PAPUA NEW GUINEA

SANCTIONS SECRETARIAT

(In collaboration with the Financial Analysis and Supervision Unit and Department of Justice & Attorney-General)

GUIDELINES FOR DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONALS

ON THE IMPLEMENTATION OF TARGETED FINANCIAL SANCTIONS UNDER THE UNITED NATIONS FINANCIAL SANCTIONS ACT 2015

(Disclaimer: This guide summarises publicly available information from the UN sanctions committees and the PNG Sanctions Secretariat. It is not legal advice.)

Table of Contents

I. INTRODUCTION

1.1 PURPOSE AND OBJECTIVE

These guidelines have been developed by the Sanctions Secretariat of Papua New Guinea in collaboration with the Financial Analysis and Supervision Unit (FASU) and Department of Justice & Attorney-General (DJAG) and with assistance from the Asian Development Bank (ADB) as a reference source to assist designated non-financial businesses and professionals (DNFBPs) in complying with the requirements of the United Nations Financial Sanctions Act 2015 (UNFSA). The purpose is to protect the public, and the financial system of Papua New Guinea, by helping to ensure that DNFBPs are not utilized, whether purposely or unwittingly, for terrorist financing (TF) or financing of weapons of mass destruction (WMDs), referred to here as "proliferation financing" (PF).

1.2 WHY ARE FINANCIAL SANCTIONS NECESSARY IN PNG?

Terrorist Financing

Although currently TF risk in PNG is considered to be low, this situation could change rapidly. Unless the issue is kept under very active review, there is a real danger that PNG could become a conduit to channel or store funds that could be used for carrying out terrorist acts. Given the very small amounts of money needed to fund terrorist activities, these may well escape detection. The emerging informal value transfer operations in PNG also provide a significant risk that need to be better understood and scrutinised by the FASU, the Royal Papua New Guinea Constabulary (RPNGC) and the banks which might be used to move larger amounts to offset transactions.[1] There is therefore good reason for DNFBPs to be diligent in instituting measures to counteract these undesirable circumstances.

Proliferation Financing

Similarly, PNG's current exposure to WMD-related sanctions evasion of PF is relatively moderate.[2] However, there is good reason for DNFBPs to be diligent in their efforts to combat PF, just as with TF. While WMDs may be quite sophisticated (such as a long-range missile system), they can also be as simple as a crude home-made explosive device. Detection and prevention of PF can be particularly difficult because the materials, parts, equipment, technology, or expertise used in WMD production may also have legitimate uses.

1.3 WHAT ARE FINANCIAL SANCTIONS?

Under sections 14 and 15 of the UNFSA, sanctions are prohibitions on any person:

- dealing with assets belonging to or owned, held or controlled (directly or indirectly) by a "designated person or entity" (DPE) ("asset freezes"); and

[1] National Risk Assessment, pp. 22-25, 131.
[2] 2024 MER, p. 9, par. 23 and Chapter 4, *Terrorist Financing and Financing of Proliferation*, Key Findings, Section 10.11, p. 77.

- making assets or financial services available directly or indirectly to, or for the benefit of, a DPE.

These sections of the UNFSA implement specific resolutions of the United Nations Security Council (UNSC)[3] and Recommendations 6 and 7 of the Financial Action Task Force (FATF), which are aimed at countering TF and PF.

Links to the UNSC sanctions lists, as well as the "Consolidated List" maintained by the PNG Sanctions Secretariat, are provided below:

List	Direct link
DPRK (1718 Committee) Sanctions List	https://main.un.org/securitycouncil/en/sanctions/1718/materials main.un.org
ISIL (Da'esh) & Al-Qaida (1267/1989 Committee) Sanctions List	https://main.un.org/securitycouncil/en/sanctions/1267 main.un.org
Taliban (1988 Committee) Sanctions List	https://main.un.org/securitycouncil/en/sanctions/1988 main.un.org
Iran – Annex B to UNSCR 2231	https://main.un.org/securitycouncil/en/content/2231/list main.un.org
PNG Consolidated List & local guidance	https://pngsanctionssecretariat.gov.pg/ (see "Consolidated List" tab) pngsanctionssecretariat.gov.pg

1.4 Overview of the Legislative Framework For Sanctions in PNG

The legislative framework regarding financial sanctions in PNG consists of:

- the Criminal Code Act 1974 (Criminal Code Act), as amended by the Criminal Code (Money Laundering and Terrorist Financing) (Amendment) Act 2015 (the Criminal Code Amendment Act);
- the UNFSA; and
- the Anti-Money Laundering and Counter Terrorist Financing Act 2015 (AML/CTF Act).

The Criminal Code Act

The Criminal Code Amendment Act introduced comprehensive and effective criminal law provisions to create a comprehensive offence for TF in the Criminal Code Act 1974. Per the 2015 amendments, Section 508J of the Criminal Code Act ("Terrorist Financing") makes it a crime for a person, by any means, to directly or indirectly provide or collect property with the

[3] These UNSC Resolutions are listed in Schedules 1 and 2 of the UNFSA. Schedule 1 includes: Resolutions on Al-Qaida (Resolutions 1267/1989 and successor resolutions); Resolutions on the Taliban (Resolution 1988 and successor resolutions); Resolutions on Democratic People's Republic of Korea (DPRK) (Resolution 1718 and successor resolutions); and Resolutions on Iran (Resolution 1737 and successor resolutions). Schedule 2 refers to Resolution 1373 on the suppression of terrorism and successor resolutions.

intention or knowledge that it be used to finance a terrorist act, a terrorist (without lawful justification) or a terrorist organisation. Such action is an offence under Section 508J:

- even if a terrorist act does not occur or is not attempted;
- even if the property was not actually used to commit or attempt to commit a terrorist act, or linked to a specific terrorist act;
- regardless of whether the property was from a legitimate or illegitimate source;
- regardless of the country in which the terrorist or terrorist organization is located; and
- regardless of the country in which the terrorist act has occurred or is intended to occur.

"Property" is broadly defined. Per Section 508I of the Criminal Code Act, property means:

> "assets of every kind, whether tangible or intangible, corporeal or incorporeal, moveable or immovable, however acquired, including an enforceable right of action, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including but not limited to currency, bank credits, deposits and other financial resources, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit, whether situated in Papua New Guinea or elsewhere, and includes a legal or equitable interest, whether full or partial, in any such assets."

Section 508I of the Criminal Code Act provides for the definition of key aspects of TF such as "terrorist," "terrorist act," and "terrorist organisation." These key definitions are also applied in the UNFSA specifically for the designation process described below. Per Section 508I of the Criminal Code Act, a "terrorist" means any natural person who:

- commits, enables, aids, counsels or procures a terrorist act;
- attempts to commit a terrorist act; or
- conspires to commit (whether directly or indirectly) a terrorist act.

A "terrorist organization" means a group of persons or a body corporate that:

- commits, enables, aids, counsels or procures a terrorist act;
- attempts to commit a terrorist act; or
- conspires to commit (whether directly or indirectly) a terrorist act.

Per Section 508I of the Criminal Code Act, there are two types of terrorist acts:

- an act which is an offence under any of the following treaties:
  - the Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970;

- the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971;
- the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973;
- the International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979;
- the Convention on the Physical Protection of Nuclear Material, adopted at Vienna on 3 March 1980; and
- the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988;
- the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10 March 1988;
- the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on 10 March 1988;
- the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997;

- any other act or threat of action that:
  - involves serious violence against a person not taking an active part in hostilities in a situation of armed conflict;
  - involves serious damage to property;
  - endangers another person's life;
  - creates a serious risk to the health or safety of the public or a section of the public; or
  - is designed to seriously interfere with or to seriously disrupt an electronic system;

  and
  - is designed to influence a government, or international organisation or to intimidate the public or a section of the public; or
  - is made for the purpose of advancing a political, religious or ideological cause.

The UNFSA

Section 14 of the UNFSA prohibits DNFBPs from:

- dealing with an asset knowing that the asset is owned, controlled or held, directly or indirectly, wholly or jointly, by or on behalf of or at the direction of a DPE;

- dealing with an asset reckless as to whether the asset is owned, controlled or held, directly or indirectly, wholly or jointly, by or on behalf of or at the direction of a DPE.

Section 15 of the UNFSA prohibits DNFBPs from:

- making an asset or financial service available knowing that it is being made available, directly or indirectly, wholly or jointly, to a DPE or a person or entity owned or controlled by, or acting on behalf of, a DPE;

- making an asset or financial service available to any person knowing that the asset or financial service is for the benefit of a DPE;

- making an asset or financial service available reckless as to whether it is being made available, directly or indirectly, wholly or jointly, to a DPE or a person or entity owned or controlled, or acting on behalf of a DPE; or

- making an asset or financial service available to any person reckless as to whether the asset or financial service is for the benefit of a DPE.

The AML/CFT Act

Under section 40 of the AML/CTF Act, a DNFBP must report to FASU any assets which it holds of a DPE. The report must be made as soon as is reasonably practicable or within 10 working days from the date notification of a designation is received.

Part 2 below explains the sanctions process under the UNFSA and AML/CFT Act in more detail.

1.5 WHY IS A FINANCIAL SANCTIONS REGIME IMPORTANT FOR PNG?

A key feature of TF and PF is that they have no boundaries. Terrorists and WMD financiers are always looking for gaps across jurisdictions to find safe havens for illicit assets. It is important for PNG, and other countries in the region, to ensure that their laws are robust and comprehensive, to close any potential gaps that terrorists and financiers of WMDs can exploit.

1.6 CHALLENGES FOR DNFBPS: UNDERSTANDING SANCTIONS EVASION

DPEs will rarely – if ever – show up in a transaction but will instead utilize well-rehearsed tricks to conceal who they are and where the money or goods are going. It is therefore crucial that DNFBPs consider how DPEs may indirectly attempt to gain access to funds or financial services. Common sanctions evasion techniques used by DPEs include:

Evasion tactic	What it looks like in real life
1. Fake or "front" companies	A new firm with no track record, often registered overseas, suddenly orders high-value goods or opens accounts.
2. "Straw" customers or clients	A person who purports to be acting on his/her own behalf, but is in fact acting on behalf of an undisclosed DPE. Such customers may be unfamiliar with the business they claim to represent, or with the transaction they are undertaking.
3. Non-transparent ownership structures	A company that is part of a corporate group whose ownership or control structure is extremely convoluted or confusing for no apparent business or economic reason.
4. False information	The use of aliases and/or falsified documentation to hide involvement of a DPE.
5. Doing business in high-risk jurisdictions	Customers/clients who are located or do significant business in high-risk jurisdictions (i.e., jurisdictions known to be locations for terrorist activity, public corruption, or financial crime).
6. Suspicious shipping moves	Ships that switch off their trackers, change names or flags mid-voyage, or transfer cargo at sea so paperwork shows the wrong port or owner.
7. Mislabelled trade paperwork	Invoices that under-price, use incorrect HS codes, or claim the buyer is in a low-risk country, even though the goods ultimately end up in the DPRK or Iran.
8. Money moved in small pieces	Dozens of low-value transfers through different banks or money-transfer agents ("smurfs") to keep each payment below monitoring thresholds.
9. Cryptocurrency detours	Funds converted to Bitcoin or privacy coins, sent through mixing services, then cashed out on an exchange with weak controls.
10. "Charity" or NGO cover	A non-profit organisation raises donations supposedly for "humanitarian aid" but quietly sends the cash or dual-use items to a sanctioned group.
11. Help from professional enablers	Lawyers, accountants or company-service providers who set up the structures, open accounts, or re-flag ships for a hidden client.

1.7 WHY DO DNFBPS NEED TO BE CONCERNED ABOUT SANCTIONS COMPLIANCE?

Apart from the obvious need to comply with the AML/CFT Act and the UNFSA, there are many reasons that DNFBPs need to ensure that they have strong sanctions compliance programs. Terrorists and proliferation financiers are always looking for ways to fund their activities, and their efforts are not limited to traditional financial institutions (FIs). Experience around the world teaches that DNFBPs have – whether wittingly or unwittingly – helped to develop elaborate schemes to facilitate sanctions evasion; DNFPBs need to be vigilant to ensure that they do not inadvertently fall into such behaviour.

DNFBPs are vulnerable to penetration by terrorist financiers and proliferation financiers in a number of ways. Sometimes the involvement may be direct, such as by actually handling DPE-controlled assets. In other cases, the DNFBP's involvement may be indirect, such as through facilitating the transfer or conversion of assets by a DPE. Either of these scenarios can lead to liability under Section 508J(1) and (3) of Criminal Code Act, which provides for the offence of TF irrespective of whether it was done directly or indirectly, and regardless of whether the financing comes from a legal or illegal source. The DNFBP may also be found to have aided or enabled the actual DPE in committing the offence under Section 7(1)(b) or (c) of the Criminal Code Act. Some examples follow.

Legal professionals[4]

Legal services are particularly vulnerable to being misused to facilitate TF and PF. Terrorists and WMD financiers (or those "front persons" acting at their behest) may seek legal services to lend the appearance of legitimacy to their TF or PF transactions. There are three main ways that this can come about:

- Lawyers – particularly those with transnational practices – handle client money in many jurisdictions, which entails transferring funds between parties and even between these jurisdictions. This raises the possibility that a lawyer may become involved in transmitting DPE-controlled money by simply putting it into a client account, thereby running afoul of the prohibition of Section 14 of the UNFSA on dealing with DPE-related assets.

- Many of the services that lawyers provide, such as setting up companies and trusts, or carrying out real estate conveyancing transactions, are methods that can be used to facilitate TF or PF. A lawyer who provides such services for or on behalf of a DPE could be considered to have violated the prohibition of Section 15 of the UNFSA on providing financial services to a DPE, as these functions often entail legal advice on issuance of securities and/or management of assets.

- Even routine matters such as entering into general commercial contracts – big and small – for and on behalf of clients is also one of the principal services that lawyers carry out, with the classic contractual arrangement being a retainer between the lawyer and the client. If the client is a DPE, the lawyer risks running afoul of Sections 14 or 15 of the UNFSA.

- Engaging a lawyer adds respectability and an appearance of legitimacy to any activities being undertaken. Terrorists and WMD financiers who wish to make their activities appear legitimate will often seek the involvement of a lawyer as a "stamp of approval" for certain activities. For example, often a lawyer's involvement with a company may consist of performing a role within that company, such as serving as a director, general counsel or the corporate secretary, or providing services as a company representative. If the company is a DPE, or controlled a DPE, the lawyer could be deemed to have participated in, or facilitated, dealing with tainted assets in violation of Section 14 of the UNFSA, as the company will undoubtedly transfer assets at some point.

Accountants

Accounting is a core component of the broader financial services industry. It entails recording, analysis and reporting of financial information. Accounting services can include preparing financial statements, managing accounts payable and receivable, and providing tax preparation and planning services. Businesspersons often seek the advice of accountants; persons who are trying to evade financial sanctions may attempt to conceal the origin of funds

[4] Anna Bradshaw and Alistair Jones, *The Guide to Sanctions – Fifth Edition: A UK Lawyer's Perspective on Representing Designated Persons,* https://globalinvestigationsreview.com/guide/the-guide-sanctions/fifth-edition/article/uk-lawyers-perspective-representing-designated-persons;
FINTRAC (Canada), *Special Bulletin on the use of the legal profession in money laundering and sanctions evasion,* https://fintrac-canafe.canada.ca/intel/bulletins/legal-juridique-eng.pdf.

and assets by various means, such as offshore accounts, shell companies and moving money through multiple jurisdictions. The intent is to lose track of the funds and reintegrate them into the economy, often by buying real estate, luxury boats and businesses.[5] Accountants run many of the same risks in this area as lawyers. Indeed, they often work closely with lawyers in providing client services. It therefore behooves accountants to become familiar with the examples noted above regarding legal professionals.

Real estate professionals[6]

Persons who wish to evade financial sanctions often invest in real estate as convenient way to disguise their activities. Consequently, real estate professionals need to be aware of techniques that these persons use to accomplish this. Some of the most common ways are:

- *Buying property with cash.* This is the easiest and most common way of using real estate to conceal ownership and control of property. Using cash avoids the creation of an audit trail such as would be present if property were purchased through a bank or other financial institution and required mortgage-related paperwork, financial analysis of the purchaser, and so forth.

- *Use of "shell companies" and trusts.* DPEs often use shell companies (companies that exist only "on paper" but in fact conduct no business) and trusts in order to conceal their ownership stake in property. Particularly with high-value properties, many layers of legal entities and trusts may be involved, and they may be spread across multiple jurisdictions. These features can make it difficult for DNFBPs to identify the beneficial owners of these entities. Even legitimate businesses (*e.g.*, real estate development or asset management companies) may, even if unwittingly, be part of property ownership structures involved in a sanctions evasion scheme, creating additional challenges in identifying the bad actors.

- *Successive selling ("flipping").* Selling a piece of property many times within a relatively short period of time in order to confuse the audit trail.

Real estate professionals who provide services to DPEs, DPE-controlled entities or persons acting the behest of DPEs risk prosecution by dealing with DPE-related assets (e.g., receiving and transmitting down payments or earnest money deposits) or facilitating the transfer of an asset (e.g., the real estate property itself) in violation of Section 14 of the UNFSA, including by aiding or enabling such transfers under Section 7(1)(b) or (c) of the Criminal Code.

Precious Metal and Stone Dealers

All U.N. Member States are prohibited by UNSC Resolutions from providing certain services, including export of bulk cash and gold, that could contribute to the DPRK's prohibited programs or activities, or to the evasion of sanctions. Further, the DPRK is prohibited from

[5] CPA Canada, *Why CPAs Need to Watch Out for Sanctions Evasion,* *https://www.cpacanada.ca/news/accounting/the-profession/2022-05-04-russian-ties*

[6] U.S. Financial Crime Enforcement Network (FinCEN) *Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies* (2023), https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Real%20Estate%20FINAL%20508_1-25-23%20FINAL%20FINAL.pdf.

supplying, selling, or transferring certain metals, including gold and silver, and U.N. Member States are prohibited from procuring such metals from the DPRK.

The DPRK has been known to employ various methods to circumvent sanctions involving the import or export of prohibited goods, including gold. Indeed, North Korea's gold sanctions evasion network is complex and multifaceted, leveraging smuggling, diplomatic cover, and financial manipulation to generate revenue for the regime and its prohibited programs. These techniques include:[7]

- **Gold Smuggling**:
  - *Physical Smuggling*: North Korea engages in the physical smuggling of gold across borders, often utilizing land routes into China. Diplomats have also been caught attempting to smuggle gold through airports, exploiting their diplomatic immunity, although this tactic has faced increased scrutiny.
  - *Transit Hubs*: North Korea uses transit hubs in Southeast Asia and elsewhere to facilitate the illegal trade of gold and other sanctioned goods.
  - *Underground Market*: A network exists within North Korea where individuals mine and sell gold, which is then purchased by corrupt officials or individuals with connections to the regime. This gold is then resold at a significant markup, often in China, generating illicit funds for the North Korean government.
- **Misuse of Diplomatic Cover:**
  - *Diplomats as Smugglers*: North Korean diplomats have been implicated in smuggling gold and cash, using their diplomatic status and privileges to bypass customs and airport security.
  - *Embassy Operations*: North Korean embassies have been used as bases for illicit activities, including coordinating and facilitating the smuggling of gold and other prohibited items.
- **Exploitation of Financial Networks**:
  - *Shell Companies and Front Companies*: North Korea utilizes shell companies and front companies, often registered in other countries, to obscure the origin and destination of gold and other restricted materials and transactions.
  - *Bulk Cash and Gold*: When access to the formal financial system is restricted, North Korea resorts to using bulk cash and gold to circumvent the system entirely.

Gold transactions are particularly relevant for PNG. In 2023, PNG exported $1.85B of gold making it the 40th largest exporter of gold (out of 167) in the world. During the same year, gold

[7] Rand Corporation, *North Korean Sanctions Evasion Techniques* (2021). https://www.rand.org/pubs/research_reports/RRA1537-1.html#:~:text=North%20Korea%20engages%20in%20four,of%20civilians%20with%20chemical%20weapons.

was PNG's 2nd most exported product (out of 451).[8] FATF has identified the following factors that make gold particularly attractive to terrorists and money launderers:[9]

- It is easily smuggled and traded.
- It is a cash-intensive commodity.
- It can be traded anonymously.
- Investment in gold provides reliable returns.

Precious metal and stone dealers need to be aware of these factors in order to avoid falling into evasion schemes.

Trusts

Trusts can be attractive to those who seek to evade sanctions because they can be created without naming the people who own and control them. While most trusts are perfectly legitimate (they are often used for family estate planning purposes), this lack of transparency can make it easy to conceal the true purpose of the trust if aim is to conduct TF or PF. DNFPBs who help to create trusts, or who have trusts as clients, need to be sure that they know who the beneficial owners of these trusts are, and that the trusts have legitimate purposes.

Motor vehicle dealerships

DPEs often purchase and sell motor vehicles (MVs), particularly luxury cars. A common sanctions evasion technique involving MVs is the use of third countries as transit points. Vehicles may be shipped to the "intermediary" country and then re-exported to a sanctioned country, making it difficult to trace the origin and final destination of the vehicles. Businesses involved in MV sales or financing therefore need to be alert to red flags that could indicate that a customer may be involved in nefarious activity and attempting to utilize the dealer's business in furtherance of that activity. MV dealers can potentially become involved in sanctions evasion in a number of ways:

- MV dealers might unknowingly sell vehicles or parts to DPEs or persons or entities controlled by or acting at the behest of DPEs.
- DPEs might use shell companies or third-party intermediaries to conceal the true buyer or the ultimate destination of vehicles or parts.
- DPEs, or persons or entities controlled by or acting at the behest of DPEs, might provide false documents or other information MV dealers to conceal the true nature or destination of the vehicles they are purchasing.
- Dealers might provide services like maintenance, repairs, or financing to DPEs, persons or entities controlled by or acting at the behest of DPEs.

[8] Organization of Economic Complexity (OEC). 2025. *Gold in Papua New Guinea*. https://oec.world/en/profile/bilateral-product/gold/reporter/png
[9] FATF. July 2015. *Money Laundering / Terrorist Financing Risks and Vulnerabilities Associated with Gold.*

- Dealers could become involved in selling or facilitating the sale of dual-use goods (goods with both civilian and military applications) to DPEs or persons or entities controlled by or acting at the behest of DPEs.

2. OPERATION OF THE PNG FINANCIAL SANCTIONS REGIME

2.1 THE SANCTIONS SECRETARIAT

Section 25 of the UNFSA establishes the Sanctions Secretariat within the Department of Prime Minister and National Executive Council. As the secretariat to the National Security Advisory Committee, the Sanctions Secretariat has an integral role in the effective implementation of a successful financial sanctions regime in PNG. It performs a number of key functions, including:

- providing support to the National Security Advisory Committee and the Prime Minister in exercising designation powers;

- maintaining an up-to-date Consolidated List of DPEs, which consists of four UNSC Committee Sanctions Lists implementing the UNSC Resolutions listed in note 1 above on Al-Qaida, the Taliban, the DPRK and Iran;

- issuing public guidance to promote and assist compliance with PNG's financial sanctions legislation.

Other functions include:

- receiving proposed designations from agencies within PNG and from foreign agencies (including preparing internal recommendations for such designations);

- notifying financial institutions and DNFBPs (and others) of designations through the FASU;

- preparing guidelines and forms for use by FIs, DNFBPs and the public;

- receiving and responding to enquiries from the public and private sector about authorisations to deal with frozen asset of DPEs; and

- generally raising awareness about the risks and dangers of money laundering, TF and PF.

The Sanctions Secretariat's website contains valuable information for DNFBPs, including identification of DPEs and regular updates. The website is located at https://pngsanctionssecretariat.gov.pg.

2.2 DESIGNATED PERSON OR ENTITY STATUS

According to Section 5 of the UNFSA, a "designated person or entity" means a person or entity –

(a) designated by the Prime Minister or the court under the UNFSA; or

(b) designated by the United Nations Security Council or its Committees pursuant to Resolutions listed in Schedule 1 to the UNFSA or prescribed by Regulations made under Subsection 29(2) of the UNFSA.

The Prime Minister, through the Sanctions Secretariat and FASU, notifies FIs and DNFBPs of a designation, redesignation, revocation and expiry. The notifications are also published in the National Gazette.

Publication in the National Gazette is not required where the UNSC or its Committees make a designation or revocation in respect of a person located outside PNG.

The UNSC has made all DPE designations to date. There have been no domestic designations, and all UNSC-designated DPEs are located outside of PNG.

The UNSC designations have immediate application in PNG and the immediate effect of imposing the prohibitions in the UNFSA.

Upon UNSC designation / redesignation, FIs and DNFBPs must immediately cease dealing with an asset and cease to make available financial services where:

- the asset is held directly or indirectly, wholly or jointly by or on behalf of or at the direction of a DPE;

- the asset or financial service is made available directly or indirectly, wholly or jointly to a DPE or a person or entity owned or controlled or acting on behalf of a DPE; or

- the asset or financial service is for the benefit of a DPE.

Likewise, if a person's DPE status has been revoked, the prohibitions in the UNFSA cease to apply.

The above situation could change in the future, and DNFBPs should therefore keep informed as to any domestic designations that may be implemented under the UNFSA.

The current number of DPEs on each UN sanctions list is provided below:

Sanctions group	Individuals	Entities/undertakings	Total	Source & last update (June 2025)
DPRK (1718 Committee)	**80**	**75**	**155**	**UN 1718 list page, updated 17 Sep 2024 main.un.org**
ISIL (Da'esh) & Al-Qaida (1267/1989 Committee)	**253**	**89**	**342**	**UN 1267/1989 list page, updated 9 Jun 2025 main.un.org**
Taliban (1988 Committee)	**135**	**5**	**140**	**UN 1988 list page, updated 30 Jan 2019, main.un.org**
Iran – Annex B to UNSCR 2231	**23**	**61**	**84**	**main.un.org**

Penalties for failure to comply with these requirements are described in Section 2.7 below.

2.3 FREEZING OF ASSETS

Overview

Section 14 of the UNFSA prohibits DNFBPs from dealing with an asset knowing that the asset is owned, controlled or held, directly or indirectly, wholly or jointly, by or on behalf of or at the direction of a DPE. Such assets are defined by Section 5 of the UNFSA as "frozen assets."

Under Section 5 of the UNFSA, an "asset" is very broadly defined. It includes:

> *"funds, property and financial resources of every kind, whether tangible or intangible, corporeal or incorporeal, moveable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including but not limited to currency, bank credits, deposits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit and any interest, dividends, income or value accruing from, generated by or derived from such asset."*

"Dealing," when used in relation to an asset, includes the transfer, conversion, disposition, movement or use of that asset.

The prohibition on dealing with or providing assets or financial services to DPEs (or persons or entities controlled directly or indirectly by DPEs) must be implemented immediately upon identification of a person or entity as a DPE or controlling person, without prior notice to that person or entity. DNFBPs must not inform a customer, their BO(s) or authorised representative(s) that assets will be frozen or assets or financial services will not be provided prior to any taking any such action. This is important because not only is advising, warning or "tipping off" the affected customer itself an offence (which can result in significant penalties), but it can prompt the DPE to move assets out of reach.

Authorisation to Deal With Frozen Assets

Part III of the UNFSA sets out a process for enabling a person to seek authorisation to deal with frozen assets or make an asset or financial service available in certain circumstances. Section 17 of the UNFSA provides that a person may apply in writing to the Prime Minister for such an authorisation, and the Prime Minister may grant such an authorisation upon that application, or upon the Prime Minister's own instigation.

Such authorisations may only be given on certain conditions, namely that the asset is required to meet -

- *a basic expense* (defined in Section 5 of the UNFSA as obtaining foodstuffs; paying rent or mortgage; obtaining medicine or medical treatment; paying taxes; paying insurance premiums; paying public utility charges; paying reasonable professional fees; paying reasonable expenses associated with the provision of legal services; and paying fees or service charges in accordance with laws of PNG for the routine holding or maintenance of a frozen asset);

- *a contractual obligation* (defined in Section 5 of the UNFSA as an obligation whereby a payment is required under contracts or agreements made before the date of the designation and where the payment required does not defeat the object and purpose of the UNFSA); or

- *an extraordinary expense* (defined in Section 5 of the UNFSA as a payment which is not a basic expense or contractual obligation, that the Prime Minister considers necessary and that he considers does not defeat the object and purpose of the UNFSA).

The application must be accompanied by sufficient evidence to support the request and to demonstrate that the above criteria are satisfied. The Prime Minister may authorise the management, or administration of a frozen asset for purposes including, but not limited to, maintaining the value of the asset, but may not grant an authorisation where there are reasonable grounds to believe that the asset or financial service will be used for a purpose other than fulfilling the stated conditions. The Prime Minister may also impose other conditions on any authorisations granted.

Another key element of the authorisation process requires that prior to authorising any dealing with a frozen asset or the making available of an assets or financial service, the Prime Minister must-

- seek any approvals required by, and make any notifications required to, the UNSC or its Committees; and

- consider any communication from a foreign government relevant to the authorisation.

A person may also apply directly to the relevant UNSC Committee through a procedure described on the websites of the Sanctions Secretariat and the U.N. Security Council.[10]

[10] https://pngsanctionssecretariat.gov.pg/authorization/; https://main.un.org/securitycouncil/en/content/2231/assets-freeze-exemptions

2.4 REVOCATION

A DPE may be removed from the Sanctions Lists (Consolidated List) by the UNSC or one of its Committees, or by the Prime Minister or a PNG court. The Sanctions Secretariat's website noted above provides information regarding the revocation process (also known as "delisting").

Per Section 6 of the UNFSA, a Schedule 1 designation (see Note 1 above) can only be revoked by the UNSC or the relevant UNSC Committee that oversees the particular sanctions program in question. The Prime Minister may submit a request for revocation to the UNSC or its relevant Committee for their consideration and subsequent decision. A DPE can also apply directly to either the U.N.'s Office of the Ombudsperson or Focal Point,[11] depending on the Sanctions List(s) on which the DPE is included.

For Schedule 2 (domestic) designations (DPEs designated under UNSCR 1373), Section 11 of the UNFSA provides the procedures for de-listing (note that currently there are no domestic designations). The Prime Minister is required to periodically review all interim designations, final designations and Prime Ministerial and court re-designations to determine whether the grounds for the designation continue to be satisfied. Where the Prime Minister is of the view that such grounds are no longer satisfied, the Prime Minister, acting on the advice of the National Security Advisory Committee, is required to –

- in the case of an interim designation or Prime Ministerial re-designation, revoke the designation or re-designation; or

- in the case of a final designation or National Court re-designation, make an application to the National Court for it to revoke the designation or re-designation. If the National Court agrees that such grounds are no longer satisfied, it is required to revoke the designation.

The Prime Minister notifies FIs, DNFBPs, and any other necessary persons of any revocations.

2.5 ASSISTANCE FROM THE COMMISSIONER OF POLICE

At times, a DNFBP may suspect that it is holding an asset that is, or may be, owned, controlled or held on behalf of, or at the direction, of a DPE. In this event, Section 16 of the UNFSA provides a process whereby the DBFBP may seek the assistance of the Commissioner of Police in order to help verify that suspicion. The request must be accompanied by details of the asset and the owner or controller of the asset, if known to the person making the request. The Commissioner of Police is obligated use his best endeavours to assist in making that determination, including providing a written response as soon as is reasonably practicable after receiving the request.

[11] DPEs seeking to be removed from the UNSC's ISIL (Da'esh) and Al-Qaida Sanctions List can submit their request to an independent and impartial Ombudsperson who has been appointed by the U.N. Secretary-General. DPEs on the sanctions list of one of the UNSC sanctions committees, except for individuals inscribed on Al-Qaida Sanctions List can submit such requests either through the U.N.'s Focal Point, which is a mechanism established by the UNSC to facilitate delisting requests from UN sanctions lists, or through their State of residence or citizenship (in this case, PNG).

2.6 REPORTING OBLIGATIONS

Under section 40 of the AML/CTF Act, a DNFBP must report to FASU any assets which it holds of a DPE. The report must be made as soon as is reasonably practicable or within 10 working days from the date notification of a designation is received.

A DNFBP must also file a suspicious matter report (SMR) with the FASU without delay whenever it has reasonable grounds to suspect that:

- an asset, transaction or attempted transaction may breach sections 14-15 of the UNFSA (i.e., dealing with or providing assets/services to a DPE); or

- information in its possession may be relevant to detecting, investigating or prosecuting such a breach.

2.7 OFFENCES AND PENALTIES

PNG's sanctions regime will be far more effective if DNFBPs voluntarily comply with their obligations under the UNFSA and AML/CFT Act. This will assist in detecting, deterring and preventing terrorist and proliferation financing, which in turn will contribute to strengthening the safety and financial stability of PNG. However, Sections 14 and 15 of the UNFSA prescribe a broad range of enforcement measures and failure to comply with obligations under the UNFSA or AML/CFT Act will attract heavy penalties, which are summarised below:

Offence	Individual	Company
Dealing with frozen asset(s) (s 14)	≤ PGK 100 000 or 9 years imprisonment	≤ PGK 450,000 or asset value
Making assets available (s 15)	Same	Same
Reckless breach	≤ PGK 50 000 or 5 years imprisonment	≤ PGK 250,000 or asset value

3. ELEMENTS OF AN EFFECTIVE SANCTIONS COMPLIANCE PROGRAM

Because of the above factors, it is critical that each DNFBP establish and maintain an effective sanctions compliance program (SCP). Such a program will consist of the following elements:

- Management Commitment
- Risk assessment
- Internal controls
- Testing and auditing
- Training

3.1 MANAGEMENT COMMITMENT

Sanctions Compliance Program

Each DNFBP should have a SCP. The program should be tailored to the size and risk profile of the business. Most DNFBPs in PNG are small organisations, and many are sole practitioners. As such, their sanctions compliance programs (SCPs) are likely to be relatively simple.[12] In a small DNFBP, the SCP should be developed and approved by the persons who manage the business on a day-to-day basis. For a solo practitioner, that person will need to create the SCP. For most small businesses, the program does not need to be complicated or excessively detailed, but should contain the following elements:

- policies and procedures for identifying persons and entities that are subject to sanctions, reporting and transfer of information and documents to the responsible compliance officials within the DNFBP, and to the competent governmental authorities as appropriate;

- procedures for maintaining a current list of DPEs. The procedures should require that all new accounts be compared with the sanctions lists when accounts are opened. Established accounts should be checked regularly with the current and updated sanctions lists;

- provisions for training for all employees of the DNFBP whose job responsibilities entail contact with customers who may be subject to sanctions, or for reviewing and analysing information collected by the front-line employees;

- periodic assessment of the DNFBP's sanctions-related risk in relation to its customers, services and products;

- in some cases, independent testing of the effectiveness of the policies and procedures; and

- procedures in relation to enhanced due diligence (EDD) in case of higher risk customers.

Larger DNFBPs should appoint an official to oversee sanctions compliance, either on a stand-alone basis or as part of a broader AML/CFT/sanctions program; however, most DNFBPs in PNG will likely not fit into this category. In such cases the management body or practitioner will need to ensure that they understand the requirements of the UNFSA and how to comply with them.

Resources

The management body or practitioner should ensure that the business has adequate resources—including in the form of human capital, expertise, information technology, and other resources,

[12] Larger DNFBPs that have a board of directors and a full senior management team, may wish to consult the Sanctions Secretariat's guidance for financial institutions, which contains advice for larger and more complex organisations.

as appropriate—that are relative to the DNFBP's breadth of operations, target and secondary markets, and other factors affecting its overall risk profile.

3.2 SANCTIONS RISK ASSESSMENT

It is a good business practice for DNFBPs to conduct a "top-to-bottom" assessment of their sanctions risks, which will assist them in developing their sanctions programs. A good risk assessment should:

- be in writing (it can be stored electronically);
- identify and assess the nature and level of TF and PF risks that the DNFBP may reasonably expect to face in the course of its business; and
- be maintained and updated as required to take into account new and emerging risks.

Risks specific to sanctions compliance generally can be defined as *potential threats or vulnerabilities that, if ignored or not properly handled, can lead to violations of the UNFSA or related regulations, and negatively affect a DNFBP's reputation and business*. The main sources of these risks are:

- the DNFBP's customers, supply chain, intermediaries, and counter-parties;
- the products and services that the DNFBP offers, including how and where such items fit into other financial or commercial products, services, networks, or systems; and
- the geographic locations of the DNFBP, as well as of its customers, supply chain, intermediaries, and counter-parties.

Some of the key focus items that a DNFBP should consider include:

- **Direct exposure to DPEs.** This is the most obvious risk, and it is what most people think of when they hear the term "sanctions risk."
- **Indirect exposure to DPEs.** This can occur through a variety of channels, such as doing business with a company that is owned or controlled by a DPE, and is particularly problematic in cases where DPEs attempt to hide their involvement in transactions or business relationships in order to evade sanctions.
- **Failure to properly screen customers and transactions.** This can lead to inadvertent violations of sanctions, even if the DNFBP is not directly exposed to DPEs.
- **Inadequate training for employees.** Employees who are not properly trained on sanctions compliance are more likely to miss situations that could lead to violations of the UNSCA and related regulations.

While there is no "one-size-fits all" formula for a risk assessment, the exercise should generally consist of a holistic review of the DNFBP's operations and assess its touchpoints to the outside

world. This process allows the DNFBP to identify potential areas in which it may, directly or indirectly, engage with DPEs.

A good risk assessment will:

- identify the degree of risk to which the business is exposed, taking into account its customers (who they are, where they are from and the nature of their business), the geographic locations in which the business and its customers operate, its delivery methods (e.g., face-to-face; via internet, or through agents or intermediaries);

- determine what controls the business has instituted to mitigate those risks, and whether the controls are working as intended; and

- come up with an overall, "net" risk rating that considers the amount of risk in the business and how well the control techniques are handling each risk area.

Each DNFBP will need to design its own risk assessment based on its particular circumstances. A suggested risk assessment framework for a small DNFBP is presented in **Appendix 1**.

3.3 INTERNAL CONTROLS

An effective set of internal controls will contain the following elements:

- **Written policies and procedures outlining the SCP.** These policies and procedures should be relevant to the DNFBP, capture the its day-to-day operations and procedures, be easy to follow, and be designed to prevent employees from engaging in misconduct. In a small business, the policies and procedures are likely to be relatively simple; however, it is essential to maintain a written outline of how the business will go about complying with the requirements of the UNFSA.

  Lawyers will need to pay particular attention to the issue of client-lawyer confidentiality, which is a key element of services rendered by lawyers. Exceptions to the client lawyer confidentiality are addressed in Section 9 of the *Professional Conduct Rules*, which is aligned with compliance of the UNFSA. In terms of TF and PF sanctions, the exception under Section 9 can be captured within the standard retainer as part of its standard retainer/contract with its clients (which would include DPEs).

- **Effective implementation of the internal controls.** This should adequately address the results of the DNFBP's risk assessment and profile. The internal controls should enable the DNFBP to clearly and effectively identify, interdict, escalate, and report to appropriate personnel within the DNFBP any transactions or activity that may be prohibited by the UNFSA or related regulations. To the extent that information technology solutions form part of the DNFBP's internal controls, the DNFBP should ensure that it has selected and calibrated the solutions in a manner that is appropriate to address its risk profile and compliance needs. The DNFBP should routinely test the solutions to ensure effectiveness.

- **Appointment of personnel responsible for integrating the policies and procedures into the daily operations of the DNFBP.** This process entails consultations with relevant business units, and ensuring that the DNFBP's employees understand the policies and procedures. In a small business, and particularly for a sole practitioner, this task will not be very complicated; each client-serving employee (or the proprietor) will simply need to understand the requirements of the UNFSA and related regulations, and how to comply with them.

- **Enforcement of the policies and procedures** through an effective compliance function headed by the designated sanctions compliance officer (SCO), as well as internal and/or external audits.

- **Recordkeeping policies and procedures** to document adherence to the requirements of the UNFSA and related regulations.

- **Clear communication** of the policies and procedures to all relevant staff, including personnel within the SCP program, as well as relevant gatekeepers and business units operating in high-risk areas (e.g., customer acquisition, payments, sales, etc.) and to external parties performing SCP responsibilities on behalf of the DNFBP.

- **Corrective action** upon learning of any weaknesses in the internal controls, to identify the root cause of the weakness institute remedial action.

The following sections highlight some of the most critical internal control mechanisms.

Customer Due Diligence and Screening Procedures

The cornerstone of a strong SCP is the ability of a DNFBP to *know its customers,* in order to be satisfied that a customer (or potential customer) is not a DPE, or associated in any way with a DPE. The AML/CFT Act sets out the CDD obligations in Part II, Division 2 (Sections 15 to 29). Specifically:

- Subdivision 1 – General due diligence requirements (Sections 15 to 19);

- Subdivision 2 – Customer due diligence requirements (Sections 20 to 29); and

- Subdivision 5 – Offences (Sections 36 to 38).

These obligations apply to DNFBPs in the circumstances set out in Section 52 of the AML/CFT Act.

Section 8 of the FASU AML/CFT Guidance for DNFBPs elaborates on this topic in the AML/CFT context; however, there are steps that should be taken *in addition to baseline customer due diligence (CDD) procedures and other anti-money laundering (AML) controls* which can be critical for detecting, stopping, and reporting attempted or suspected sanctions evasion. These additional steps involve *screening*.

Screening refers the comparison of one string of text against another to detect similarities that would suggest a potential match. If a match is detected, and the DNFBP maintains accounts,

or otherwise holds or controls funds and other assets for DPEs (or any entity owned or controlled by DPEs, or acting on their behalf of for their benefit), DNFBPs should immediately:

- not deal with those funds and other assets, per Section 14 of the UNFSA;
- not make funds and other assets available to or for the benefit of DPEs, per Section 15 of the UNFSA;
- report the situation to the FASU as required by Section 40 of the AML/CFT Act; and
- if the situation warrants, investigate further as detailed below.

DNFBPs will typically utilize two main screening techniques:

- customer/name screening to identify DPEs during onboarding and also at other crucial stages of the customer relationship; and
- transaction screening, which seeks to identify transactions that involve DPEs.

Many businesses use sanctions screening software that is available from commercial vendors. The type and degree of sophistication will depend on the type and complexity of the DNFBP; a small stand-alone DNFBP that mainly serves established local customers operating in the domestic market will have very different screening needs than a large DNFBP that is part of a group with customers and transactions spanning many jurisdictions. In practice, most DNFBPs in PNG will not fall into the latter category, and many will not have the resources to invest in commercial screening software. In this case, the DNFBP will need to be as proficient as possible at screening customers manually; however, this need not preclude the DNFBP from implementing an effective screening process (see Text Box on page 29).

The Screening Process

The screening process generally consist of the following steps:

- **Data collection and preparation:** This entails gathering by the front-line business units of relevant customer data, which typically includes names, addresses, and identification numbers, as well as transaction details and BO information. Strictly speaking, this is not part of the screening process; however, it is critical to the proper functioning of that process. Customer data must be accurately entered and maintained. Poor data quality and integrity can have a severely negative impact on the ability of the DNFBP to know its customers and conduct customer due diligence. This data therefore must be standardized and formatted for efficient screening.
- **Screening against sanctions lists:** The prepared data is screened by one or more sanctions analysts against the U.N. Consolidated List published by the Sanctions Secretariat. This screening process can involve exact matches, fuzzy logic (finding partial matches with imprecise data), or phonetic matching (matching names that are pronounced the same) to identify potential matches.

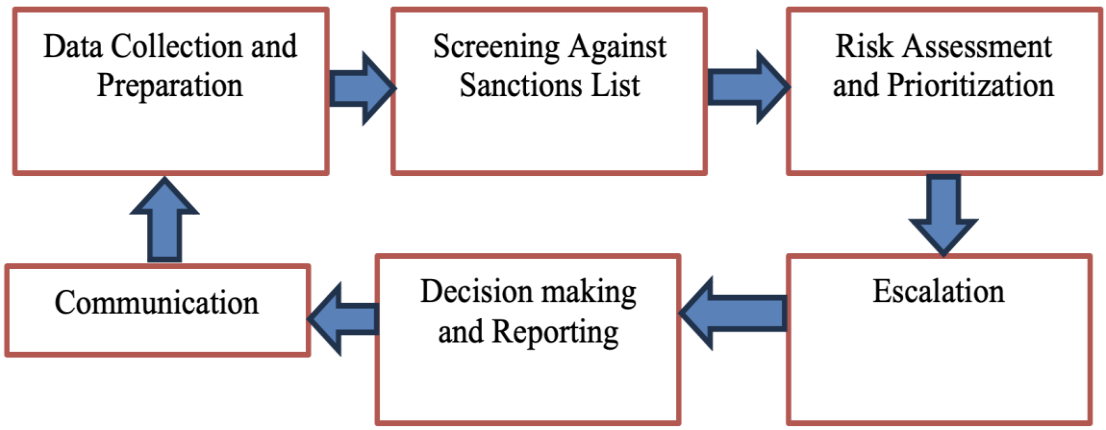
- **Risk assessment and prioritization:** Risk assessments are conducted on any identified matches. The potential risk associated with each match is evaluated based on factors such as the type of transaction, and the customer's risk profile. Matches should be prioritized for further investigation.

- **Escalation:** High-risk matches should undergo a more thorough investigation including additional research and due diligence, and, potentially, contacting relevant authorities. This step determines whether the match is a true positive or a false positive. Typically, this step would be conducted by a more experienced analyst.

- **Decision-making and reporting:** Based on the investigation's findings, a decision is made regarding the match. If the match is a true positive, the decision will be communicated to the relevant business line and appropriate action is taken, such as freezing assets, blocking transactions, or reporting to FASU. False positives are documented and cleared. Typically, this decision will be taken by a senior member of the sanctions compliance function, such as the DNFBP's SCO or an experienced member of the staff with delegated authority.

Of course, the details of the above scenario can vary depending on the size and risk profile of each DNFBP. Smaller DNFBPs will likely not have the resources or personnel to institute multiple layers of review; in this case the DNFBP will need to ensure that the person(s) performing the initial screening are thoroughly competent regarding use of the Consolidated List and the criteria for DNFBP action when DPEs are identified.

The following figure depicts the screening process:



Customer Name Screening

DNFBPs must have a system in place to screen customers during on-boarding and through the life cycle of the customer relationship. This also includes directors and BOs of corporate customers and legal arrangements, and any other parties with access to the account. At a minimum, screening should take place when establishing a new relationship, and at regular intervals either upon a trigger event (such as a change in directors or ownership) or when a sanctions list changes.

Sanctions screening should be a top priority after the initial risk assessment when onboarding a customer or third party. In addition, DNFBPs should that ensure existing customers and third parties are screened on a regular basis. Possible matches should be addressed urgently, with clearly defined processes for escalation. Some of the main issues include:

Name variations

This is an extremely important part of the screening process. DNFBPs should ensure that their screening system (whether manual or automated) can handle name variations. Some of the more common issues likely to be encountered are summarized in **Appendix 2**.

Issues Regarding Birth Dates

Dealing with birthdates can present challenges for two main reasons:

- High risk individuals often do things to obscure their real date of birth.

- In many jurisdictions, birth certificates do not exist. Some people may not know their exact date of birth, and even if they do, they may not have any documentation to verify it. For some individuals, dates of birth may simply be guessed or interpreted based on other characteristics such as when they went to school or when they got married (which would be accurate to within a few years at best).

In the cases where an exact birthdate is not available, birthdate filters should be set to match the level of risk. For example, a DNFBP might filter its screening results against a "politically exposed person" ("PEP") filter with a configuration of plus or minus one year. This will allow the DNFBP to narrow its screening hits to the most likely results and help to balance resources spent while still allowing for a risk-based approach. If the DNFBP screens for adverse media, this can be a larger range such as plus or minus four years (depending on the DNFBP's risk appetite). DNFBPs should screen against law and regulatory enforcement data with a much wider net, such as plus or minus five or six years.

Finally, as with any filter, there is always a possibility of false negatives. DNFBPs should set their filters to ensure that they are not missing any high-risk false negatives. Some jurisdictions have reliable birthdate information, so DNFBPs can use a tighter date range. For other high-risk jurisdictions where birthdate information cannot be trusted, a wider threshold will be necessary.

Transaction Screening

Each customer or potential customer, and each incoming and outgoing transaction should be screened for a potential match with the Sanctions List. This is the first, and most critical step. Screening prior to completing a transaction is known as *real-time screening* and is the most widely used. In transaction monitoring, some of the most common screening data points include:

- Parties involved (remitter, beneficiary, other financial institutions involved in the transaction, intermediaries);

- Vessels and International Maritime Organization (IMO) numbers (unique identifier number assigned to each vessel) – especially relevant for DPRK;

- Bank names, bank identifier codes (BIC) and other routing codes;

- Free text fields (e.g., payment reference)

DNFBPs should pay particular to those data points within the transactional process where information could be modified or removed to undermine screening controls, for example evidence that information has been stripped from the transaction, or the transaction exhibits signs of sanctions evasion techniques.

Updating Sanctions Records

An DNFBP's internal controls should include policies, procedures, and processes for timely checking for updates of the list of DPEs published by the Sanctions Secretariat, and disseminating any updates to all relevant DNFBP personnel, including to its branches and subsidiaries, if any.

Controls Pertaining to Asset Freezes

Once assets are frozen, they should be placed in a separate account specifically designated to hold frozen assets. The screening process should clearly identify the DNFBP personnel with the authority to approve the freezing of assets, indicate how the decision to freeze assets will be identified to other DNFBP staff, and include a procedure for maintaining a written record of the determination to freeze the asset(s).

More information on recordkeeping regarding frozen assets is provided below.

Controls Pertaining to Authorisations

A DNFBP's internal controls should contain provisions to ensure that they do not apply the prohibitions to persons and entities that have been issued such an authorisation by the Prime Minister or by the UNSC or one of its Committees (described in Section 2.3 above). The controls should:

- indicate how unfrozen assets will be identified to other DNFBP staff, including all relevant information (e.g., which assets of a given DPE are unfrozen and which, if any, remain frozen and any conditions that may be attached to the authorization);

- include a procedure for maintaining a written record of the determination to unfreeze the asset(s), and for ensuring that the list of unfrozen assets remains current and accurate;

- require written records to document any use of unfrozen assets in order to demonstrate that any such use in in line with the authorisation granted by the Prime Minister or the UNSC or relevant Committee, including compliance with any conditions that may accompany the authorisation.

Resolving False Positives

False positives are potential matches to listed persons and entities, either due to the common nature of the name or due to ambiguous identifying data, which prove not to be matches on examination. This can occur for a number of reasons:

- **Overly sensitive systems:** Some systems might be set up capture too much information, triggering alerts for a wide range of customers or transactions that are actually legitimate.

- **Data quality issues:** Inaccurate or incomplete data can lead to incorrect matches and flags.

- **Outdated systems:** Older systems may rely on older matching methods and rules that are no longer effective.

- **Similar names or patterns:** International naming conventions or common transaction patterns can lead to false matches with individuals or entities on sanctions lists (see **Appendix 2**).

False positives can cause a number of problems for any business:

- **Waste of resources:** False positives consume significant resources, including time, personnel, and financial resources, for investigations that ultimately prove unnecessary.

- **Delays in legitimate customer onboarding:** Until all screening procedures are completed and a decision is made, the DNFBP cannot onboard a customer.

- **Business disruption:** False alerts can disrupt legitimate business operations, causing delays in transactions and potentially damaging relationships with legitimate customers.

- **Erroneous freezing of assets:** One of the unfortunate consequences of false positives is that a person or entity might mistakenly have its assets frozen. Where a person or entity believes that their assets have been frozen in error, they should immediately contact the asset holder (the FI or DNFBP) directly.

- **Obstruction of actual threats:** If a high number of false positives occur, the sheer volume of matches could be so high that some actual positives might be missed. This can result in under-reporting of information to the FASU, which in turn can lead to fines and penalties.

- **Reputational damage:** False positives can harm the reputation of individuals and businesses, leading to unnecessary scrutiny and potential reputational damage.

False positives can never be completely eliminated. They can, however, be significantly minimised. DNFBPs can take several steps to accomplish this:

- **Regular review***:* DNFBPs should periodically review and optimize their transaction monitoring systems to balance sensitivity with accuracy.

- **Data quality improvement:** DNFBPs should invest the time and resources to improving data quality and ensuring that their systems have access to accurate, complete and up-to-date information.

- **Implement "whitelisting:"** DNFBPs may consider creating lists of known legitimate customers and transactions to prevent them from being flagged unnecessarily.

- **Collaboration and information sharing:** DNFBPs that have different units or departments should promote collaboration between those units or departments (and where applicable, entities within the same group) to share insights and improve the effectiveness of customer identification efforts.

- **Use sophisticated algorithms:** DNFBPs that use commercial software should employ more advanced matching algorithms that can distinguish between true and false positives.

- **Use entity resolution:** DNFBPs should implement entity resolution to match multiple pieces of information to identify and resolve false positives more efficiently.

- **Leverage AI:** DNFBPs that use commercial software may use AI-powered tools to reduce false positives and improve the accuracy of screening.

- **Training and awareness**: DNFBPs should provide training to employees on how to identify and respond to false positives effectively.

In some cases, additional follow-up measures may be necessary. While a potential match does not always indicate an actual match, where the above steps are inconclusive, the issue should be investigated further, and either confirmed or dismissed based on that investigation. Such follow-up techniques can include:

- Communicating compliance expectations to customers on a risk basis, including informing them that they may not use their accounts to do business with DPEs. This may also include sharing the list of DPEs with customers, especially customers engaged in import-export activity, manufacturing, or any other relevant business lines.

- Sending questionnaires, on a risk basis, to customers known to deal in high-risk jurisdictions or other parties to better understand their counterparties.

- Using open-source information and past transactional activity to inform due diligence and to conduct proactive investigations into possible sanctions and export control evasion.

- Undertaking proactive investigations into suspected sanctions evasion. These often involve post-transaction reviews for typologies, networks, and/or suspicious activity, as opposed to real-time, list-based screening. Sanctions-related information (e.g., interaction with listed entities prior to designation) can serve as an input for these investigations. The results of these investigations could then be used to further identify risky customers and other sanctions related risks.

- Using information received through requests for information from PNG governmental sources and FIs, including global correspondent banks where applicable, as well as data from commercial service providers or public data sources such as trade and customs data, to inform due diligence and conduct proactive investigations.

- When appropriate, obtaining attestations from high-risk customers that they do not engage in any sales or transfers or otherwise conduct any transactions with DPEs.

- Taking appropriate mitigation measures for any customers or counterparties engaged in high-risk activity or who fail to respond to requests for information regarding activity of concern. These measures include restricting accounts, limiting the type of permissible activity, exiting relationships, and placing customers or counterparties on internal "do not onboard" or "do not process" watchlists.

- Incorporating risks related to DPEs into sanctions risk assessments and customer risk-rating criteria. This includes updating jurisdictional risk assessments as appropriate.

- Implementing enhanced trade finance controls related to the specified items, including monitoring information collected as part of documentary trade.

Beneficial Ownership

One of the most critical aspects of customer identification is knowing the *beneficial owner* (BO) of an account or of a legal entity or legal arrangement that is or seeks to become a customer. Section 5(1) of the AML/CFT Act defines a BO as a natural person who –

- has ultimate control, directly or indirectly, of a customer; or

- ultimately owns, directly or indirectly, the customer.

According to FASU Guidance, "control" includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, where or not having legal or equitable force and whether or not based on legal or equitable rights. This includes exercising control through the capacity to make decisions about financial and operating policies. "Owns" means ownership, either directly or indirectly, of 25% or more of a person or unincorporated entity.[13]

Beneficial ownership is easy to define, but can be extremely challenging to identify in practice. DNFBPs need to be extremely diligent to ensure that they know who is actually controlling their customers or potential customers, not just who the nominal owners are. **Appendix 3** provides detailed guidance on this issue.

Distinctions between BO Status and Ownership for DPE purposes

For purposes of determining control for sanctions screening purposes, the BO criteria described **in Appendix 3** is helpful. However, there are some important differences that must be kept in mind:

[13] FASU Guidance for Financial Institutions on their Obligations under the *Anti-Money Laundering and Counter Terrorist Financing Act* 2015 (No. 1 of 2019) Section 8, page 25.

- A BO is always a natural person; a DPE can be either a natural or legal person.

- The numerical tests/thresholds for determining ownership are different. In PNG, 25% is the relevant ownership threshold for BO identification. Based on international practice, 50% is more typical in for determining DPE status for an entity.

When assessing ownership of a given entity, the aggregated ownership of the entity should be taken into account. For example, if one DPE owns 30% of the entity and another DPE owns 25% of the entity, the entity should, in principle, be considered as owned by DPEs.

Sanctions Compliance Officer

Each DNFBP needs to ensure that there is at least one person who is responsible for sanctions compliance. The SCO may be an employee of, or external to, the business. For a sole practitioner, this is an easy decision: the sole practitioner will be the compliance officer unless the role is outsourced. In a small organisation, the persons who manage the business on a day-to-day basis should designate one person to perform this role. That person should thoroughly understand the requirements of the UNFSA and related regulations and how to comply with them, and have sufficient authority to take decisions affecting the firm's risk exposure.

Recordkeeping and Reporting

Section 40 of the AML/CFT Act requires DNFPBs to report to the FASU any assets that they hold of a DPE. The report must be made as soon as is reasonably practicable or within 10 working days from the date notification of a designation is received.

A DNFPB's controls should include policies, procedures, and processes regarding frozen assets, including the procedure for escalating suspected positive matches (described above regarding the screening process), identification of the person within the organisation responsible for submitting the required reports to the FASU (normally this will be the SCO), and the steps in the process for doing so. Records should include:

- the amount of frozen assets;
- the ownership of those assets;
- interest paid on any frozen accounts;
- a description of any transaction associated with frozen assets, including:
  - the type of transaction;
  - any persons, including FIs or other DNFPBs, participating in the transaction and their respective locations; and
  - any reference numbers, dates, or other information necessary to understand the transaction;
- written documentation of the DNFPB's decision to freeze the assets, including the date the assets were frozen, the approving official within the DNFPB, copies of any relevant documentation supporting the decision, and any other communications with, or information received from, any regulatory authority regarding the assets; and
- documentation regarding any decision to unfreeze assets (see discussion above).

I RUN A VERY SMALL BUSINESS AND CANNOT AFFORD EXPENSIVE SANCTIONS SOFTWARE – HOW CAN I COMPLY WITH THE USFSA?

Sanctions compliance need not be prohibitively expensive or impede your ability to provide high-quality service to legitimate clients or customers. Smaller businesses can comply quite effectively by implementing a few simple steps.

- **Know your obligations.** Review the UNFSA and become familiar with its requirements. Bookmark the Sanctions Secretariat's website and check frequently for new announcements and updates.
- **Know your sanctions risks.** No one knows your business better than you. Conduct a thorough – and candid – risk assessment. Make an honest assessment of the risks posed by your customers, products, services, and the geographic region(s) in which you and your customers operate. Assess the quality of the controls you have put in place to mitigate these risks. Take steps to reduce unacceptably high risks and to improve control functions when necessary.
- **Focus on high-risk clients and transactions.** Prioritise compliance efforts on areas most susceptible to sanctions violations. Consider creating a "whitelist" of low-risk established clients whose transactions demand less attention.
- **Share the load internally.** If possible, delegate routine tasks (e.g., initial screening new customers) to a junior team member with proper training.
- **Implement a simple, user-friendly compliance framework.** Without clear processes, you might miss steps or apply standards inconsistently. A straightforward compliance framework can guide you through routine checks without overcomplicating things. The framework should be easy to follow but robust enough to handle non-routine matters. Develop a one-page checklist for sanctions compliance tasks and keep it visible in your workspace.
- **Screen all new customers against the Consolidated List.** Check the Consolidated List frequently. Consider checking other jurisdictions' sanctions lists if you operate internationally; this could reveal some connections to your clients that could raise some issues that should be investigated further.
- **Perform enhanced due diligence (EDD) for any high-risk customers.** Consider implementing thresholds for escalating risks, such as involving external experts when very complex analysis is required.
- **Train your team.** Even if you are the primary person responsible, ensure other key staff understand the basics of sanctions compliance to share the load when needed.
- **Keep good records and document everything.** Maintain a clear paper trail that confirms your company's compliance efforts. Maintain logs of CDD checks and decisions to decline to establish customer relationships, or to terminate any relationships, and to freeze and unfreeze assets. Keep copies of all correspondence with the regulators – especially reports required by Section 40 of the AML/CFT Act. Maintain compliance records in a single, organised system that is accessible but secure. This can be as simple as a shared folder (which can be electronic or a paper folder) or as advanced as a compliance software platform. Create a dedicated "Sanctions Compliance" folder in your company's shared drive and organise it by year and transaction. The exact format is not very important – what is critical is that YOU understand it and can access information quickly when necessary.
- **Engage external experts:** If you encounter complex situations (e.g., screening a high-risk client or working through a convoluted client ownership structure), consult with a compliance specialist or external legal counsel. Building relationships with compliance consultants or law firms that specialise in sanctions and having that trusted source on "speed dial" can alleviate a lot of stress and save precious time during a crisis.
- **Talk to your regulators:** The Sanctions Secretariat, FASU and similar bodies can provide guidance to small businesses. Contact them if you're unsure about an issue. They would rather help you avoid violations than penalise you after the fact.

Adapted from https://www.sanctions.io/blog/sanctions-compliance-for-non-dedicated-roles#final-thoughts-sanctions-compliance-for-non-dedicated-roles

3.4 INDEPENDENT TESTING AND AUDITING

DNFBPs generally should have their SCPs audited by an independent party on a regular basis. However, this is not a hard and fast rule. In a very small DNFBP, where senior people have a good understanding of all the business's clients and matters, a formal audit may not be necessary. An independent audit is more likely to be needed if junior employees undertake a significant volume of work. A sole practitioner with no relevant employees or agents need not implement formal regular independent audits or reviews unless requested to do so by the Sanctions Secretariat or the FASU. They should, however, regularly assess their compliance procedures and determine if any changes are necessary. For those DNFPBs that do decide to undertake an audit, some recommended points are included here.

- The auditor does not need to be independent of the business, but must be independent of the function being reviewed.

- While the frequency of independent audits is not specifically defined in UNFSA or the FASU Guidelines for DNFBPs, it is a good business practice to conduct independent testing generally every 12 to 18 months, commensurate with the DNFPB's risk profile.

- Testing should address:

  - the content of the DNFPB's sanctions policies and procedures and their overall implementation;

  - the quality of the DNFPB's sanctions risk assessment given the DNFPB's risk profile (products, services, customers, entities, and geographic locations);

  - the effectiveness of the DNFPB's customer and transaction screening systems;

  - management's efforts to remedy any violations and deficiencies noted in previous audits or supervisory inspections, including progress in addressing outstanding corrective actions required by the supervisory authority, if applicable;

  - the DNFPB's staff training for adequacy, accuracy, and completeness;

  - an assessment of the reporting process to the FASU, including a review of filed or prepared reports to determine their accuracy, timeliness, and completeness.

3.5 TRAINING

A sanctions program cannot be effective if a DNFBP's personnel do not understand the requirements and how to comply with them. It is essential that all personnel whose function requires sanctions knowledge are appropriately trained.

Training should:
- include legal and regulatory requirements and the SCP;
- be tailored to specific job responsibilities;
- be provided to all new staff as soon as possible following on-boarding;

- be provided periodically (annually or at least every two years) on a "refresher" basis;
- be provided by instructors who are thoroughly familiar with the UNFSA, AML/CFT Act, relevant UNSC Resolutions and recommendations of international standard-setting bodies (e.g., FATF);
- include examples and real-world case studies of sanctions evasion techniques; and
- describe the DNFBP's process for detecting suspected cases of sanctions evasion and dealing with them within the organization, as well as reporting to the FASU.

DNFBPs should document their training programs. Training and testing materials, the dates of training sessions, and attendance records should be maintained. Employee knowledge based on the training should be checked and serious deficiencies should be remedied. Management should ensure that sufficient resources are devoted to sanctions-related training.

Some small DNFBPs may not have the capacity to develop in-house training programs themselves. In such cases, the training function can be outsourced to a reputable outside training organization. However, the DNFBP must have a written contract or engagement letter regarding the content of the training, and means to ensure the reliability of the persons providing the training. The DNFBP itself remains responsible for ensuring that effective training is provided.

Sole practitioners do not need to establish a formal training program, but they should ensure that they are keeping up to date with legal and regulatory developments, the content of the Consolidated List, and any sanctions-related information that might impact their business (such as how persons who are likely to use their services may attempt to evade sanctions). It is a good practice for sole practitioners to:

- Take advantage of learning opportunities offered by the Sanctions Secretariat, FASU, or industry groups;

- Exchange ideas and experiences with other DNFBPs with similar practices; and

- Keep written records of what they are doing to maintain a high level of sanctions compliance knowledge (e.g., a list of sanctions-related courses attended, updates that they are making in their internal processes as a result of such training, etc.).

Key contacts

Office	Purpose	Contact
Sanctions Secretariat	List updates, licences, and public guidance	mailto:pngsanctions@pmnec.gov.pg
FASU (Bank of PNG)	Suspicious Matter Reports	mailto:fasu@bankpng.gov.pg

REFERENCES

Alessa, Inc., *How to Test Your Sanctions and Watch List Screening Software*, *https://alessa.com/wp-content/uploads/2020/06/How-To-Test-Sanctions-Screening-Software.pdf*

AML compliance requirements for the real estate sector in the UAE, *https://amluae.com/a-deep-dive-into-the-aml-compliance-requirements-for-the-real-estate-sector-in-the-uae/*

Anna Bradshaw and Alistair Jones, *The Guide to Sanctions – Fifth Edition: A UK Lawyer's Perspective on Representing Designated Persons*, *https://globalinvestigationsreview.com/guide/the-guide-sanctions/fifth-edition/article/uk-lawyers-perspective-representing-designated-persons*

Australian Department of Foreign Affairs and Trade, Sanctions Office, *Sanctions Compliance Toolkit* https://www.dfat.gov.au/international-relations/security/sanctions/guidance/sanctions-compliance-toolkit

CPA Canada, *Why CPAs Need to Watch Out for Sanctions Evasion*, *https://www.cpacanada.ca/news/accounting/the-profession/2022-05-04-russian-ties*

Compliance Commission of The Bahamas, *Sanctions Guidance for DNFBPs Supervised By The Compliance Commission of The Bahamas* (2020) https://ccb.finance.gov.bs/wp-content/uploads/2020/12/SANCTIONS-GUIDANCE.pdf

European Lawyers' Foundation, *Development and Organization of Training for Lawyers on AML-CFT Rules at the EU Level* (2021) https://finance.ec.europa.eu/system/files/2022-03/aml-ctf-lawyers-training-users-manual_en.pdf

European Union Best Practices for the Effective Implementation of Restrictive Measures https://data.consilium.europa.eu/doc/document/ST-11623-2024-INIT/en/pdf

FATF, *Risk-based Approach Guidance for the Real Estate Sector*, *https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-real-estate-sector.html*

FATF, *Money Laundering and Terrorist Financing Through the Real Estate Sector*, *https://www.fatf-gafi.org/en/publications/Methodsandtrends/Moneylaunderingandterroristfinancingthroughtherealestatesector.html*

FATF, *Legal Professionals: Guidance for a Risk-Based Approach* (2019) https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Legal-Professionals.pdf.coredownload.pdf

FATF, *Guidance for a Risk-Based Approach – Accounting Profession* (2019) https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Rba-accounting-profession.html

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), *Special Bulletin on the Use of the Legal Profession in Money Laundering and Sanctions Evasion* (2024) https://fintrac-canafe.canada.ca/intel/bulletins/legal-juridique-eng.pdf

European Parliament, *Understanding money laundering through real estate transactions, https://www.europarl.europa.eu/cmsdata/161094/7%20-%2001%20EPRS_Understanding%20money%20laundering%20through%20real%20estate%20transactions.pdf*

Institute of Chartered Accountants in England and Wales, *Anti-money laundering for Smaller Practices* (2019) https://www.icaew.com/technical/tas-helpsheets/anti-money-laundering-helpsheets/anti-money-laundering-for-smaller-practices

International Bar Association, American Bar Association and the Council of Bars and Law Societies of Europe, *A Lawyer's Guide to Detecting and Preventing Money Laundering* (2014). https://www.lawsociety.org.uk/topics/anti-money-laundering/global-aml-guidance#:~:text=A%20lawyer%27s%20guide%20to%20detecting,comply%20with%20international%20legal%20obligations

Law Society of England and Wales, *Anti-money laundering (AML) Compliance for Small Firms,* https://www.lawsociety.org.uk/topics/anti-money-laundering/aml-compliance-for-small-firms

Mauritius National Sanctions Secretariat, *Guidelines on the Implementation of Targeted Financial Sanctions Under the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019* https://www.bom.mu/financial-stability/supervision/guidelines/guidelines-implementation-targeted-financial-sanctions-under-united-nations

New Zealand Ministry of Foreign Affairs and Trade, *Russia Sanctions Guidance - Sanctions Evasion: Common Red Flags* (2024) https://www.mfat.govt.nz/assets/Countries-and-Regions/Europe/Ukraine/Guidance-note-Sanctions-evasion-red-flags.pdf

OECD *Ending the Shell Game: Cracking down on the Professionals who enable Tax and White Collar Crimes* (2021) *http://www.oecd.org/tax/crime/ending-the-shell-game-cracking-down-on-the-professionals-who-enable-tax-and-white-collar- crimes.htm*

PNG Sanctions Secretariat: https://pngsanctionssecretariat.gov.pg.

Risk Assessments: Your Risk Management Compass
(CBA Regulatory Compliance Conference – October 4, 2017)
https://www.westernbankers.com/post/39th-annual-regulatory-compliance-conference-materials

Stanford Law School (U.S.) Policy Practicum on Regulating Professional Enablers, *Regulating the Lawyer-Enablers of Russia's War on Ukraine* (2024) (Prepared for the International Working Groupon Russian Sanctions)

https://law.stanford.edu/wp-content/uploads/2024/05/SLS_Policy_Lab_Lawyers-Enablers_Report_May20241.pdf

U.K. *Anti Money Laundering Guidance for Accountancy Sector* (2018) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/694687/Anti-Money_Laundering_Service_-_Guidance_for_Accountancy_Sector.pdf

U.K. National Crime Agency, *Gold-based Financial and Trade Sanctions Circumvention* (2023), https://www.nationalcrimeagency.gov.uk/who-we-are/publications/679-necc-red-alert-gold-sanctions-circumvention/file

United Nations Office on Drugs and Crime (UNDOC) https://www.unodc.org/unodc/en/money-laundering/overview.html#:~:text=Money%20provides%20terrorist%20organisations%20with,be%20divided%20in%20following%20stages:

U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), *A Framework for OFAC Compliance Commitments* https://ofac.treasury.gov/media/16331/download?inline

U.S. Federal Financial Institutions Examination Council (U.S.) *Bank Secrecy Act/ Anti-Money Laundering Examination Manual* (2014) https://bsaaml.ffiec.gov

U.S. Financial Crime Enforcement Network (FinCEN) *Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies* (2023), https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Real%20Estate%20FINAL%20508_1-25-23%20FINAL%20FINAL.pdf

U.S. Financial Industry Regulatory Authority (FINRA), *Anti-Money Laundering (AML) Template for Small Firms*, https://www.finra.org/compliance-tools/anti-money-laundering-template-small-firms

Wolfsberg Group, *Guidance on Sanctions Screening* https://db.wolfsberg-group.org/assets/4b6c2db6-696d-492e-bdd5-c51552708597/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

Wolfsberg Group, *Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption* https://db.wolfsberg-group.org/assets/3deb66d7-6aca-490c-bcd9-c1a3d34a807b

APPENDIX 1

SAMPLE FIRM-WIDE SANCTIONS RISK ASSESSMENT FOR A SMALL BUSINESS

DNFBPs need to assess the services they provide and the types of clients they have, to understand how DPEs could use them to conceal the sources or destinations of their funds or activities, or use the DNFBP's services to create arrangements that could facilitate TF or PF.

If you are providing services that could enable DPEs to achieve these results, you will need to step back and think about the risks affecting your business as a whole.

Your risk assessment should identify the areas of your business that are most at risk and this will enable you to focus your resources on the areas of greatest risk.

It is the responsibility of your firm's senior management (or you, if you operate as a sole practitioner) to approve the policies, controls and procedures that address and mitigate the risks and you should document all these aspects.

PROFILE OF FIRM

- Number or employees
- Total firm income in PNG kina.
- Services (e.g., accounting, law firm, real estate, etc.).
- Client base (e.g., mainly individuals, small businesses, small/medium companies, larger companies, etc.)
- Geographic reach (e.g., mainly locally based clients? If any operate overseas, indicate how many)

STEP 1: DETERMINING INHERENT RISK FACTORS	High = 3	Moderate = 2	Low = 1	Score
Nature of Business: Does your industry or type of business involve activities that are frequently targeted by DPEs? Yes, frequently = High Some, but not frequent = Moderate Very little or never = Low				
Customers: Are any of your customers, directly or indirectly, located in high-risk jurisdictions? Many = High Moderate amount = Moderate Few or None = Low				
Customers: Large and growing customer base in an international environment = High Customer base increasing due to branching, mergers/acquisitions, mainly domestic = Moderate Stable, well- known local customer base = Low				
Delivery Channels: How are your services mainly delivered? Mainly internet based = High Mixture of internet and face-to-face = Moderate Mainly face-to-face = Low				
Supply Chain: Are any of your suppliers, or their suppliers, located in high-risk jurisdictions? Many = High Moderate amount = Moderate Few or None = Low				
Intermediaries: Are you using intermediaries or agents that could be involved in sanctions evasion? Many = High Moderate amount = Moderate Very few or None = Low				

Transactions: Have you observed any unusual transaction patterns or payment methods that could indicate sanctions evasion? Many = High Moderate amount = Moderate Few or None = Low				
Client funds: Does your firm handle client money (e.g., in a client trust account?) Yes = High No = Low				
RISK RATING SCORE: Numerical average of risk rating scores: High Risk = 2.5 or greater. Moderate Risk = 1.6 to 2.49. Low Risk = 1.5 or less				
STEP 2: DETERMINING QUALITY OF CONTROLS	**High Quality (3)**	**Moderate Quality (2)**	**Low Quality (1)**	
Policies and Procedures: Do you have clear policies and procedures in place for sanctions compliance? Yes = High quality Generally acceptable, some gaps = Moderate quality No = Low Quality				
Beneficial Owners/Control: Are you able to correctly identify the BOs of your customers and other third parties with whom you do business? Yes, consistently = High quality Sometimes = Moderate quality With great difficulty or not at all = Low quality				
Consolidated List: Do you frequently check the Consolidated List to ensure that you are up-to-date? Yes, frequently = High quality Sometimes = Moderate Never or rarely = Low quality				

Sanctions Screening: Are you screening customers and other parties with whom you do business against the Consolidated List? Yes, consistently = High quality Sometimes = Moderate Never or rarely = Low quality				
False positives: Is your screening process able to identify and resolve false positives? Yes, consistently = High quality Sometimes = Moderate With great difficulty or not at all = Low quality				
Due Diligence: Are you conducting sufficient due diligence on high-risk customers and other third parties with whom you do business? Yes, consistently = High quality Sometimes = Moderate Never or rarely = Low quality				
Periodic Review: Do you periodically review your SCP (whether via formal audit or less formal internal review) to determine its effectiveness, and take action to remedy any identified deficiencies? Yes, consistently = High quality Sometimes = Moderate Never or rarely = Low quality				
Training: Do your employees receive training on sanctions compliance? Yes, frequently (soon after on-boarding, with periodic refresher training (e.g., annually) = High quality Sometimes (occasionally, but no specific pattern) = Moderate Never or rarely = Low quality				
Average of quality control risk ratings: High Quality = 2.5 or greater. Moderate Quality = 2.5 or greater = 1.6 to 2.49. Low Quality = 1.5 or less				

Having assessed both your organisation's inherent risk factors (Step 1), and the quality and effectiveness of the controls in place to mitigate those risk factors (Step 2), you are in a position to determine your organisation's overall sanctions risk. A suggested sample is provided here:

Risk Rating Score	Control Quality	Overall Risk Rating
High	High	Moderate
	Moderate	High
	Low	High
Moderate	High	Moderate
	Moderate	Moderate
	Low	High
Low	High	Low
	Moderate	Low
	Low	Moderate

Once your risk assessment is complete, you should determine whether any changes are necessary. This may entail reducing your organisation's "inherent risk," improving the quality of your mitigating controls, or both.

It is a good practice to conduct a risk assessment periodically (e.g., annually). You should document in writing the results of your risk assessment, and any follow-up measures you have instituted to correct any shortcomings.

APPENDIX 2 – COMMON ISSUES REGARDING NAME SCREENING[1]

- *Variations in upper and lower cases*.

- *Identical matching*, in which the full name is matched against all the lists. This involves the ensuring the accuracy of the matching process itself, and ensuring that the data will provide a positive match against different sources.

- *Missing or additional hyphens or spaces.* These can occur when character sets are converted (for example, a non-Latin name to a Latin name). DNFBPs should ensure that their screening system can deal with differences in punctuation, and missing components or letters.

- *Missing components/letters or truncated names* can become especially troublesome with very long last names. DNFBPs need to be aware of any character limitations in any fields within their screening system, and what happens if that limitation is exceeded.

- *Incorrect database fields* can occur if data is entered from other systems are not divided correctly.

- *Spelling differences* in names that can be spelled in different ways (examples: "Sean" vs. "Shaun," "Shawn," or "Sian");

- *Nicknames:* (example: "William," "Bill," "Will," "Billy," or "Willy").

- *Titles and Honorifics,* such as "Reverend," "Imam," "Mister," "Miss," "Lady" or "Lord." DNFBPs should ensure that their screening system can handle these.

- *Out of order components,* such as when given names are switched with surnames.

- *Multiple languages.* DNFBPs should ensure that their system can handle names in their native character set such as Arabic or Chinese.

- *AKAs* ("also known as"). DNFBPs should know how their system handles these variations.

- *Initials*. DNFBPs should know how the system handles initials rather than the full first names.

- *Similar names or phonetic similarities:* Names that may sound similar but are in fact different (example: "Jang" and "Jung").

[1] Adapted from Alessa, Inc., *How to Test Your Sanctions and Watch List Screening Software,* https://alessa.com/wp-content/uploads/2020/06/How-To-Test-Sanctions-Screening-Software.pdf

- *Noise simulation*, where characters are added or are switched (for example, insertion of extraneous characters or when a zero is used instead of the letter O.

- *Accents, Transliteration and Translation*: Screening names in their non-Latin native characters can be challenging for DNFBPs that communicate in languages that use Latin characters. However, even languages that use Latin characters, like Spanish, Portuguese, Dutch, French and German, can be challenging due to some unique letters and accents. The system needs be able to deal with names with and without accents (for example, the Hispanic name Jose/José). DNFBPs also need to decide how to handle variations such as "Joe," or "Joseph," which can be a translation of José. Non-Latin conversions are particularly complex. Some systems transliterate names, while others translate them (transliteration is the process of transferring a word from one alphabet or language into the corresponding, similar-sounding characters of another alphabet, such as from the Latin to the Cyrillic; translation informs the meaning of a word in another language).

- *Variations of Muhammed*: The name Muhammad is one of the most common first names in the world. There are at least 65 common variations of this name, and it is one of the most frequently misspelled when it comes to onboarding customers. The spelling of the name varies based on different jurisdictions, different standards across different countries and in different scripts. DNFBPs need to be sure that the way the person spells it is the way it actually appears on file. Problems arise when there is an error in data input or how the name was entered.

- *Variations by region:* There are also many other complexities according to geographic region.

  - Some of the most complex issues revolve around marriage. In Western Europe and North America, many people assume that a person's surname is the father's last name. Also, by tradition, when a woman gets married, she adopts her husband's last name, but that tradition is changing. The situation is different in Spanish speaking Latin America; a person's last name is the father's first last name and then the mother's first last name. In most countries in Latin America, women do not change their names when they get married. The tradition is still different in Portuguese speaking countries. In Brazil, a person's surname is the mother's first last name followed by the father's first last name. Therefore, a DNFBP will likely run into some complexities in the case of customers from Latin American countries. For example, if it has a customer who is originally from Brazil, but now has moved to Columbia, there can be some very complex issues as that person's name may now be changed.

  - In some countries (e.g., Eritrea, Ethiopia and Iceland), there are cases where a person's last name is the father's first name rather than a traditional last name.

  - In the Arab world, names may be [first name] bin [father's name] [sometimes another descriptor such as a family name or ancestral home].

- In Japan, China and Korea, the last name appears first, although in Japan this is beginning to change to a western style in documents that appear with the Latin alphabet.

APPENDIX 3 – GUIDANCE ON BENEFICIAL OWNERSHIP

Overview

One of the most critical aspects of customer identification is knowing the *beneficial owner* (BO) of an account or of a legal entity or legal arrangement that seeks to become a customer. Section 5(1) of the AML/CFT Act defines a "beneficial owner" as a natural person who –

- has ultimate control, directly or indirectly, of a customer; or
- ultimately owns, directly or indirectly, the customer.

Thus, there are two means of determining beneficial ownership, both of which need to be taken into account:

- the "ownership" component; and
- the "control" component.

According to FASU Guidance, "control" includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, where or not having legal or equitable force and whether or not based on legal or equitable rights. This includes exercising control through the capacity to make decisions about financial and operating policies.

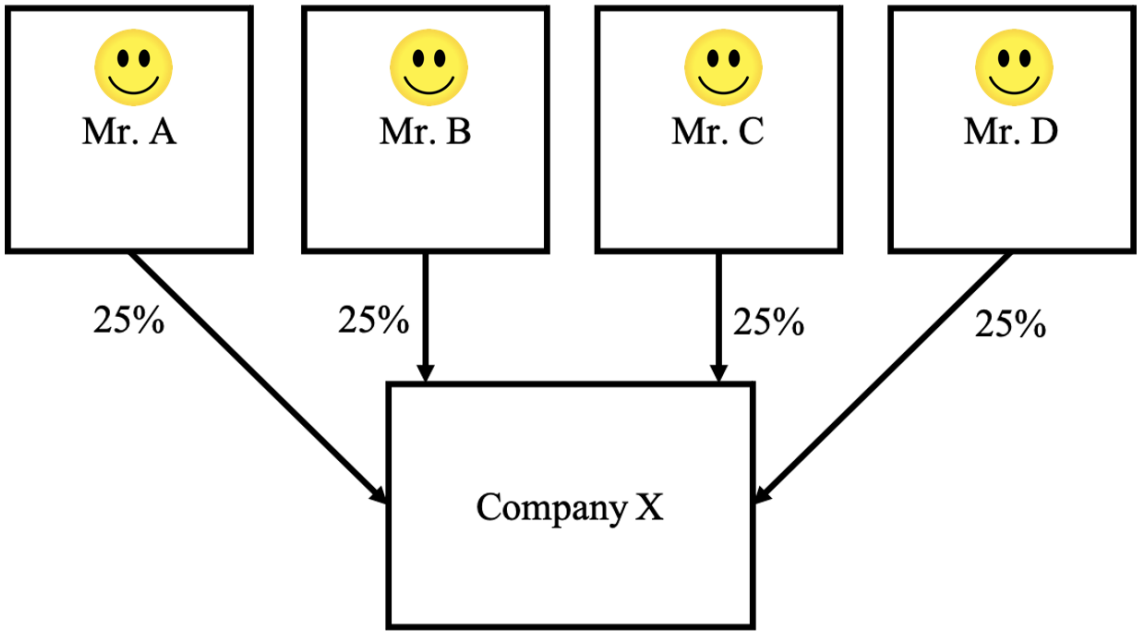
"Owns" means ownership, either directly or indirectly, of 25% or more of a person or unincorporated entity.

Both components should be examined. In other words, once the 25% numerical threshold is reached, that person should be considered a beneficial owner, regardless of whether there is also a *de facto* controlling person. However, the inquiry should not stop there. It should also be determined whether there is any person who exercises actual control, even if owning less than the requisite ownership amount of shares or voting power, and even if a BO can be identified based on share ownership. The rationale for this approach is that while in some cases the BO may appear to be clear based on the ownership structure, in fact there may be a *de facto* controlling person with little or no formal ownership. In order to be certain that all possible means of control have been addressed, this inquiry should be made.

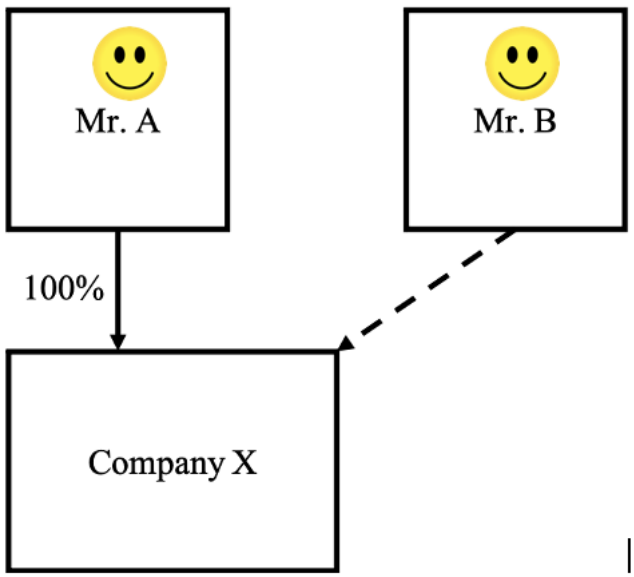
Most of the discussion below will pertain to companies. However, beneficial ownership of cooperatives, partnerships, trusts,[15] non-profit organizations and other legal persons and legal arrangements must also be kept in mind.

In the following simple example, "Mr. A," "Mr. B," "Mr. C" and "Mr. D" are all BOs of Company X, because each of them owns at least 25% of the shares of Company X.

[15] In the case of a trust, according to FATF standards, there is no numerical ownership threshold. A natural person who is a trustee, settlor, protector, and beneficiary of a trust should be considered a BO of the trust.



A person may be a BO under the "control" component while owning few or no shares. The following simple example illustrates this point:



In this example, "Mr. A" owns all of the shares, and holds all of the voting rights, of Company X. However, "Mr. B" makes all of the decisions about Company X. Both Mr. A and Mr. B would be considered BOs of Company X.

It is possible that in some circumstances the same person or persons might be identified pursuant to both the "ownership" and "control" components. For example, in the scenario presented above, if one of the legal owners is an actual controlling person, there would be 4 BOs – the 4 individuals who each own 25% of the company, one of whom would also be the actual "control" person. However, it is also possible that in addition to the four 25% owners,

there could be a different person who has no formal ownership interest, but who exercises real control of the company. In this scenario, there would be as many as 5 persons who would qualify as BOs – the four 25% shareholders, and the person who actually controls the company. This will occur most often in the case of "nominee" shareholders, but could occur in any situation of "*de facto"* or concealed beneficial ownership.

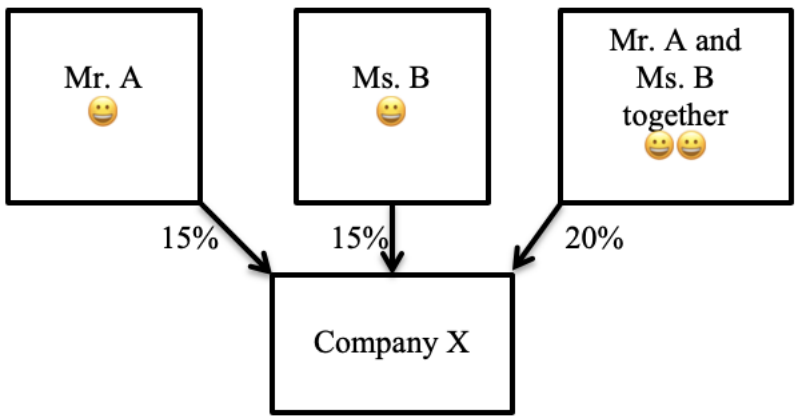
The Ownership Component

The first task is to determine who owns shares in a company. Such ownership may be direct or indirect, i.e., through one or more controlled entities, such as subsidiaries. It includes ownership that is exercised alone or jointly with one or more other persons.

Direct Ownership

Direct ownership refers to actual direct legal ownership of shares of a legal entity. In most companies, this is a fairly straightforward matter. The legal owner(s) will be the person or persons listed as shareholders on the register of members or shareholders. In simpler structures (i.e., with only one layer of ownership), these are likely to be natural or legal persons who hold their shares for themselves. Any such natural person who holds at least 25% of the issued share capital or voting rights would therefore be both the legal owner of the shares and a BO of that company.

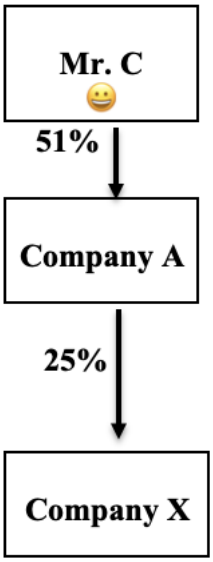
It is important to note that where shares are owned jointly by more than one person, this must be taken into account in determining those persons' total ownership. For example, if two or more shareholders own shares jointly, they are both considered to own all of the shares, and their percentage ownership will include their joint holding and any other shareholding. A simple example follows:



In the above example, shareholders Mr. A and Ms. B are natural persons who each own 15% of Company X in their individual capacities. In addition to their individual holdings, they jointly own 20% of the company. The shares that are owned jointly (here, 20%) are combined with the shares that each of them owns individually (here, 15% each). Mr. A and Ms. B would thus be considered BOs of the company, as each would be the owner of his or her 15% plus the 20% held jointly with the other shareholder (total 35% each).

Indirect Ownership

Indirect ownership refers to ownership that is achieved through one or more controlled enterprises, or through a "chain of ownership." The following example illustrates this.



In the above example, "Mr. C" owns 51% of Company A, which holds 25% of Company X; Mr. C is therefore a beneficial owner of Company X.

A potential problem for DNFBPs is that legal entities sometimes have multiple layers of ownership. DPEs and criminals frequently use this technique to conceal their beneficial ownership of legal entities. The question is how to determine 25% ownership beyond the second level where there are multiple ownership layers. For this purpose, the "**majority stake**" test should be applied.

The Majority Stake Test

The *majority stake* test entails determining whether any person holds shares in a company through one or more entities in which he or she holds a "majority stake," which entails direct or indirect ownership of at least 50% of the voting shares or capital; if so, ownership held by a shareholder is attributed *in full* to any person that holds a majority stake (whether a natural or legal person) in that shareholder.

A person holds a share indirectly if the person has a majority stake in a legal person or legal arrangement and that legal person or legal arrangement:

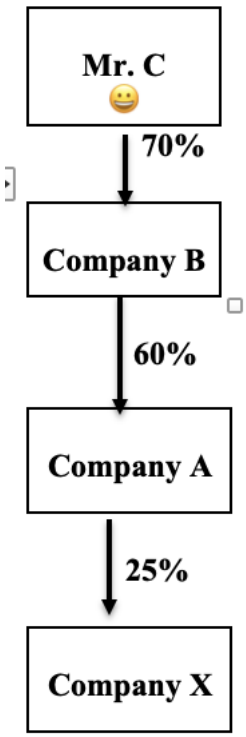
- holds the share in question; or
- is part of a chain of legal persons or legal arrangements:
  - each of which (other than the last) has a majority stake in the legal person or legal arrangement immediately below it in the chain; and
  - the last of which holds the share.

A person holds a right indirectly if the person has a majority stake in a legal person or legal arrangement and that legal person or legal arrangement:

- holds that right; or
- is part of a chain of legal persons or legal arrangements:
  - each of which (other than the last) has a majority stake in the legal person or legal arrangement immediately below it in the chain; and
  - the last of which holds that right.

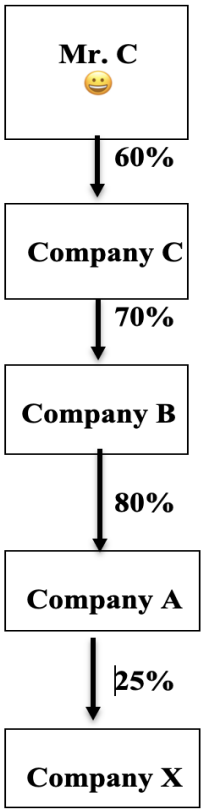
According to this definition, the majority stake test is only applicable where there is an unbroken chain of at least 50% ownership in the chain of legal persons or legal arrangements (other than the one in question). It is important to note that the real focus here is the "second" ownership layer (i.e., the entity that owns at least 50% of the 25% legal entity shareholder of the entity in question).

The following example illustrates how the majority stake test works in practice:



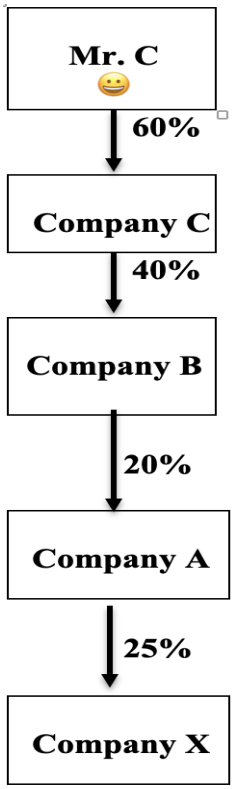
In the above example, "Mr. C" has a majority stake (70%) in Company B, which owns 60% of Company A, which holds 25% of Company X. Mr. C would be considered a BO of Company X.

This same principle applies regardless of how many layers there may be in an ownership chain. For example:



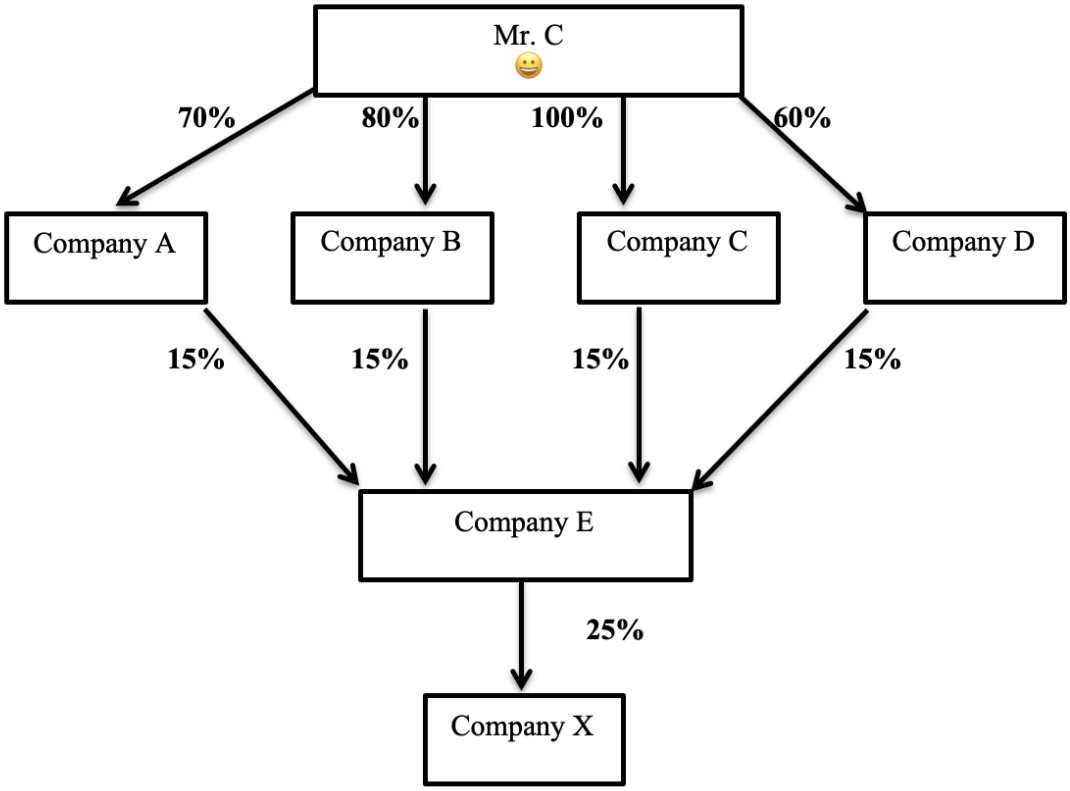
In the above example, “Mr. C” has a majority stake (60%) in Company C, which has a majority stake (70%) in Company B, which owns 80% of Company A, which holds 25% of Company X. Because there is an unbroken chain of majority stakes in the corporate shareholder (Company A) that owns 25% of Company X, Mr. C would be considered a BO of Company X.

The following example shows a different result:



In the above example, "Mr. C" has a majority stake (60%) in Company C, but Company C does not have a majority stake (only 40%) in Company B, the 20% owner of Company A, which holds 25% of Company X. Because there is not an unbroken chain of majority stakes in the Company A, which that owns 25% of Company X, Mr. C would be not considered a BO of Company X based on ownership. Note, however, that Mr. C could still be considered a BO of Company X if he satisfied one of the "control" tests described below.

A person may hold beneficial ownership through multiple entities within an ownership layer. The following example illustrates this point:



In the above example, "Mr. C" has a majority stake in each of 4 companies, each of which holds 15% of Company E, which owns 25% of Company X. Mr. C would thus be considered a BO of Company X: he controls (via his majority stake) 4 companies, which collectively own 60% of Company E, the corporate shareholder of 25% of Company X.

The Multiplication Test

In contrast to the majority stake test, the multiplication technique determines ownership by simply multiplying the ownership percentages.

In the first example in the "majority stake" section above, multiplying the ownership percentages results in "Mr. C" having a 10.5% indirect ownership stake in company X (25% X 60% X 70% = 10.5%). Because the ownership test for BO status is 25%, Mr. C would not be considered a BO of Company X under the "multiplication" test.

However, it is quite clear that Mr. C can, in substance, control how Company A's 25% of Company X's shares are voted: by holding a majority of the shares in Company B, Mr. C can control the composition of Company B's board of directors, which normally would determine how 60% of Company A's shares are voted. Company B can, therefore, control the composition of the board of directors of Company A, which would determine how Company A's shares (here, 25%) of Company X are voted. Stated differently, Mr. C can do, relative to Company X, what a 25% shareholder can do.

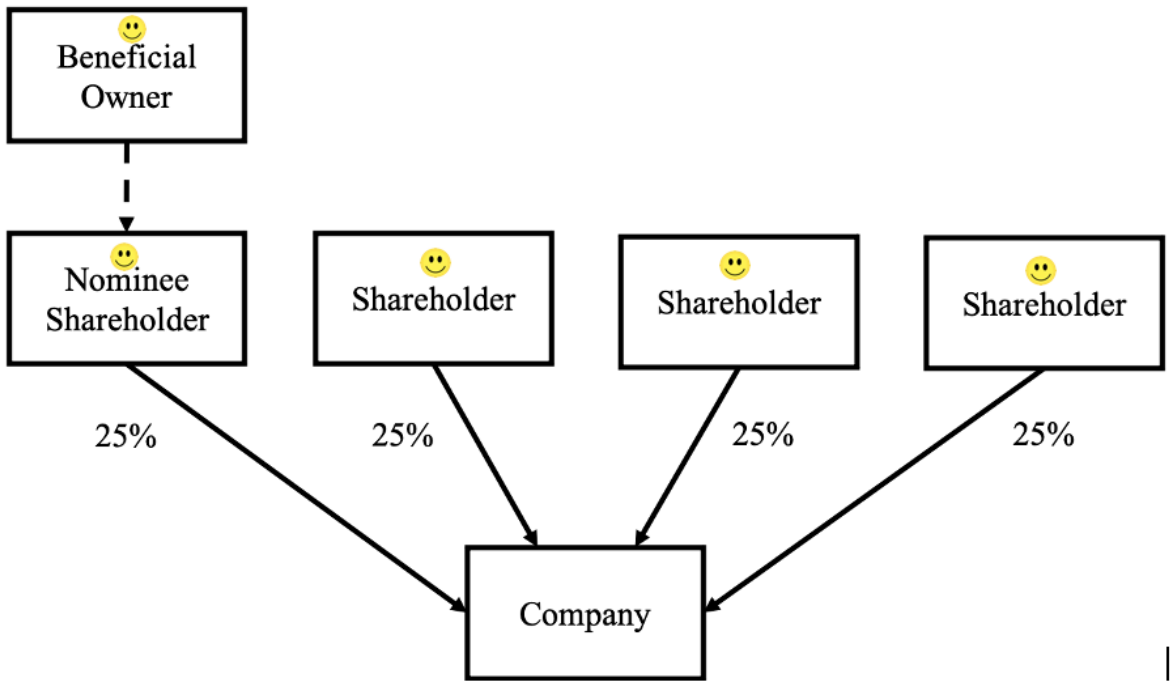
The multiplication test is unsatisfactory by itself for determining BO, as it focuses only on the size of the shareholdings but disregards real ability to effectuate voting rights. However, it can

be useful for those situations where the majority stake test is not applicable due to the lack of an unbroken ownership chain.

Nominee Shareholders

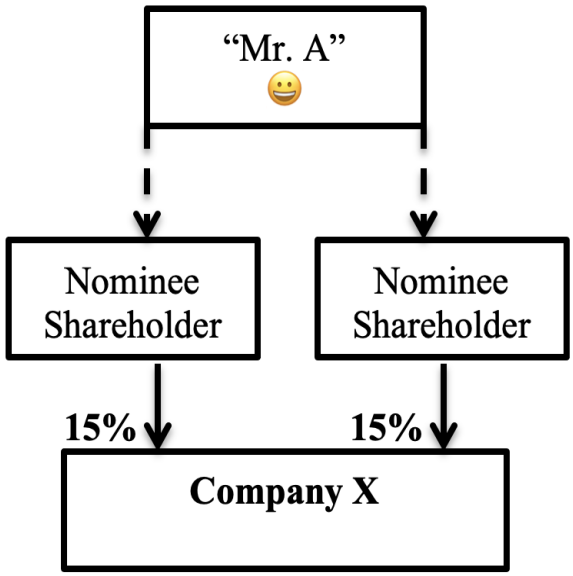
A natural person shareholder might hold shares as "nominee" for another natural person. The legal shareholder may hold the shares in trust for that underlying natural person, or the underlying natural person may simply wish to keep his or her ownership hidden (even if there is no actual trust document, or any other formal contract or agreement). The person holding the shares in this situation is the legal owner and the person for whom they hold the shares is the BO. If that BO holds at least 25% of shares of the company in this manner (either entirely through such an arrangement, or in any combination of legal and beneficial ownership), that person is considered to be a BO of the company.

In the following example, the company has 4 natural person shareholders, 3 of whom hold the shares for themselves, while the fourth holds the shares for someone else. Because all 4 shareholders are legal owners of 25% of the company, they are both legal and beneficial owners. There is also an individual for whom the nominee shareholder holds shares.



In the above example, there are 5 BOs: the 4 "legal" 25% shareholders, and the BO of the shares held by the "nominee" shareholder.

A person might be the BO of a company through more than one nominee shareholder, even if all of the nominee shareholders would not be considered BOs based on their legal ownership. The following simple example illustrates this point. In this example, there are two 15% shareholders who are nominees for "Mr. A," who formally owns no shares in the company at all:



In this example, "Mr. A" must be considered a BO of Company X, because his total beneficial ownership amounts to 30%, despite being held by two different nominee shareholders.

The Control Component

In determining beneficial ownership of a legal person or legal arrangement customer, the DNFBP should look beyond formal (direct or indirect) ownership and should examine ultimate effective control. "Control" of a legal entity or arrangement can be exercised in a number of different ways, including extortion, coercion, or merely through secret agreements between an entity's managers or directors and the actual controlling person.

Examples of ultimate effective control over a legal entity include:

- the power (whether formalized or not) to appoint a majority of the members of the board of directors of the entity, or in the case of a company, the board of directors of a parent company of that company;

- the person's representatives or nominees constitute a majority of the members of the board of directors of the entity, or in the case of a company, the board of directors of a parent company of that company;

- the person has such controlling power pursuant to an agreement with the company, or a provision in the constitutive documents of the company, or in a parent company of that company, such as the charter, articles of association, or any similar document;

- a majority of the members of the board of directors of the company, or of a parent company of that company, or the senior managing official of that company or parent company, are accustomed or under an obligation, whether written or unwritten, formal or informal, to act in accordance with the instructions, directions, or wishes of a given natural person in conducting the affairs of the company; or

- a person makes recommendations to the shareholders or members of the company, or of a parent company of that company, on matters requiring shareholder or member approval, and these recommendations are always or almost always followed by shareholders or members holding at least 25% of the voting rights in that company or parent company, when they are deciding how to vote.

Some persons can exert a considerable degree of influence on a legal entity or arrangement through the provision of professional services. Because of the nature of these relationships, these persons should not be considered to be BOs based on that relationship alone. A BO therefore would not include a natural person in accordance with whose directions, instructions or wishes the directors, partners, or senior managing officials, or persons in equivalent positions of any entity are accustomed to act, or whose recommendations are customarily followed, solely based on advice given by that person in his or her professional capacity. Such persons could include, for example:

- a lawyer;
- an accountant or auditor;
- a management consultant;
- an investment manager;
- a tax adviser; or
- a financial advisor.

Because DNFBPs do not have the same kinds of resources or investigative powers as supervisory or law enforcement authorities, they are not expected to conduct detailed investigations to determine the existence of undisclosed or "secret" beneficial owners. However, they should make inquiries of potential customers at the time of account opening or prior to executing an occasional transaction. For this purpose, it is a good business practice to require each customer, and in particular each legal entity or legal arrangement customer, to verify its BO(s) for each account or prior to carrying out an occasional transaction.

"Acting in Concert"

Both the ownership and control components of the BO concept must consider the possibility that ownership or control can be achieved through persons acting together.[16] FASU Guidance recognizes this by noting that "control" includes control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, where or not having legal or equitable force and whether or not based on legal or equitable rights. In international practice this is often referred to as "acting in concert."

"Acting in concert" generally can be defined as "a conscious course of parallel action taken by two or more persons, in accordance with any agreement, commitment or understanding, whether formal or informal, verbal or written, to act jointly or in combination with each other

[16] FATF Recommendation No. 10, par. 5(b) (referring to persons "acting alone or together" who exercise control of a legal person or arrangement); FATF, *Transparency and Beneficial Ownership* (October 2014), p. 15 (referring to "shareholders who exercise control alone or together with other shareholders, including through any contract, understanding, relationship, intermediary or tiered entity).

with a view toward achievement of a common objective." Persons are often presumed to be acting in concert with each other unless it is shown otherwise. The following are examples of relationships that should be presumed to involve concerted action:

- A legal person should be considered to be acting in concert with a controlling person of that legal person.

- A person should be presumed to be acting in concert with his or her close family members (i.e., spouse, parents, grandparents, children, grandchildren and siblings).

- Legal persons in the same group (i.e., parent, subsidiary and sister companies) should be presumed to be acting in concert with each other.

- Legal persons that are controlled by the same person (legal or natural) should be presumed to be acting in concert with each other.

- Persons should be presumed to be acting in concert with each other relative to a legal person ("Entity A") where -

  – they are both members of the board of directors, senior management officials, or controlling persons of the same legal person other than "Entity A;" or

  – one person provides credit to the other person or is instrumental in obtaining financing for the other person to purchase shares of Entity A (other than a situation where one such person is a financial institution that provided credit to the other person to purchase the shares in the ordinary course of business and holds a security interest in the shares so purchased).

- The trustee of a trust should be presumed to be acting in concert with the trust and with the beneficiaries of the trust.

- Beneficiaries of a trust should be presumed to be acting in concert with the trust and with each other.

- General partners in a partnership should be presumed to be acting in concert with each other and with the partnership.

At the same time, not every situation of persons acting in a similar manner necessarily indicates that those persons are acting in concert. Examples include:

- discussions with each other about possible matters to be raised with their company's board or management;

- making representations to a company's board or management about company policies, practices or particular actions that the company might be considering;

- exercising shareholders' legal rights in the same manner with regard to items such as:

- adding items to the agenda of a general meeting;
- recommending draft resolutions for items included or to be included on the agenda of a general meeting; or
- proposing to call a special meeting, apart from the annual general meeting;

- other than in relation to appointment of members of the board, agreeing to vote in the same way on a particular resolution put to the general shareholders' meeting, such as, for example, votes on proposals regarding:
  - directors' remuneration;
  - an acquisition or disposal of assets;
  - a reduction of capital and/or share buy-back;
  - a capital increase;
  - a dividend distribution;
  - the appointment, removal or remuneration of auditors;
  - the appointment of a special investigator;
  - approval of the company's financial statements;
  - the company's policy in relation to major social or political questions; or
  - approval of related party transactions.

In addition**,** persons need not be presumed to be acting in concert relative to a given entity solely because:

- they both serve as members of the board of directors or senior management officials of that entity;
- one of them is a proxy holder for one or more of the others regarding the voting of shares at an annual or special shareholders' meeting in accordance with applicable securities legislation; or
- they independently exercise voting rights attached to shares or ownership interests in that entity in the same manner.

Where No Beneficial Owner Can Be Identified Based on Ownership

or Control

There may be some cases where no natural person who ultimately owns or exerts control over a legal entity or arrangement can be identified based on the above criteria. In such cases, DNFBPs may consider one or more senior managing officials (such as the Chief Executive Officer) to be the BO(s). This, however, should be done after the DNFBP is satisfied that it has exhausted all other means of identification, and that there are no grounds for suspicion. The DNFBP should keep records of the actions it has taken to identify the beneficial ownership.

Ownership/Control Structure: Legal Entities

For companies with multiple layers in their ownership structures, DNFBPs should take reasonable measures to verify the identity of the BO, and understand the ownership and control structure of that customer. This means, among other things, that any intermediate layers of the company's ownership structure should be fully identified. The manner in which this information is collected should be determined by the DNFBP and incorporated into its policies and procedures. An effective means of doing this is to obtain a declaration from a senior official (such as the chief executive officer or corporate secretary) of the entity incorporating or attaching an ownership chart or organogram clearly showing the ultimate parent company (if any), each intermediate company, and the respective ownership of each company, including the ownership interests of the beneficial owner(s).

The amount and degree of detail of the information to be included should be determined on a risk sensitive basis, but at a minimum should include company name and place of incorporation, and where applicable, the rationale behind the particular structure employed. The objective should always be to follow the chain of ownership and actual effective control "all the way to the top," i.e., to the individuals who are the ultimate BOs of the direct customer, and to verify the identity of those individuals.

It is usually not necessary for DNFBPs to routinely verify the details of the intermediate companies in the ownership structure of a company. Usually the names, locations and type of businesses of the companies, and their respective ownership will be sufficient. However, complex ownership structures (e.g., structures involving multiple layers, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk. In these cases, further steps may be necessary to ensure that the DNFBP is satisfied on reasonable grounds as to the identity of any BOs.

The need to verify the intermediate corporate layers of the ownership structure of a company will therefore necessarily depend upon the DNFBP's overall understanding of the structure, its assessment of the risks and whether the information available is adequate in the circumstances for the DNFBP to consider if it has taken adequate measures to identify the BOs.