

# **PROLIFERATION FINANCING**

**A guide to compliance**

---

**Requirements for money  
laundering regulated entities**



## TABLE OF CONTENTS

<b>Legislative background</b>	<b>3</b>
<b>Who is required to comply?</b>	<b>4</b>
<b>What is proliferation financing?</b>	<b>5</b>
How is proliferation financing different from money laundering or sanctions?	6
Stages of PF	7
Stage 1 - Raising of funds	7
Stage 2 - Obscuring of funds	7
Stage 3 - Procurement and shipping of goods and technology	7
<b>How can proliferation financing occur?</b>	<b>8</b>
Direct proliferation financing	8
Insuring a North Korean ship	8
Covering up Iranian procurement	9
Lessons from these cases	10
<b>Preventing proliferation</b>	<b>11</b>
<b>The risk of state actors</b>	<b>12</b>
<b>North Korean risks factors</b>	<b>13</b>
<b>Iranian risk factors</b>	<b>15</b>
<b>Key proliferation financing risks in the UK</b>	<b>16</b>
Payments linked to proliferation	16
Maritime and insurance	16
Ease of establishing companies in the UK	17
Low awareness of PF	18
UK Crown Dependencies and Overseas Territories	18
Cryptocurrencies	19

Global defence manufacturing	19
Education and research sectors	20
<b>How to counter proliferation financing</b>	<b>21</b>
Good practice	21
Poor practice	21
<b>Proliferation financing red flags</b>	<b>22</b>
Customer profile	22
Account and transaction activity	22
Trade finance	23
Maritime sector	23
Other red flags	24
<b>What to do now</b>	<b>25</b>
<b>Glossary</b>	<b>26</b>
<b>VinciWorks AML onboarding solution</b>	<b>28</b>
<b>Contact us</b>	<b>30</b>

## Legislative Background

A series of amendments to the UK Money Laundering Regulations 2017 came into force 1 September 2022. The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022 include an obligation for regulated entities to identify, assess and mitigate the risk of proliferation financing (PF).

Regulated entities have the flexibility to create a new risk assessment on PF, or to incorporate proliferation financing into their existing money laundering and terrorist financing risk assessments.

The Treasury will conduct a national risk assessment in relation to proliferation financing, and regulated persons will also be required to take appropriate steps to identify and assess the risks to which their business is subject, and to establish and maintain policies, controls and procedures to mitigate and manage these effectively.

Recommendation 7 of the FATF Standards requires countries to implement proliferation financing-related Targeted Financial Sanctions (TFS) made under United Nations Security Council Resolutions.

Recommendation 2 requires countries to put in place effective national cooperation and, where appropriate, coordination mechanisms to combat the financing of proliferation of weapons of mass destruction (WMD). Immediate Outcome 11 and certain elements of Immediate Outcome 1 relating to national cooperation and coordination aim to measure how effective countries are implementing these Recommendations.



## Who is required to comply?

According to FATF standards, all persons which are regulated entities, including credit institutions, financial institutions, estate agents and others, will be required to assess their PF risks. This includes sectors which are likely to pose a low proliferation financing risk. Relevant supervisors are likely to produce sector-specific guidance in coordination with the Treasury.



## What is proliferation financing?

Proliferation financing is defined by the FATF as the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials, including both technologies and dual-use goods used for non-legitimate purposes.

It can be described as providing financial services and products for the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials. It involves the financing of trade in proliferation sensitive goods, but could also include other financial support. In many cases, PF activity has the sole aim of generating access to foreign currency and the international financial system. It may look like a legitimate trading transaction.

In complex structures PF may

not necessarily be directly connected to the physical flow of goods. For example, PF can include:

- Financial transfers
- Provision of loans
- Ship mortgages and registration fees
- Insurance and re-insurance services
- Credit lines for shipment of illicit sensitive goods
- Trust and corporate services
- Acting as an agent for, to, or on behalf of someone else
- Facilitation of any of the above.

A key focus on preventing the threats posed by Proliferation Financing is the strict implementation of the sanctions regime on North Korea and Iran, as well as preventing chemical weapons activity.

Sanctions laws apply to all businesses. Any business who breaches a UK sanctions regime could be fined or subject to criminal prosecution. Breaching sanctions was recently made a strict liability offence, meaning a

business only has to have breached the law to be liable for a penalty, there is no requirement for intent.

## How is proliferation financing different from money laundering or sanctions?

PF can be described as both a distinct financial crime risk and a sanctions risk. It may share certain characteristics with other forms of financial crime, such as money laundering and terrorist financing.

PF tends to be more linear than money laundering or terrorist financing. Funds are used to purchase materials and goods. However PF threats are typically posed by proliferation networks, which are created by states targeted by UN resolutions or international sanctions. Their financing needs and approaches may not be the same as other criminal actors, as the ultimate goal is not to turn ill-gotten assets into legitimate-seeming funds, or to finance specific terrorist attacks, but to bring restricted goods or cash into certain states, i.e., Iran and North Korea, and use those state assets to enable the proliferation of

weapons of mass destruction. The number of customers or transactions related to proliferation activities is likely to be smaller than those involved in other types of financial crime. Predicate offences and criminal actors are relevant considerations for PF, but the complex nature of PF means that the range of possible threats is broader than in considering money laundering or terrorist financing in isolation.

Since PF networks may derive funds from both criminal activity and / or legitimately sourced funds, transactions related to PF may use the international financial system under the umbrella of legitimate business and may not exhibit the same characteristics as traditional money laundering or terrorist financing.



## Stages of PF

Stage 1 - Raising of funds



Stage 2 - Obscuring of funds



Stage 3 - Procurement and shipping of goods and technology

### Stage 1 - raising of funds

Initially, financing can be sourced from both legitimate and illegitimate activities raising funds or obtaining foreign exchange. This can include trading or procuring dual-use goods or trade in natural resources, illegal export of coal, sand, oil, the smuggling of oil and gold, cyber-attacks, crypto raids, drug trafficking, weapons export and more.

### Stage 2 - obscuring of funds

Entities or states undertaking proliferation techniques may use highly sophisticated means to obscure the source of funds to inject money into the international financial system. This is done, for example, via the

use of opaque ownership structures or management, use of false documentation, middlemen, or front companies, i.e., companies that appear to undertake legitimate business but which, in reality, are serving to obscure illicit financial activity.

### Stage 3 - Procurement and shipping of goods and technology

Procurement and shipping of goods and technology is the final stage where the proliferator pays for goods, materials, technology, and logistics needed for their WMD programme. The final stage will involve international financial institutions processing the related transactions.



## How can proliferation financing occur?

Because proliferation financing is a financial crime, it can affect any business. In fact, those involved in PF are more likely to target smaller companies or those with less robust procedures.

### Direct proliferation financing

The direct procurement of dual-use items for proliferation activities normally involves a procurement network seeking to export controlled items to a high risk jurisdiction.

The UK is a major arms manufacturer and producer of dual-use items, including nuclear-related material, so the risk is high.

Many UK industrial sectors can be procurement targets. Everyday goods that often have innocent purposes can be used in proliferation. UK-manufactured electronic components were found in the debris of a 2012 North Korean missile test. Some high-risk

goods include:

- Carbon fibres
- Vacuum pumps
- Electronic components
- Testing equipment
- Flame retardant

Proliferation financing can also occur by those evading sanctions regimes and export controls. There are often cases where indirect methods are used to fund proliferation. The use of front companies is prominent in PF cases. There are usually networks of companies designed to obscure the origin of financing.

### Case study: Insuring a North Korean ship

A UK-based specialist underwriter was provided with a re-insurance policy for a vessel which had links to North Korea. This was presented through a subsidiary based in a third country, and the underwriter provided cover for an insurer in that third country, who in turn insured the vessel.

After it was insured, both the vessel and the owning company were designated by the UN and UK sanctions regimes for involvement in ship-to-ship petroleum transfers with a North Korean flagged vessel. The underwriter was informed of the sanctions breach, cancelled the policy and notified the OFSI.

Because the insurance policy was provided prior to the application of international sanctions, the policy was then cancelled and no premiums were received afterwards, so no sanctions breach occurred. The underwriter was urged to freeze any designated entity premium payments received in the future, however.

Had the insurance policy not been quickly cancelled, it would have posed a serious proliferation financing risk. This is due to the fact the UK underwriter would have facilitated the transport of proliferation-sensitive items and materials, thereby generating funds for the North Korean regime and furthering proliferation.

The business could have faced a range of penalties, including a monetary penalty of up to £1m or 50% of the value of the breach, whichever was higher.

### Case study: Covering up Iranian procurement

A UK national was successfully prosecuted for their involvement in the purchase of US and Russian aircraft parts for Iran. The UK national worked for a Singaporean company which procured aircraft parts from the US, imported them to Singapore and diverted the goods to Iran.

The company directors were indicted, and one was prosecuted and jailed in the US. But the UK national subsequently set up front companies in the UK, UAE, Malaysia and the British Virgin Islands to re-establish the illicit procurement network.

The UK company was the ultimate beneficiary through payments made from a Cypriot bank account opened by the British Virgin Islands based company. The Malaysian entity then exported the aircraft parts

from Malaysia to Iran. The Iranian entities were subject to UN and EU sanctions, and the payments were made through third party Iranian entities via money exchanges in several Middle Eastern countries, before the funds were then sent to Malaysia.

## Lessons from these cases

Procurement financing is as complex and involved as many other types of financial crime and money laundering. Actors will take extensive steps to obscure their activities and ownership, and will manipulate the financial system and legitimate businesses in order to further the proliferation of weapons of mass destruction.



## Preventing proliferation

The UK sanctions regime is designed to combat the threat posed by proliferation financing. The main sanctions regimes related to PF are:

- Sanctions on North Korea
- Sanctions on Iran
- Sanctions to prevent chemical weapons proliferation
- Sanctions on military and dual use items

There is a wide array of specific rules under these sanctions regimes. These should be consulted or reviewed in any PF risk assessment.

It is also critical for sanctions compliance policies and resources to be consulted in any PF risk assessment. It is not only AML procedures which may have to change, but sanctions compliance ones as well.

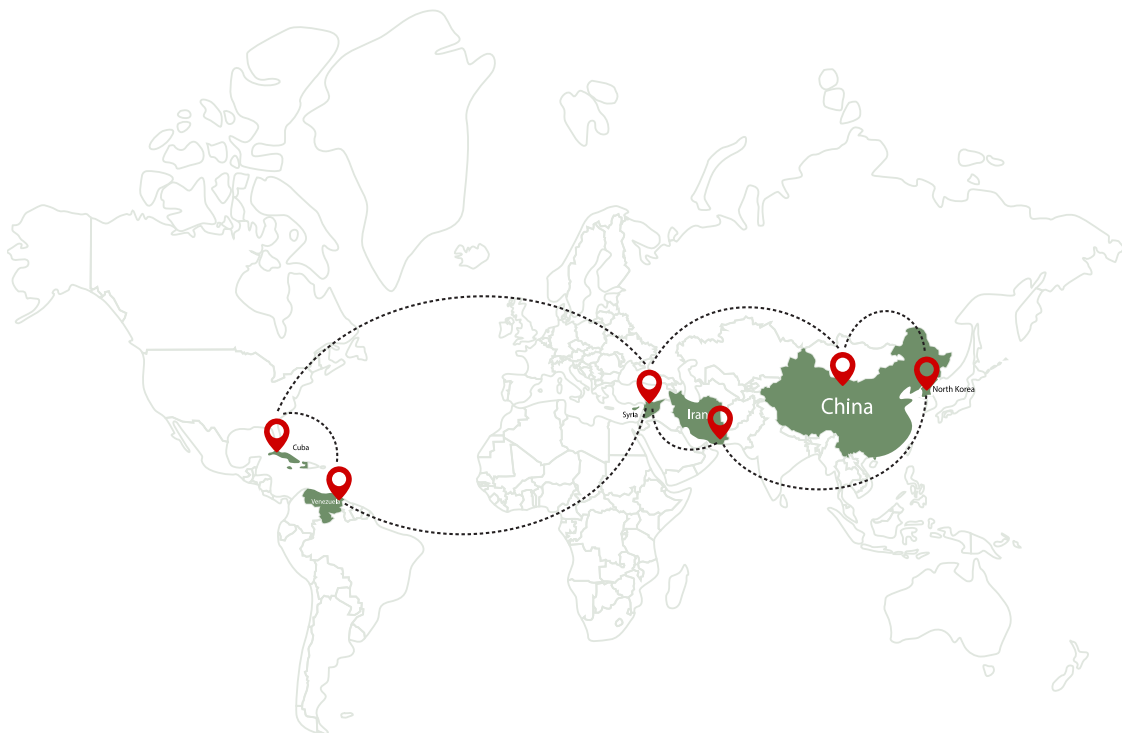
This is particularly relevant for those regulated entities who may be providing professional services for higher risk business, such as exporters and manufacturers



## The risk of state actors

Within proliferation financing, state actors pose a particular risk as they have featured prominently as key actors impacting the UK. Ultimately, state actors are the final beneficiaries of PF, as they are aiming to secure weapons of mass destruction for their regimes in violation of international law and in order to commit atrocities.

State actors may not only involve North Korea and Iran, however. Chinese state actors have been known to play a key role in PF, as have state actors aligned with the Iranian and North Korean regimes, such as Syria, Cuba, Venezuela, or other sanctioned countries.



## North Korean risks factors

North Korea is the primary state actor in proliferation financing, and given the UK's role in the global financial system, this increases the threat to the UK from North Korean-affiliated proliferating actors.

### **North Korean diplomatic staff**

North Korean embassies and diplomatic staff have been known to actively engage in proliferation finance activities. They seek to generate revenue through extra-diplomatic means and identify business opportunities for North Korean entities and assist them in accessing the financial system in violation of UN sanctions. North Korean diplomatic property and privileges, such as using diplomatic bags to move cash and goods, is known to have been used in proliferation financing.

The UK hosts a North Korean embassy in London which poses a threat, particularly to the UK banking system.

### **Presence of North Korean workers**

North Korean workers in a country or business pose a direct PF threat. North Korean nationals working in Malaysia exploited their visa status to raise revenue for the regime and transport goods to the country.

UN resolutions ban North Korean workers in other countries and require repatriation by December 2019, which has not been fully complied with.

The UK does not host any North Korean workers, but the presence of North Korean nationals in the UK, such as those on student visas, may present opportunities for raising revenue for the North Korean regime.

### **Trade in luxury goods**

North Korea is generally prohibited from importing or exporting luxury goods, unless a specific exemption applies. Luxury goods may be resold to favoured members of the

regime, generating revenue which can be used for proliferation. Luxury goods may be resold to favoured members of the regime, generating revenue which can be used for proliferation. Luxury goods also serve as a form of patronage and enable the continuation of elite networks within the country, further serving the regime.

The UK is a potential source of luxury goods to North Korea.

## **Ship-to-ship transfers**

There are multiple cases of documented ship-to-ship transfers carried out in Chinese jurisdiction. There are hundreds of cases of shipments of coal from North Korea to China, and a series of large-scale sand extraction activities carried out by vessels in North Korea, which is then transferred to China.

There are satellite images of vessels owned by UK registered entities or which had previous links to UK entities, taking on cargo at coal facilities in North Korean ports, then transporting them to foreign jurisdiction.

The supply, sale or transfer of coal and sand from North Korea is explicitly prohibited by UN Security Council resolutions, nonetheless, North Korean coal exports remain one of the regime's most effective means of raising finances for its nuclear programmes.



## Iranian risk factors

Trade with Iran is not expressly illegal, but there are a range of financial and other sanctions on Iran. Facilitating payments for UK exporters to export goods to Iran, or any financial transaction which involves an Iranian entity, will have some level of risk.

US sanctions on Iran are considerably more widespread than UK, EU or UN sanctions. Many UK entities have US exposure, which can bring them under the scope of the extensive US sanctions regime.

The Iranian economy is generally seen as opaque, and there are significant illicit financing risks, including money laundering, terrorist financing, as well as proliferation financing. Hence Iran is on the FATF's list of high risk jurisdictions. There are considerable risks and financial costs for UK companies looking to operate in Iran.

There have been instances of Iranian individuals with UK bank accounts receiving payments from unrelated individuals outside of the UK, with those payments then being made to a UK company from the UK account, thus obscuring their origins.

Oil and petrochemical export, particularly to China and Syria, creates significant proliferation financing income for Iran.





## Key proliferation financing risks in the UK

The attractiveness of London for foreign investors and the size and scope of the UK's financial services and professional services centres makes the UK a prime target for proliferation financing. The UK's significant economic role means businesses are more at risk, despite the lack of geographic proximity.

### Payments linked to proliferation

Actors may interact with the UK financial system and overseas branches may interact with the UK, including through subsidiaries of UK-headquartered financial institutions. Most of these financial institutions have a wide international reach, including countries particularly exposed to PF networks or involved in trade with those countries.

Local branches of UK-headquartered banks may facilitate access to financial services for proliferation actors either directly through links to national banks, or insufficient

compliance controls.

Even if proliferation-sensitive items or goods are not directly shipped to or from the UK, the financial transactions to enable this may be facilitated through the UK, purchased, paid, or insured.

### Maritime and insurance

London is a global hub for maritime insurance products. The most significant PF risk is re-insurance into London, particularly when the primary insurer is located in Asia. This is similar to the correspondent banking risk as the UK insurance provider is removed from the original underwriting process. Therefore they will have reduced awareness of due diligence and sanctions screening conducted by the primary insurer.

UK insurers often rely on sanctions clauses which retroactively halt insurance services if a vessel is found to have been involved in sanctioned activities. However this is largely

reliant on information provided by the customer, and it may not always be possible to proactively investigate shipments.

The general size and scope of the maritime sector in the UK, and the fact the maritime sector is frequently targeted by PF actors, makes this industry particularly vulnerable. Over 95% of UK imports and exports are moved by sea, with the sector contributing £14bn to the UK economy.

The maritime risks include:

- Carriers clandestinely shipping prohibited items
- Insurance or re-insurance from UK-based providers
- Insurance for illicit businesses conducted in third countries for procurement of defence materials
- Marine insurance for oil and gas carriers used by sanctioned destinations

### Ease of establishing companies in the UK

Registration of a corporate entity in the UK can be seen as a green flag for companies aiming to access the UK financial system, and could enable proliferation-linked companies access. This

creates a front for companies to carry out illicit procurement. If one entity is uncovered during a transaction, it can easily and quickly be replaced with a new entity. It is also possible for Trust or Company Service Providers to buy shelf companies with established banking and credit histories, in order to give the appearance of a reputable company. Nominee shareholders or directors have also been used.

Companies House has been linked to a number of PF cases and is a likely target of continued activities by PF actors. A number of UK entities have been sanctioned by the US Treasury for owning vessels trading in North Korean coal. In some cases, shell companies have been used in the UK by a Chinese-based trader involved in cross-border trades with North Korea, who acted on behalf of North Korean proliferators and helped procure items for their weapons programme while laundering tens of millions of dollars.

Ongoing reform of Companies House is aimed at adding additional layers of security to the system, and provide

Companies House a bigger role in combatting economic crime. The Economic Crime and Corporate Transparency Bill will expand the remit of Companies House. The powers of the Registrar of Companies will be broadened so they become a more active gatekeeper for company creation and custodian of more reliable data, including new powers to check, remove or decline information submitted to, or already on, the Company Register.

Companies House will also have increased investigation and enforcement powers, and will be better able to cross-check data with other public and private sector bodies.

There will be a new identity verification requirement for people who manage, own and control companies and other UK registered entities. This requirement is aimed at improving the accuracy of Companies House data, to support business decisions and law enforcement investigations.

### Low awareness of PF

There is generally low awareness

of proliferation financing risks among Designated Non-Financial Businesses and Professions (DNFBPs), and the focus against PF continues to be on financial institutions, potentially at the expense of other DNFBPs. Given the role these UK-based bodies play in facilitating global finance, this creates a particular risk to the UK. Low awareness of PF, as part of sanctions and money laundering compliance, could enable PF risks. This is particularly relevant for trust and company service providers given the ease of establishing a company in the UK.

### UK Crown Dependencies and Overseas Territories

The UK has a close relationship with Crown Dependencies and Overseas Territories who are intrinsically linked to the UK financial system. Criminals often seek to exploit this relationship and disguise illicit assets by taking advantage of services offered in these jurisdictions. Financial centres in the Crown Dependencies and Overseas Territories may be used for proliferation financing purposes, in particular by establishing

corporate entities and accessing the formal financial system.

Businesses which have close links to the Crown Dependencies and Overseas Territories, or those based there or with officers in those jurisdictions, should pay particular interest to PF risks.

## Cryptocurrencies

Sanctioned actors are known to use cryptocurrency to evade international sanctions. Despite the security of some aspects of cryptocurrency, there are also key AML and PF risks, given the ease with which cash can be converted into cryptocurrency in places like El Salvador and Venezuela.

The use of cryptocurrencies as both a tool for fundraising – such as via hacking exchanges or receipt of payments – as well as fund movement, has allowed North Korea to evade the traditional financial system in a new way that does not require a physical presence in the target countries.

At least \$316m of virtual assets was stolen by North Korea just in

2019-2020. Iran may have also launched a Central Bank Digital Currency to operate as part of an alternative financial system. Iran has also raised assets by mining digital currency.

Despite cryptoasset businesses in the UK coming under the scope of the MLRs in 2020, many UK consumers rely on non-UK based exchanges. Despite exchanges having to be registered and supervised by the FCA, a significant number are not meeting the required standard and many may not have adequate AML procedures.

## Global defence manufacturing

The UK is the world's second largest defence exporter and third largest security exporter. These industries offer widespread opportunities for proliferation actors. All UK sectors connected to production of military and dual-use items can be exploited by proliferating actors. This includes sectors such as chemical production and the life sciences.

How PF actors approach these sectors can depend on whether

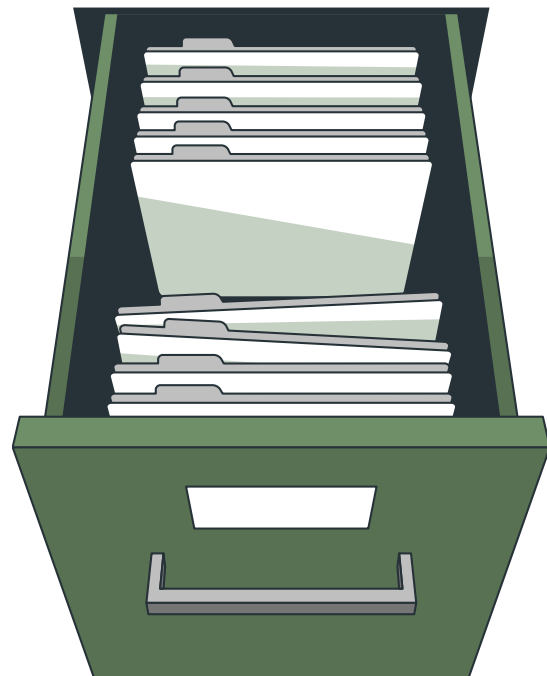
they are a state or non-state entity. It is unlikely for major defence suppliers to contract with private entities. Therefore the most at risk areas are medium-sized sub-contractors and the dual-use sector. Small arms and light weapons; small arms ammunitions and tank/artillery munitions; individual ballistic protection; vehicle armour and vehicles; communications (also dual-use); chemical and biological materials and related equipment, are types of items that attract procurement attempts from overseas actors.

The UK operates its own export control regimes and complies with international regimes, such as the Australia Group and the Wassenaar Agreement, to ensure that the trade in dual-use and sensitive items does not pose a threat to international security. North Korean actors have often attempted to procure these items through Chinese front companies.

## Education and research sectors

The UK is an education hub for research in specific technologies,

particularly those that could have a role in proliferation and weapons of mass destruction. Increasing levels of funding from overseas to British academic institutions makes the sector vulnerable to potential pressure from states with proliferating ambitions. The UK expects universities to implement guidelines to make informed decisions around international collaborations, and provide security advice on topics such as export controls, cyber security and protection of intellectual property.



## How to counter proliferation financing

### Good practice

- ✔ Adequate and effective onboarding processes and procedures for customers
- ✔ Enhanced customer due diligence procedures
- ✔ Maintaining and managing lists of customers/associated parties/ships/aircraft/entities/persons identified as potentially related to the TFS-PF designations
- ✔ Adequate controls to ensure effectiveness of procedures for sanctions screening to identify and mitigate potential sanctions evasion
- ✔ Providing staff training that includes training on PF risks, risk mitigation measures, policies and procedures
- ✔ Demonstrating awareness of entities and persons who are not designated, but who are known from reliable and independent third party sources to have connections to proliferation activities
- ✔ Tailored sanctions training
- ✔ Supplementing reliance on list-based screening by enhanced customer due diligence measures to also capture indirect relationships and underlying assets which may be included on a sanctions list.
- ✔ Maintaining documentation which clearly sets out who is responsible for screening systems

### Poor practice

- ✘ Staff dealing with trade-related sanctions queries are not appropriately qualified and experienced
- ✘ Failure to screen trade documentation or document decision-making
- ✘ Failure to screen against all relevant international sanctions lists
- ✘ Failure to record the rationale for decisions to discount name matches
- ✘ Failure to undertake risk-sensitive screening of information held on agents, insurance companies, shippers, freight forwarders, delivery agents, inspection agents, signatories, and parties mentioned in certificates of origin, as well as the main counterparties to a transaction
- ✘ Failure to record the rationale for decisions that are taken not to screen particular entities and retaining that information for audit purposes
- ✘ No clear dual-use items policy
- ✘ Failure to undertake further research where goods descriptions are unclear or vague third-party data sources are not used where possible to undertake checks on dual-use items

## Proliferation financing red flags

### Customer profile

- ✓ Customer is vague or provides incomplete information about their proposed trading activities or is reluctant to provide additional information
- ✓ Customers, in particular trade entities, owners or managers, appear on sanctioned lists or in adverse news reports alleging criminal activity, investigations or convictions
- ✓ The customer is a person connected with a country of proliferation or country of concern, e.g. Syria or China
- ✓ The customer deals with dual-use items or goods subject to export control but lack the technical background or their profile does not align with expectations
- ✓ The customer engages in complex trade deals involving numerous third-party intermediaries, in lines of business that do not accord with their stated business profile as established during the on-boarding of the business
- ✓ A customer or counterparty, declared to be a commercial business, conducts transactions that suggest they are acting as if they were a money-remittance business or as a pay-through account
- ✓ A customer affiliated with a university or research institution is involved in the trading of dual-use items or goods subject to export control

- ✓ A customer deals, directly or indirectly, with trade of sanctioned goods or under embargo, such as oil or other commodities, luxury goods, metals etc

### Account and transaction activity

- ✓ The originator or beneficiary of a transaction is a person or an entity ordinarily resident of or domiciled in a country of proliferation e.g. North Korea or Iran
- ✓ Account holders conduct transactions that involve items controlled under dual-use or export control regimes, or the account holders have previously violated requirements under dual-use or export control regimes
- ✓ Accounts or transactions involve possible companies with opaque ownership structures, front companies or shell companies
- ✓ There are links between representatives of companies exchanging goods, e.g. the same owners or management, same physical address, IP address or telephone number, or which otherwise indicates their activities may be coordinated
- ✓ An account holder conducts financial transactions in an indirect manner, or in a manner that otherwise does not appear to make business sense

- ✔ Account activity or transactions where the originator or beneficiary of associated financial institutions is domiciled in a country with weak implementation of relevant UNSCR obligations and FATF Standards, or a weak export control regime, or vulnerable correspondent banking services
- ✔ A customer of a manufacturing or trading firm wants to use cash in transactions for industrial items or for trade transactions more generally
- ✔ Transactions are made on the basis of ledger arrangements that remove the need for frequent international financial transactions
- ✔ A customer uses a personal account to purchase industrial items that are under export control, or otherwise not associated with corporate activities or congruent lines of business

## Trade finance

- ✔ Prior to the account approval, the customer requests letter of credit for a trade transaction for shipment of dual-use items or goods subject to export control
- ✔ There is a lack of full information or inconsistencies are identified in trade documents and financial flows, such as names, companies, addresses, or final destination
- ✔ Transactions include wire instructions or payment details from, or due to, parties not identified on the original letter of credit or other documentation

## Maritime sector

- ✔ A trade entity is registered at an address that may be a mass registration address, e.g. high-density residential buildings, post-box addresses, commercial buildings or industrial complexes, particularly when there is no reference to a specific unit
- ✔ The person or entity preparing a shipment lists a freight forwarding firm as the product's final destination
- ✔ The destination of a shipment is different from the importer's location
- ✔ Inconsistencies are identified across contracts, invoices, or other trade documents, e.g. contradictions between the name of the exporting entity and the name of the recipient of the payment, differing prices on invoices and underlying contracts, discrepancies between the quantity, quality, volume or value of the actual commodities and their descriptions, or which otherwise do not appear to correctly reflect what is to be anticipated
- ✔ Shipment of goods have a low declared value in comparison with the shipping cost
- ✔ Shipment of goods is incompatible with the technical level of the country to which it is being shipped, e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry



- ✔ Shipment of goods is made in an indirect fashion that cannot be easily explained, including multiple destinations with no apparent business or commercial purpose, indications of frequent flags hopping (flags of convenience practices), or using a small or old fleet
- ✔ Shipment of goods is inconsistent with normal geographic trade patterns, e.g. the destination country does not normally export or import the goods listed in the trade transaction documents
- ✔ Shipment of goods is routed through a country with weak implementation of relevant UNSCR obligations and FATF Standards, export control laws or weak enforcement of export control laws
- ✔ Payment for imported commodities is made by an entity other than the consignee of the commodities for no clear economic reasons, e.g. by a Shell company or Front company not involved in the trade transaction

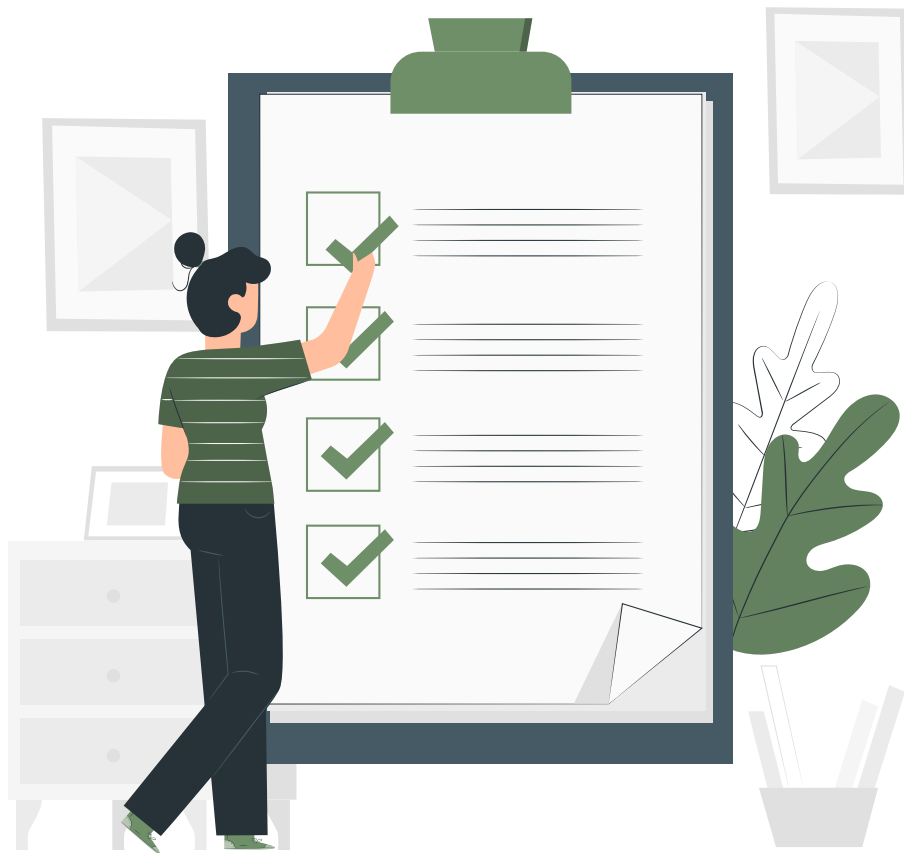
## Other red flags

- ✔ Research agreements with, or training at, universities and research centres abroad
- ✔ Acquisition of foreign licences or patents
- ✔ Merging with, absorbing, or acquiring foreign companies producing sensitive or export control goods



## What to do now

- ✔ Review your business for PF risks. Key risks could include:
  - Exposure to Iran or North Korea, including entities or individuals
  - Exposure to oil, coal and sand in relation to China and Syria
  - Involvement with exporters or manufactures of defence, dual-use or other proliferation-related goods
- ✔ Review your AML policies and sanctions policies in light of PF risks
- ✔ Amend your risk assessments to incorporate PF risks
- ✔ Implement specific controls and measures highlighted by the PF risk assessment
- ✔ Record these controls and analyse their effectiveness



## Glossary

**AML** - anti-money laundering

**CPF** - counter-proliferation financing

**Consignee** - The person or organisation to which goods are exported. Literally, the person to whom the goods are consigned. Not necessarily the end user

**DPRK** - Democratic People's Republic of Korea (North Korea)

**Dual-use** - items such as software or technology which can be used for both civil and military purposes

**FATF** - Financial Action Task Force - the global AML standards body  
**Forfeiter** - In international trade, the selling of an exporter's receivables (money due) for a particular transaction. Generally, the exporter forfeits the receivable at a discount. This improves cash flow but reduces income. The buyer is known as a forfeiter, and assumes all the risks associated with collecting the receivables

**Front company** - a company that appears to undertake legitimate business but which in reality is obscuring illicit financial activity

**Letter of credit** - A binding document that a buyer can request from his bank in order to guarantee that the payment for goods will be transferred to the seller. A letter of credit gives the seller reassurance that he will receive the payment for the goods

**Money laundering** - laundering the proceeds of crime

**PF** - proliferation financing

**Proliferation** - Proliferation of weapons of mass destruction - the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including dual-use items used for illicit purposes), in contravention of national laws or, where applicable, international obligations

**Proliferator** - A State, natural or legal person, or a legal arrangement, undertaking proliferation may, at times, be referred to as a proliferator

**Proliferation - sensitive goods** - Nuclear, chemical or biological equipment, material, or technology used in the research, design, development, testing, or production of nuclear, chemical or biological weapons

**Shell company** - An inactive company used as a conduit for money that do not have a high level of capitalisation or which displays other Shell company indicators such as long periods of account dormancy followed by a surge of activity

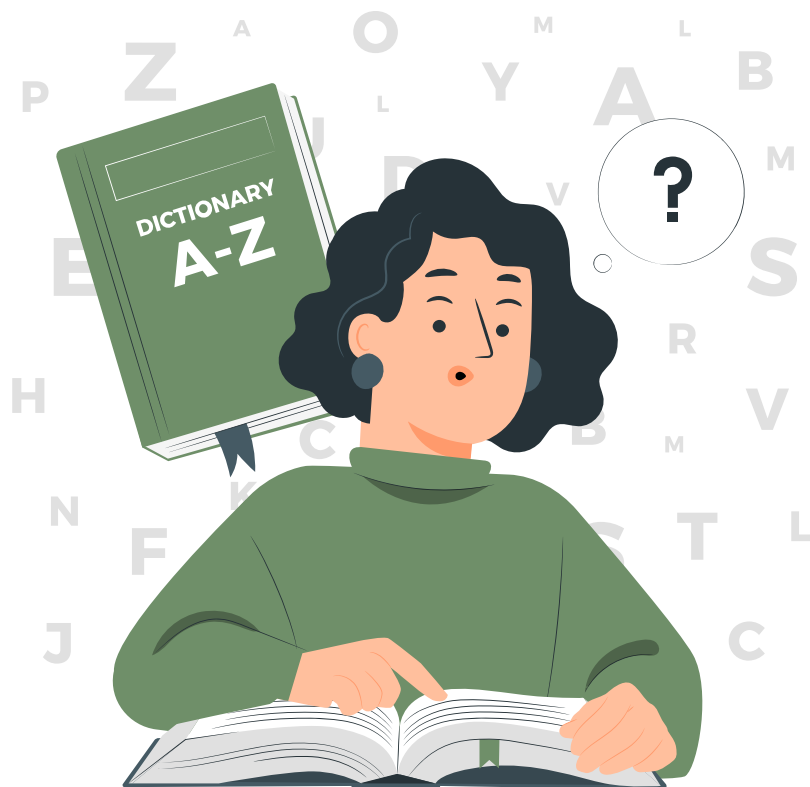
**TFS** - Targeted financial sanctions, means both (i) asset-freezing and (ii) prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of those targets designated as being subject to sanctions

**TFS-PF** - Targeted financial sanctions relating to the prevention, suppression and disruption of Proliferation of weapons of mass destruction and proliferation financing

**UNSC** - United Nations Security Council

**UNSCR** - United Nations Security Council Resolution

**WMD** - Weapons of mass destruction, including, for example, atomic explosive weapons, lethal biological and chemical weapons, radioactive material weapons and any weapons developed in the future which have comparative destructive effects



## VinciWorks' AML compliance products

### AML Audit

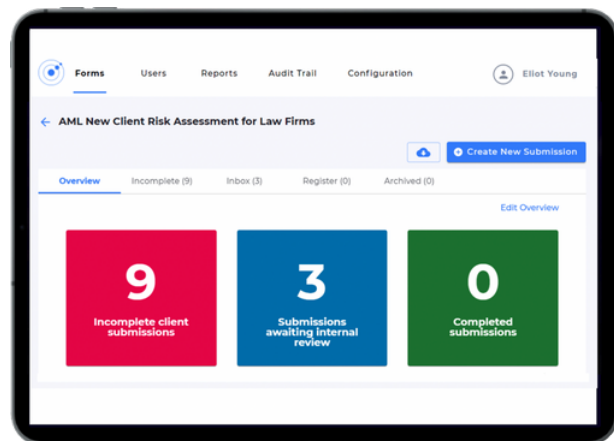
Recent SRA guidance and commentary suggests that the vast majority of law firms conducting work subject to the anti-money laundering regulations will require an independent anti-money laundering audit. While this does not necessarily need to be conducted by external specialists, increasingly that is the most popular route. Our partner, Compliance Office, has the expertise needed to help you conduct an independent AML audit. Their team keeps their pulse on the latest AML requirements and your audit will often be administered by former SRA staff.

Free Consultation

### AML Onboarding Solution

VinciWorks' AML client onboarding solution powered by Omnitrack, facilitates a seamless onboarding experience for organisation of all sizes. With multiple templates catering for different industries and jurisdictions, VinciWorks' solution provides regulatory confidence through up-to-date guidance and best practice. The streamlined solution caters for the full AML process from client identification and verification, to, document collection, to, relevant risk assessments and ongoing monitoring.

VinciWorks' industry specific templates are also 100% customisable giving you the flexibility to ensure the tool works for your organisation. Our team will guide you through every step of the process.



From integration with existing software to retrieving up-to-the-minute reports, VinciWorks have you covered.

[Book a Demo](#)

## Interactive AML training

VinciWorks strives to make its AML training more than simply a tick-box exercise. Our courses are packed with realistic scenarios, real-life case studies and every customisation option you can think of. We have everything from in-depth induction training to refresher courses and five minute knowledge checks.




Our AML courses bring a fresh, bold, new design and begin with a course builder to deliver the most relevant training to each user. Whichever industry, jurisdiction or job role you work in, a course can instantly be built just for your staff.

[Try Our Courses](#)

## Contact Us

 [www.vinciworks.com](http://www.vinciworks.com)

 [enquiries@vinciworks.com](mailto:enquiries@vinciworks.com)

 +44 (0) 208 815 9308

