bank and EN Bank Tejinder Narang: Rupee payments snags in Indo-Iran trade, The Hindu Business Line, 13 November 2012 (http://www.thehindubusinessline.com/opinion/rupee-payment-snags-in-indoiratrade/article4093384.ece).

[158] Nidhi Verma and Devidutta Tripathy, "RBI tightens compliance after suspected Iran export scam", Reuters, 10 February 2015.

[159] Indo-Iran UCO Bank Scam: CBI registers PE against unknown RBI officials, UCO Bank officials, Virendrasingh Ghunawat, India Today, 21 May 2016. The preliminary enquiry also named officials from UCO Bank and the Reserve Bank of India.

Table 7: Shell companies' accounts at a branch of UCO Bank: Sums credited and debited on the same day

Name of Company	Credited Amount (USD)	Debited Amount (USD)	Date
True Export Services Pvt Ltd[160]	79.0m	79.0m	26 Sep 2013
A&H General Exports Trades Ltd	63.2m	63.2m	25 Sep 2013
Star Elite Export Trading Pvt Ltd	33.0m	33.0m	5 Dec 2013
New Age Export Services Pvt Ltd	4.2m	4.2m	5 Dec 2013
Connect Traders Pvt Ltd	4.5m	4.5m	4 Dec 2013
Elite World General Trading Pvt Ltd	0.2m	0.2m	2 Jul 2013
Genius Exports Pvt Ltd	1.3m	1.2m	4 Dec 2013
Centroid Exporters Pvt Ltd	5.3m	5.3m	4 Dec 2013

The Central Bank of India subsequently issued a notice that when banks provide advances to companies for exports, they should check that the exports actually take place.[161]

The end-users of the misappropriated funds have not been identified and two of these suspected shell companies, True Export Services Pvt Ltd and Star Elite Export Trading Pvt Ltd were also involved in transactions with companies separately under investigation by Indian authorities for a hawala scam.[162]

However, as with the case of misappropriated CBI accounts held in banks in the RoK, the countries to where the funds were sent feature in many of the case studies in this report, and it is possible that some at least of the funds were used for FoP purposes.

[160] According to commercial databases, True Export Services Private Limited was set up on 13 August, and currently has two active Directors, Mirtagi Hadiyev and Nizami Azimov, both appointed on 5 September 2013 (http://corporatedir.com/company/true-export-services-private-limited).

[161] "Delay in utilization of advance received for exports", Reserve Bank of India Notice 74, 9 February 2015.

[162] Indo-Iran UCO Bank Scam: CBI registers PE against unknown RBI officials, UCO Bank officials, Virendrasingh Ghunawat, India Today, 21 May 2016.

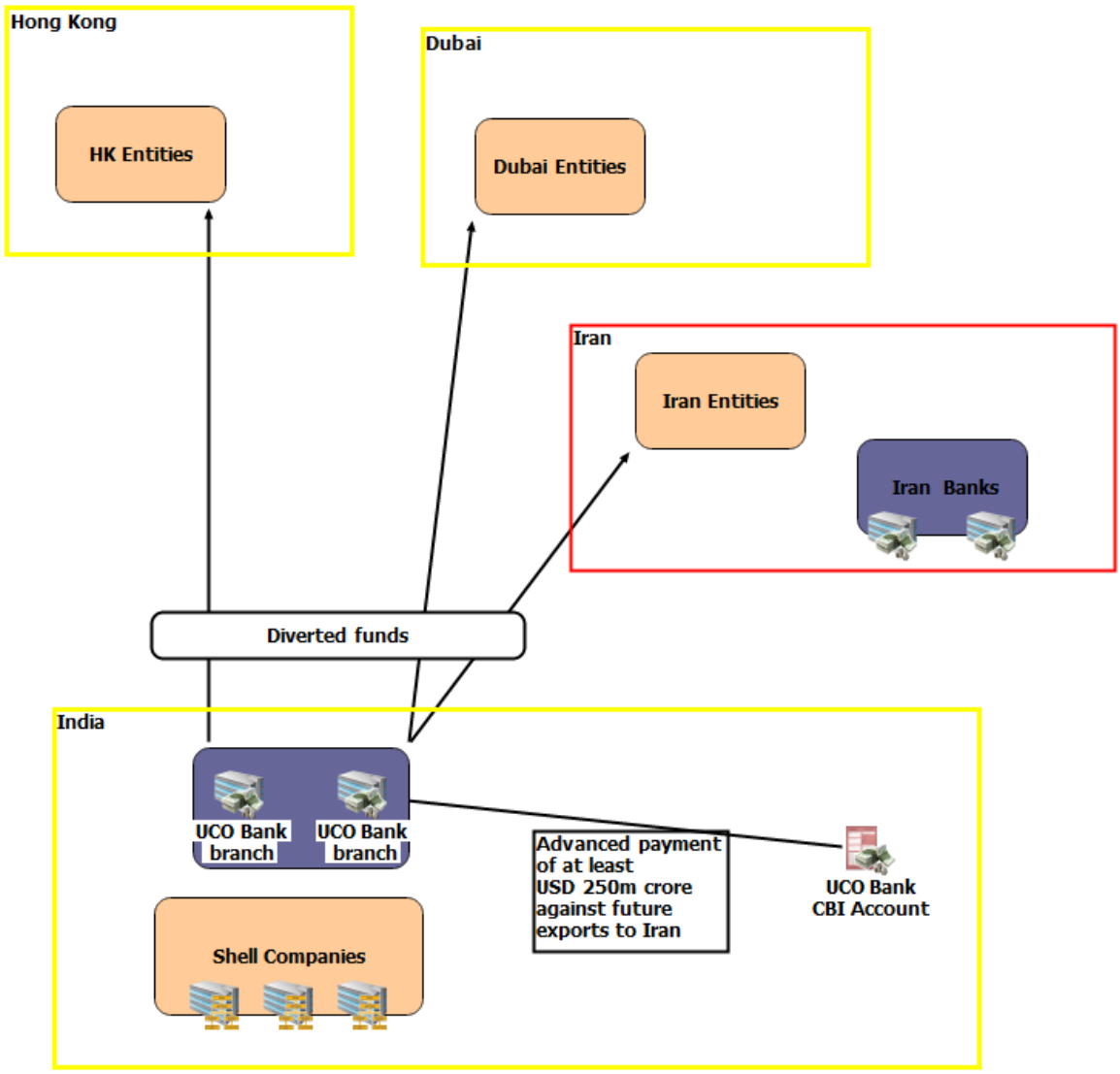


Figure 57. Funds belonging to the Central Bank of Iran at UCO Bank in India are misappropriated and sent overseas

Key Points

- The end-users of the misappropriated funds are not known. Many of the countries in the list above feature in the other case studies in this report, and it is possible that some misappropriated funds were used for financing proliferation.

Case 58: Iranian businessman overseas received income from business in Iran (probably 2012-2013)[163]

An Iranian businessman set up a business in Iran selling goods domestically and abroad.[164] He moved abroad, but continued to own his business in Iran and he received income from it.

The businessman received the income in the form of wire transactions originating from small financial institutions located in neighboring States. The accounts in the financial institutions from which the wires originated were affiliated with companies located outside Iran (figure 59).

It is not known exactly how value was transferred between the business in Iran and the companies outside Iran. It was possible that hawala methods were used.

[163] This case was Case No 15 in the Interim Report published 5 February 2017.
[164] Annex V of UN Panel on Iran Final Report 2014 (S/2014/394).

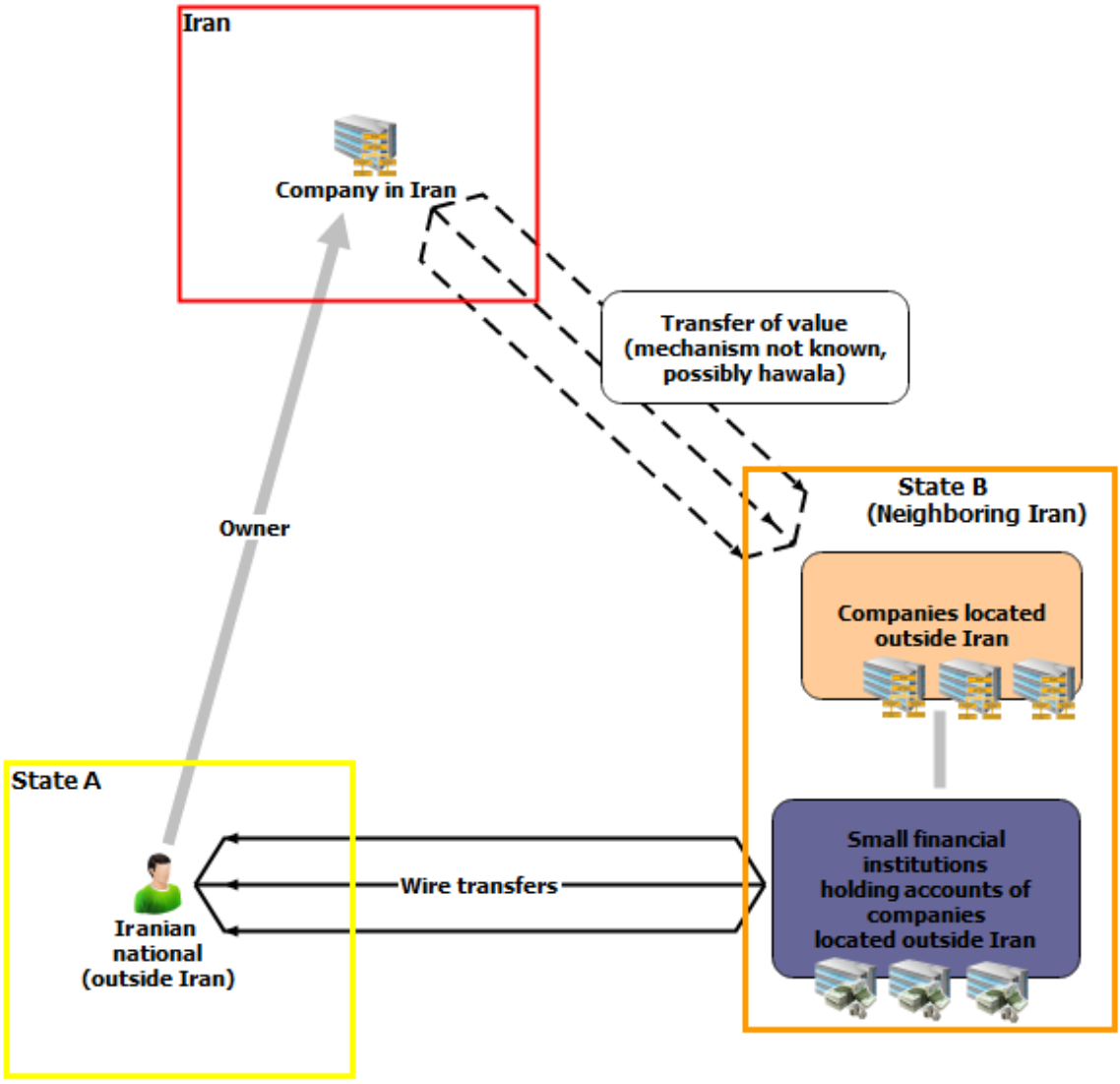


Figure 58. Iranian businessman based outside Iran received income from his Iranian-based company

Key Points

- The businessman presumably set up this elaborate scheme in order to circumvent financial sanctions on Iran;
- The scheme was based on transferring funds from Iran to companies located in a variety of states. Presumably this was done in order to spread risk;
- Detecting the Iranian origin of the funds would have been difficult for the financial institutions chosen to receive wire transfers intended for the businessman;
- It is not known whether the businessman was involved in FoP, but the mechanism set up to circumvent financial sanctions could have been put to this use.

Circumvention of Non-WMD-related Financial Sanctions

Case 59: Potential circumvention of sanctions relating to Crimea (2014-2017)

The following is based on information provided by a multinational bank, Bank A.

A customer of Bank A undertook trades with a Panama based firm, which the Bank suspected was acting as an intermediary for a Crimean based manufacturer of chemicals[165] in order to circumvent EU and OFAC sanctions on Crimea.

A new product request prompted a review and a subsequent investigation of the customer's transactions and KYC information to understand the Financial Crime risks. The investigation utilized ship tracking tools which proved suspicions that the ship involved in the customer's activity was loaded with cargo in Crimea (Figure 59). These tools were assessed to understand how they could be used to enhance Finance Crime controls.

A further consideration identified during the investigation was the screening of International Maritime Organisation (IMO) numbers. IMO numbers identify the ship regardless of name or flag changes.

[165] The chemicals were not themselves WMD-related.

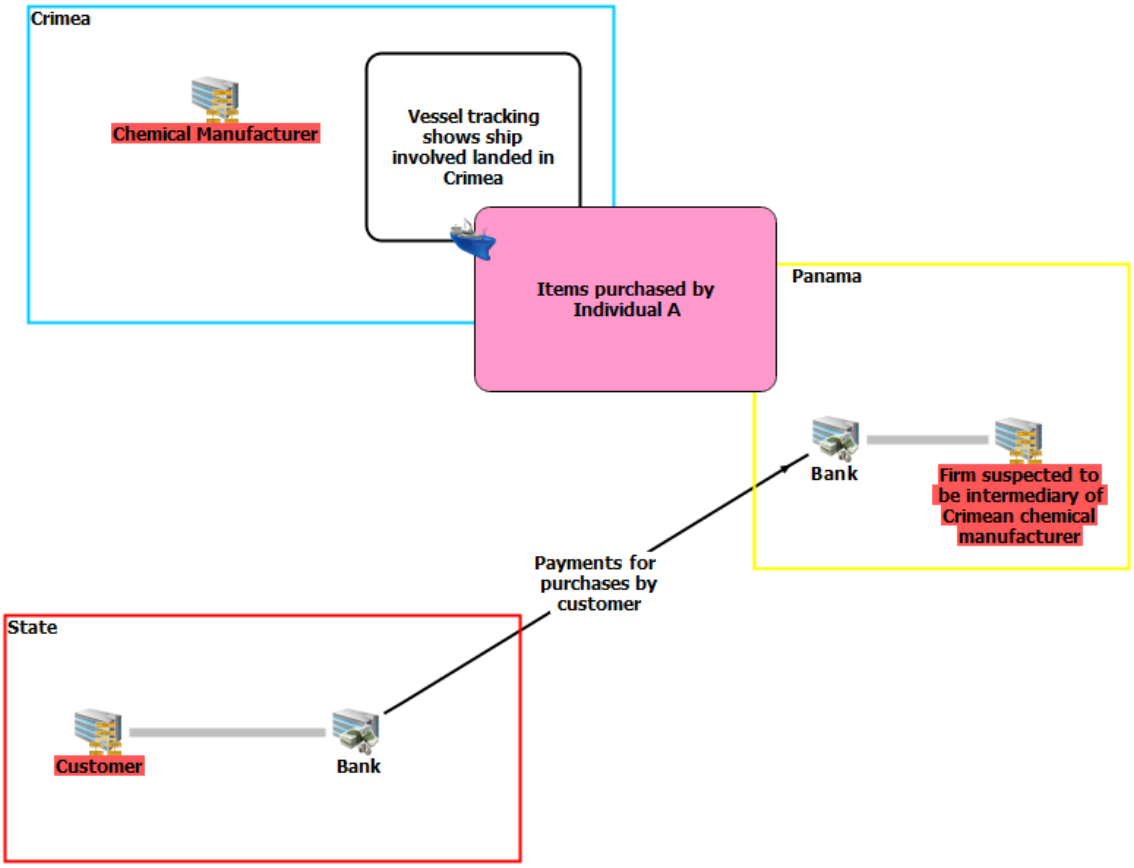


Figure 59. Company in the Crimea operates through an intermediary in Panama

The Bank's key takeaway: IMO data are useful in helping to identify Financial Crime red flags where the IMO number is falsified on trade documents, together with the use of vessel tracking data.

Case 60: Potential circumvention of sanctions relating to Sudan (2017)

The following is based on information provided by an international financial institution.

In August 2017, one of the financial institution's clients requested to remit a sum to a factory in China as payment for buying about 5,000 helmets. In the payment message, the destination of the shipment of goods was not stated. As helmets are an item listed within the Munitions List of the Strategic Commodities Control List of the Trade and Industry Department of the Hong Kong Special Administrative Region Government, our bank asked for a copy of the invoice to assist AML/CFT evaluation.

It transpired that the goods stated in the invoice were steel helmets to be shipped from China to Sudan, which is a sanctioned country. Moreover, the ultimate buyer and the end use of such steel helmets were not indicated in the invoice. Nonetheless, shipping instructions marked on the invoice suggested that the ultimate buyer of the goods was an enterprise in Sudan with a sub-branch that focuses on manufacturing military clothing. Given the uncertainties of the ultimate buyer of this shipment and that the goods themselves can be used for military purpose, the financial institution rejected to proceed with this transaction.

www.projectalpha.eu