GUIDANCE NOTES (AMENDMENTS) ON THE PREVENTION AND DETECTION OF MONEY LAUNDERING AND TERRORIST FINANCING IN THE CAYMAN ISLANDS

Section 14

COUNTER PROLIFERATION FINANCING

A. APPLICABILITY

1. This section of the Guidance Notes applies to all financial services providers in the Cayman Islands. Moreover, this section applies to any entity conducting insurance business, regardless of whether the entity carries on long-term or general insurance business. This section also applies to trust and corporate services providers and Designated Non-Financial Businesses and Professionals that provide services to shipping and freight forwarding business, import/export business activity, and clients in jurisdictions near sanctioned countries.

B. PROLIFERATION AND PROLIFERATION FINANCING

1. Proliferation is the manufacture, acquisition, possession, developing, export, transhipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. It includes technology, goods, software, services and expertise.

2. Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, to make proliferation possible. In other words, it is the financing of the proliferation activities described above.

3. Proliferation financing refers to more than simply the payment for goods and includes any financial service provided in support of any part of the procurement process (even if it is not directly connected to the physical flow of goods). Financing can include financial transfers, mortgages, credit lines, insurance services, middlemen services, trust and corporate services and company formation.

4. Proliferation financing facilitates the movement and development of proliferation-sensitive goods. The movement and development of such items poses a risk to global security and stability and may ultimately result in loss of life.

5. While the Cayman Islands has not encountered any direct acts of terrorism or proliferation to date, the risk of proliferation still exists given the size and breadth of the Cayman Islands' financial system as well as the increasingly novel and sophisticated methods, vehicles and jurisdictions used by proliferators in an attempt to escape sanctions imposed against them.

6. This section of the Guidance Notes seeks to assist financial services providers in identifying the proliferation financing risks and vulnerabilities to which they are exposed and also in the development of their systems and controls to prevent, detect and report proliferation financing.

C. INTERNATIONAL FRAMEWORK

1. The United Nations has passed three resolutions relating to anti-proliferation. Two resolutions are country specific, relating to North Korea (DPRK) and to Iran. These UN resolutions are in force in the Cayman Islands via Orders passed in the United Kingdom, namely The Iran (Restrictive Measures) (Overseas Territories) Order 2012 and the North Korea (United Nations Measures) (Overseas Territories) Order 2006.

2. The third resolution is global in nature (non-country specific). UN Security Council Resolution 1540 seeks to prevent non-State actors from obtaining weapons of mass destruction. It establishes binding obligation on member states to:

   (1) Prohibit support to non-state actors seeking weapons of mass destruction, their means of delivery and related materials
   (2) Adopt and enforce effective laws prohibiting the proliferation of such items to non-state actors, and prohibiting assisting or financing such proliferation; and
   (3) to take and enforce effective measures to control these items, in order to prevent their proliferation, as well as to control the provision of funds and services that contribute to proliferation.

3. The United Kingdom extends these resolutions to the Cayman Islands via overseas territories Orders.

D. DOMESTIC LEGISLATION

1. The Proliferation Financing (Prohibition) Law, 2017 makes it an offence for any person to provide funds and economic resources to fund unauthorised proliferation activities, or to enter into or become concerned in an arrangement which that person knows or suspects facilitates the acquisition, retention, use or control of funds and economic resources to fund unauthorised proliferation activities.

2. A person who acts in the course of a business in the financial sector may be committing an offence, even if the offence takes place wholly or partly outside the Islands.

E. HOW PROLIFERATION FINANCING DIFFERS FROM MONEY LAUNDERING

1. Proliferators operate globally, try to mask their activities as legitimate trade and exploit global commerce by trading in countries with weak export controls or free trade zones.

2. The stages of proliferation financing differ from the placement-layering-integration cycle associated with money laundering. Rather, the pattern used by proliferators is a linear Raise – Obscure – Procure & Ship.

3. During the Raise stage funds are raised from overseas criminal activities, state budgets and overseas commercial enterprises.

4. During the second stage of proliferation financing, proliferators rely on extensive networks of businesses (including front companies) and middlemen to obscure any connection on paper to sanctioned countries. Countries use opaque ownership structures for evading sanctions lists. Often proliferation financing involves companies in or near a sanctioned country and accounts under the control of a foreign national (i.e. not Iranian or a North Korean national) with sympathies to the sanctioned country. This, combined with the use of false documentation, allows proliferators to avoid detection. However, studying previous proliferation financing cases and typologies can allow FSPs to gain a better understanding of these networks.

5. The Procure & Ship stage involves expenses associated with brokers, shippers, freight forwarders, insurance coverage, for goods and technology that is intended to be delivered to conduit countries for final entry into a sanctioned country. It is important to note that proliferation involves not only the purchase of weapons but also of individual goods and component parts that can be used to develop weapons or missiles. This makes proliferation activities more difficult to detect.

6. Also, unlike money laundering, which is concerned about funds raised by illegitimate means, the source of funds used to finance proliferation can be both legal and illegal. The destination or use of those funds is for advancing the ambitions of sanctioned states. In many cases the financing source is from a state or a person acting as an indirect agent of the state.

7. As such, while some risk indicators and control elements might overlap for money laundering and proliferation financing, proliferation financing also has its own unique risk indicators and associated controls that financial institutions should implement.

Table 1: Comparison of Proliferation Financing to Money Laundering and Terrorist Financing

	Money Laundering	**Terrorist Financing**	**Proliferation Financing**
Flow of Funds	Circular – money eventually ends up with the person that generated it	Linear – money generated is to propagate terrorist groups and activities	Linear – money is used to purchase goods and parts, technology from brokers and manufacturers. Shipping and insurance also part of money trail
Conduits	Favours formal financial system	Favours cash couriers or informal systems such as hawala	Favours formal financial system

		and currency exchange firms	
Detection Focus	Suspicious transactions deposits uncharacteristic of customer's or the expected activity	Suspicious relationships, such as wire transfers to seemingly unrelated parties	Goods and materials, activities, countries, individuals
Transaction Amounts	Large, but often structured to avoid reporting requirements	Small usually below reporting thresholds	Moderate amounts – transactions appear legitimate with transaction profile
Financial Activity	Complex web of transactions often involving shell or front companies, bearer shares and countries with lax financial services regulation	Varied methods, including formal banking system, informal value transfer systems, smuggling of cash and valuables	Transactions look like normal commercial activity, structured to hide origin of funding

F. DUAL USE GOODS AND EXPORT CONTROLS

1. Proliferation financing is often associated with trade in dual use goods. Dual-use goods are items that have both commercial and military or proliferation applications. These goods could be components of a weapon or machines to manufacture a weapon that also have civilian applications (for example, certain tools that can be used to repair vehicles). Even if some goods do not appear on export control lists, they are still subject to restrictions if their end use is for illicit proliferation purposes. Dual-use goods can be identified from lists produced by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

G. CHALLENGES OF IDENTIFYING PROLIFERATION FINANCING

1. While the United Nations and several national governments have issued lists of designated persons and entities known to be associated with proliferation, sole reliance on screening against those lists might not always be effective, as they do not cover the full extent of proliferation networks and proliferation activity. Proliferators try to engage new persons or form new entities with different managers and directors to carry out transactions on their behalf. Proliferators also use several transhipment points before goods reach their target destination.

2. Proliferation financing tends to be directed by state actors, who develop their own networks and distinct ways of accessing the financial system. FSPs should be aware that proliferation networks and methods will vary from country to country. Conversely, proliferation networks from the same country tend to behave similarly.

3. Finally, illicit proliferation can include procurement of illicit materials by a sanctioned country as well as a sanctioned country that provides sensitive goods to other countries.

H. OBLIGATIONS OF FINANCIAL SERVICES PROVIDERS

1. FSPs must carry out appropriate CDD on their clients, which includes screening names of clients and clients' counterparties, including shipping companies, beneficiaries of letters of credit and freight companies, against sanctions lists. However, that is not enough, as the names of entities or individuals on sanctions lists rarely appear in financial transactions. In addition, on paper, a transaction is rarely directly connected to a sanctioned country.

2. Therefore, in addition to screening, FSPs must also implement risk-based systems and controls to detect proliferation financing. FSPs should carry out a risk assessment to determine their exposure to proliferation financing risk. The risk assessment should consider risks relating to geography, customers and products and services.

Customers

3. FSPs should determine the exposure of their clients to the manufacture, trade or provision of expertise or consulting services relating to sensitive or dual use goods or technology. Conversely, given the potential difficulties of identifying clients that are involved with sensitive goods and technology, FSPs should identify the clients that pose a smaller risk of proliferation financing and concentrate on gathering more information from the customers that remain.

4. FSPs and DNFBPs should also be aware of the transactions of their clients, particularly paying attention to payments being made to importers /exporters, shipping agents, brokers and freight forwarders, especially where controlled and dual use goods are being shipped to conduit countries (those near sanctioned countries).

Geography

5. The FSP should determine its level of business (including customers and beneficial owners) with sanctioned countries as well as with countries that are known to have ties with sanctioned countries (e.g. China, Hong Kong, Singapore and Malaysia). The FSP should remain informed about the countries that present a higher risk for proliferation financing.

6. The FSP should identify its business relationships, including correspondent banking relationships, with partners and financial services providers located in the above noted jurisdictions.

7. The FSP should identify clients with payments to importers / exporters, shipping agents, brokers, and freight forwarders that export to countries and ports near the border of sanctioned countries. For example, shipments of prohibited goods to the Democratic People's Republic of Korea (North Korea) are often marked as destined to Dangdong, China, and other nearby ports.

8. Shipments and freight forwarding destined to Iran could be labelled as being shipped to bordering countries such as Turkey, Turkmenistan, Afghanistan, Pakistan, United Arab Emirates, Oman, Qatar, Bahrain, Saudi Arabia, Kuwait, Iraq, Syria and Lebanon, and Syria.

Products and Services

9. Shipping insurance and insurance against certain risks in the trading process is a financial product that is highly sought by proliferators. FSPs that offer this type of insurance should be particularly aware of their exposures to proliferation.

10. Proliferators use trade finance to assist with the procurement and movement of goods. FSPs should determine the amount of business they conduct in loans or credit facilities to facilitate export transactions, purchasing promissory notes or bills of exchange from foreign banks to exporters, purchase of discounted foreign accounts receivable and provisions of guarantees to or on behalf of exporters.

11. FSPs should consider whether they provide loans, project financing or credit to clients in sensitive industries or to entities in higher risk jurisdictions. FSPs should note that loan repayments for these facilities may be made from corporate structures associated or linked to jurisdictions near, but not necessarily in, Iran and North Korea.

Controls and Ongoing Monitoring

12. Each FSP should implement risk-based anti-proliferation and proliferation financing policies and procedures, comparable to international standards. This should include detailed internal escalation and external reporting procedures.

13. FSPs procedures should include the use of software to screen all incoming and outgoing transactions against lists of entities and persons designated under international sanctions regimes.

14. In addition to sanctions lists, United Nations Panel of Experts reports contain names of entities and individuals involved in proliferation activities, as well as other identifying information, including addresses, names of directors, email addresses and telephone numbers. FSPs can check whether any of their clients share any of these contact details.

15. FSPs KYD and CDD frameworks should include factors relevant to proliferation financing activity. FSPs must understand the nature of their clients' business, and the clients and jurisdictions with which they trade or where they operate. FSPs should be aware of clients who are either sellers or manufacturers of proliferation sensitive goods and technology. FSPs should understand their clients' trade patterns and suppliers and buyers. FSPs should conduct ongoing monitoring of client accounts to ensure the account remains used for the originally stated purpose and to detect unusual activities.

16. Each FSP should conduct training on countering proliferation financing for relevant staff. The training should be commensurate with the staff members' role in the FSP in the identification or processing of suspicious transactions.

17. FSPs should familiarize themselves with export control lists. When applicable and possible, FSPs, particularly those facilitating trade finance, should screen for any clients' involvement with dual-use goods and technology. FSPs might need to request specific information from clients about certain transactions that involve goods being shipped. Many goods that are considered controlled or sensitive are listed in international export control regimes.

18. In higher risk scenarios, where a customer is importing or exporting goods, FSPs should be alert against proliferation financing. FSPs should ask the customer to provide

valid export licenses or letter from official sources stating that a license is not required, or other proof that a license is not required (e.g. legislation).

I. FREEZING AND REPORTING OBLIGATION

1. The Proliferation Financing (Prohibition) Law requires that any person that has in its possession, custody or control, any funds or economic resources that relate to a designated person to immediately freeze such funds and resources and ensure that no funds or resources are made available for the benefit of the designated person.

2. In addition, any person must, as soon as reasonably practicable, disclose to the Financial Reporting Authority, using the form issued for that purpose, details of any frozen funds or economic resources or actions taken in compliance with the with the prohibition requirements of the relevant Security Council measures. This includes attempted transactions.

3. Any person who fails to comply with the freezing and reporting requirement faces civil penalties and criminal prosecution.

J. RED FLAGS

1. The presence of a single red flag by itself may not automatically make a transaction suspicious. However, a combination of a red flags with other indicators might warrant the FSP to conduct a deeper investigation.

Geographical Factors

2. Transactions involve foreign country of proliferation concern (i.e. Iran and North Korea) or country of diversion concern (e.g. China, particularly Liaoning and Jilin provinces, Hong Kong, Singapore and Malaysia).

3. Transactions include countries that are known to trade with North Korea (including Syria, Egypt, the United Arab Emirates, Yemen and Iran).

4. Trade finance transaction shipment route through jurisdiction with weak export control laws or enforcement or involves entities located in jurisdiction with weak export control laws or enforcement.

5. Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. goods are shipped through several countries for no apparent reason).

6. Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped (e.g. improbably goods, origins, quantities, destinations).

7. Transaction involves financial institutions with known deficiencies in AML/CFT controls or located in weak export control and enforcement jurisdiction. For example, it is known that North Korea has used correspondent accounts held with Chinese banks to facilitate its international financial transfers.

Documentation Supporting the Transaction

8. Based on the documentation obtained in the transaction, the declared value of shipment was obviously under-valued vis-à-vis shipment cost (e.g. the transaction makes little financial sense for the seller or the buyer).
9. Inconsistencies between information contained in trade documents and financial flows (e.g. names, addresses, destinations, descriptions of goods), or changes in shipment location or goods shipped.

10. Freight forwarding company listed as final destination.

11. Obvious alterations to third party documents or the documentation appears illogical, altered, fraudulent or is absent.

Customers

12. Customer is involved in the supply, sale, delivery or purchase of dual use goods, or is a military or research body connected with a high risk jurisdiction.

13. Customer activity does not match business profile or end-user information does not match end-user profile. A customer engages in a transaction that lacks business sense or strategy, or that is inconsistent with historical pattern of trade activity.

14. Order for goods placed by person in foreign country other than the country of the stated end-user.

15. New customer requests letter of credit while awaiting opening of account.

16. Customer vague or inconsistent in information it provides, resistant to providing additional information when queried.

17. The customer or counterparty or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions.

Transaction Structure

18. Transaction concerns dual-use goods or military goods.

19. Transaction demonstrates links between representatives of companies exchanging goods (e.g. same owner or management or same address or providing a residential address or address of registered agent).

20. Transaction involves possible shell companies.

21. Wire transfer or payment from or due to parties not identified on the original letter of credit or other information, or the transaction involves an unusual intermediary, or payment to be made to a beneficiary in a country other than the beneficiary's stated location.

22. Pattern of wire transfers or payment activity that shows unusual patterns or has no apparent purpose, or payment instructions are illogical or contain last minute changes.

23. Circuitous route of shipment and/or circuitous route of financial transactions. Transaction structure (whether shipping route, financing arrangement or documentation) appears unnecessarily complex.